

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

DOKTORA TEZİ

ÖZEL YAŞAMIN BİR PARÇASI OLARAK
TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN
GİZLİLİĞİNE ÖNLEYİCİ DENETİM YOLUYLA MÜDAHALE

SAADET YÜKSEL

2502060220

TEZ DANIŞMANI

PROF. DR. BERTİL EMRAH ODER

İ. Ü. Kütüphane	
Den.	49129
Sıra No.	

İSTANBUL, 2012



DOKTORA
TEZ ONAYI

ÖĞRENCİNİN

Adı ve Soyadı : SAADET YÜKSEL
Anabilim/Bilim Dalı : KAMU HUKUKU
Danışman : Prof. Dr. BERTİL EMRAH ODER

Numarası : 2502060220
Tez Savunma Tarihi : 20.03.2012
Tez Savunma Saati : 14:00

Tez Başlığı : ÖZEL YAŞAMIN BİR PARÇASI OLARAK TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN GİZLİLİĞİNE ÖNLEYİCİ DENETİM YOLUYLA MÜDAHALE

TEZ SAVUNMA SINAVI, Lisansüstü Öğretim Yönetmeliği'nin 35. Maddesi uyarınca yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin KABULÜ'NE OYBİRLİĞİ / OYÇOKLUĞUYLA karar verilmiştir.

JÜRİ ÜYESİ	İMZA	KANAATI (KABUL / RED / DÜZELTME)
PROF. DR. ADEM SÖZÜER		Kabul
PROF. DR. FÜSUN SOKULLU-AKINCI.		Kabul
PROF. DR. NECMİ YÜZBAŞIOĞLU		Kabul
PROF. DR. SERAP YAZICI		Kabul
PROF. DR. BERTİL EMRAH ODER.		Kabul

ÖZ

Özel yaşamın gizliliği hakkının her alanda ihlal edildiği, her dönem düzenli sayılabilecek tartışmalarla kendini göstermiştir. Fakat günümüzde bu temel hak ve özgürlüğün ulusal güvenlik ve suçun önlenmesi amacıyla teknolojiden yararlanılması yoluyla ihlali, en yoğun ve güncel tartışmaları oluşturmaktadır. Çalışmada, özel yaşamın gizliliği hakkının telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesi yoluyla ihlali sorunu, kuramsal çerçeve bağlamında Türk ve A.B.D. hukukundan ve AB mevzuatından somut olaylarla incelenmiştir. Öncelikle özel yaşamın gizliliği hakkı, temel hak ve özgürlük boyutuyla ve kavramın anlam ve kapsamına ışık tutarcasına irdelenmiştir. Telekomünikasyon yoluyla yapılan iletişimin denetlenmesiyle bu hakka yapılan müdahalenin yarattığı hukuki sorun ve çözümleri tartışabilmek açısından, iletişimin denetlenmesi tedbirinin türleri de, kavramlara açıklık getirilerek incelenmektedir. Tedbir sonucu elde edilen bilgilerin, kişisel veri niteliği yine özel yaşamın ve iletişimin gizliliği çerçevesinde, ulusalüstü belgeler ışığında ele alınmaktadır. Özellikle AB ve A.B.D. hukukunun yaklaşımı, Türk hukukuyla paralellik kurularak irdelenmektedir. Son olarak, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi mevzuat ve uygulama bağlamında, anayasa ve ceza hukukuna dair yarattığı sorunlar ve çözüm önerileriyle birlikte değerlendirilmiştir.

Türk hukukunda iletişimin önleme amaçlı denetimine dair düzenleme yeni sayılabilecek niteliktedir. Çalışmada denetime yönelik spesifik hususlar, bu yenilik dikkate alınarak ve denetimin özel yaşamın gizliliği hakkına yarattığı müdahale boyutuyla ele alınmıştır. Mevcut hukuki düzenlemeler ve uygulama, iletişimin ve özel yaşamın gizliliği hakkının sınırlandırılmasına dair ilkeler ışığında değerlendirilmiştir. A.B.D. hukukundaki yargısal kararlar ve Avrupa İnsan Hakları Mahkemesi (AİHM) yaklaşımı, yararlanılan başlıca yargı düzenlerini oluşturmuştur. Çalışmada belirlenen temel husus, iletişimin önleme amaçlı denetlenmesine dair hukuki çerçevenin, keyfiligi önleyecek, hukuk devletine yaraşır bir uygulamayı

sağlayacak, temel hak ve özgürlüklerin hukuka aykırı sınırlanmasına ve belirsizliğe yol açmayacak bir anlayışla oluşturulması gerektiği olarak ortaya çıkmaktadır.

ABSTRACT

The restriction of the right to privacy is a contentious issue that has led to much debate. Increased use of information technologies for the purposes of national security, intelligence gathering, and crime prevention has intensified this debate on privacy protection. This paper explores the issue of electronic surveillance of wire and electronic communications in the context of Turkish and U.S. privacy laws and European Union directives. The paper first explores the right to privacy as a fundamental right and freedom through a detailed examination meant to shed light on the purport and scope of the right. It then sets the stage for a discussion about solutions to restricting informational privacy by taking a detailed look at every type of interception of wire and electronic communications. The paper then moves to discuss the protection of personal data so obtained in the context of international documents relating to the protection of personal privacy and the right to communication; since Turkish law in the privacy sphere is still nascent, arguments for the protection of personal data is made on the basis of the U.S. and EU privacy laws. Finally, the paper explores surveillance of electronic and wire communications within Turkish law, taking into account current legislation and constitutional problems resulting from electronic surveillance and examining alternative solutions to these problems.

Constitutional problems relating to wiretap and electronic surveillance are examined in the context of the rapid growth in Turkish privacy law and current legislation and the implementation of this legislation are discussed in connection with the principle of restriction of the right to privacy. The judicial approaches discussed in this paper are the U.S. Supreme Court's and the European Court of Human Rights' approaches. The main conclusion of this paper is that the legal framework for privacy law should be established by an approach that recognizes the importance of preventing arbitrary privacy restrictions and protecting fundamental rights and freedoms.

ÖNSÖZ

Özel yaşamın gizliliği hakkı ve korunması, Türk hukukunda, anayasayla güvence altına alınmış temel hak ve özgürlüklere dair günümüzde en çok tartışılan hususlardan birini oluşturmaktadır. Diğer toplumlarda da, farklı hukuki ve siyasi yapılanmalara rağmen, özel yaşamın gizliliği hakkına ilişkin tartışmalar ve kaygılar benzer konularda yoğunlaşmaktadır. İç içe geçmiş olan bu hususların açıklığa kavuşturulması aynı zamanda çalışmanın da ortaya çıkış amacı ve kapsamını ortaya koyacaktır. Buna göre, öncelikle özel yaşamın gizliliği hakkına müdahalenin yarattığı hukuki sorunlar kadar, hakkın kavram ve kapsamının açıklığa kavuşturulması noktasında da ortak bir kaygının mevcut olduğu söylenebilir. Nitekim teknolojinin getirdiği değişiklikler ve yaşam ilişkilerinin ve suçla mücadeledeki anlayışın bu yönde farklılaşması hemen her toplumda, farklı hızla da olsa, kendini gösterebilmiştir. Her toplumda, özel yaşamın ve iletişimin gizliliği demokrasi, güvenlik ve bağımsızlık hususlarıyla birlikte tartışılır hale gelmiş ve artan şekilde hukuki düzenlemelerin konusunu oluşturmuştur. Tüm bu özellikleri dolayısıyla, özel yaşamın ve iletişimin gizliliği hakkı sadece ulusal hukukların değil, uluslararası hukukun da üzerinde hassasiyetle durduğu konulardan biri olmuştur. Bu nedenle çalışmada, Türk hukukundaki mevcut düzenlemelere ve uygulamaya yansıyan anlayışa sadece eleştirel gözle bakılmamış; A.B.D. hukuku, Avrupa Birliği mevzuatı ve yargısal düzlemde A.B.D. Yüksek Mahkemesi (**Supreme Court**) ve AIHM yaklaşımıyla paralellik kurularak değerlendirmeler yapılmıştır.

Çalışmanın birinci bölümünde özgün bir şekilde, özel yaşamın gizliliği hakkına dair tanımlama kaygısından uzak, kavrama yönelik bütünlüklü bir bakış açısı yansıtılabilmek amacıyla, kavrama ilişkin mevcut yaklaşımlar tartışılmıştır. Bu yönüyle hakkın koruduğu temel değerler bağlamında, hakkın kapsamı açıklanmaya çalışılmış ve bu hakkın korunmasında hangi hususlara dikkat edilmesi gerektiği gözler önüne serilmeye çalışılmıştır. Bu yolu izlemedeki temel amaç, telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesinin özel yaşamın ve iletişimin gizliliği açısından yarattığı ihlale, mevcut çalışma ve bakış

açılarından farklı olarak, anayasa hukukunun hak ve özgürlüklerin sınırlandırılmasına dair esaslı unsurları açısından yaklaşılmalı istenmesi olmuştur. Buna göre, özel yaşamın gizliliği hakkı tek başına olabilmek, kişisel bilgi üzerindeki kontrol imkanı, mahremiyet, kişiye sınırlı ulaşım ve kişisel bağımsızlık yönlerinden ayrıntılı olarak ele alınmıştır. Bu hakkın korunmasıyla gözetilen değerler, A.B.D. ve AB yaklaşımı da dikkate alınarak ve hatta kavramsal farklılıklar da açıklığa kavuşturularak incelenmiştir.

Çalışmanın ikinci bölümünde, Türk hukukunda telekomünikasyon yoluyla yapılan iletişimin gizliliği ve denetlenmesi 1961 ve 1982 Anayasası'nı kapsar şekilde, Türk Anayasa hukuku ve iletişimin önleme amaçlı denetimine dair yasal dayanağı oluşturan 5397 sayılı Kanun çerçevesinde ayrıntılı olarak değerlendirilmiştir. Bu bölümde de, A.B.D. ve Avrupa anlayışı iletişimin denetlenmesine dair kullandıkları farklı kavramlar bağlamında, Türk hukukuyla paralellik kurularak analiz edilmeye çalışılmıştır. Bu bağlamda özellikle, iletişimin denetlenmesi tedbirinin türleri olarak iletişimin dinlenmesi, tespiti, kaydedilmesi ve sinyal bilgilerinin değerlendirilmesi gerek teorik altyapı gerek uygulama bağlamında incelenmiştir.

Kişisel verilerin korunması üçüncü bölümde özel yaşamın gizliliği hakkı çerçevesinde ele alınmaktadır. Zira telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesi sonucu elde edilen bilgi “kişisel veri” kapsamında nitelendirilerek; Türk hukukunda özel ve gizli yaşam alanının ve böylece kişisel verilerin kural olarak korunduğu noktasından bir değerlendirme yapılmıştır. Bu bağlamda telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetimi dolayısıyla elde edilen bilginin kişisel veri olarak, kişisel verilerin korunması güvencelerinden yararlanması gerektiği bu bölüm açısından hem bir çıkış noktası hem de yeni yapılacak düzenlemeler açısından bir öneri olarak ortaya konulmaktadır. Korumaya ihtiyacı olanın bilgi mi yoksa kişi mi olduğu bu bölümde irdelenen esaslı meselelerden biridir. Bu bağlamda, Bu bölümde Türk hukukunda kişisel verilerin korunması açısından hassasiyetle göz önünde bulundurulmuş ve hatta Türk hukuk düzenlemelerine de yansıyan AB'nin ilgili Yönergeleri de ayrıntılı olarak incelenmiştir. Buna göre, kişisel verilerin korunmasına ilişkin, ilgilinin rızasının

aranması, veri işleme sırasında ilgilinin bilgilendirilmesi, veri işlemenin gizliliği, veriye ulaşma, veriyi düzeltme, silme, veriye ulaşmayı engelleme, itiraz hakkı ve veri işleme faaliyetinin açıklığı gibi ilkeler gerek AB Yönergeleri gerek Türk hukukundaki Kişisel Verilerin Korunması Kanunu Tasarısı dikkate alınarak açıklanmıştır.

Çalışmanın son bölümünde ise, Türk hukukunda telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesinin şartları ve uygulanması ayrıntılı olarak ele alınmıştır. Önleme amaçlı denetimin kapsam ve türleri, özgün bir şekilde A.B.D. hukukundaki iletişimin denetlenmesi tedbiriyle paralellik kurularak açıklanmıştır. Bu bağlamda, iki hukuk düzeni arasındaki farklılıklar da göz önünde bulundurularak, iletişimin denetlenmesi tedbirine ilişkin Türk hukukundaki farklılık veya eksiklikler karşılaştırmalı bir bakış açısıyla yansıtılmıştır. 5397 sayılı Kanun ve TİB'in tedbire yönelik uygulaması, özel yaşamın gizliliği hakkının korunmasına dair önceki bölümlerde oluşturulan hukuki çerçeve dikkate alınarak değerlendirilmiştir. Tedbirin hukuka aykırı uygulanması ve yaptırımı da idarenin ve kamu görevlilerinin sorumluluğu ve ceza hukuku açısından irdelenmiştir.

Türk hukukunda iletişimin denetlenmesi ile ilgili ilkelerin, Avrupa ve A.B.D. yaklaşımındaki ortak ilkelerle düzenlendiği de göz önünde bulundurulursa; önleme amaçlı denetime ilişkin yasal dayanağı oluşturan düzenlemelerin, bu iki yaklaşımın ve özellikle AİHM'nin benimsediği şekliyle özel yaşamın ve iletişimin gizliliğini sınırlandıracak bir yasa olarak, açıklık ve öngörülebilirlik gibi unsurları karşılayacak şekilde düzenlenmesi gerektiği başlıca sonuç olarak ifade edilebilir.

Bu çalışmaya başlamamda ve çalışmayı akademik titizlik ve derinlikle yürütüp sonuçlandırabilmemde bana yol göstermiş olan tez danışmanım Sayın Prof. Dr. Bertil Emrah Oder'e içtenlikle teşekkür ederim.

İÇİNDEKİLER

ÖZ	ii
ABSTRACT	iv
ÖNSÖZ	v
İÇİNDEKİLER	viii
KISALTMALAR LİSTESİ	xi
GİRİŞ	1

BİRİNCİ BÖLÜM

ÖZEL YAŞAMIN GİZLİLİĞİ HAKKI ve KORUDUĞU DEĞERLER

I. ÖZEL YAŞAMIN GİZLİLİĞİ	5
A. Genel Olarak	5
B. Özel Yaşam Kavramına İlişkin Çeşitli Yaklaşımlar	7
1. Tek Başına Olabilmek Hakkı	7
2. Kişisel Bilgi Üzerindeki Kontrol İmkânı	15
3. Mahremiyet (Intimacy)	20
4. Kişiye Sınırlı Ulaşım	26
5. Kişisel Özerklik / Bağımsızlık	28
II. ÖZEL YAŞAMIN GİZLİLİĞİ KAVRAMININ KAPSAM İTİBARIYLA DEĞERLENDİRİLMESİ	29
A. Özel Yaşamın Gizliliği Kavramının Koruduğu Değerler	29
B. Özel Yaşamın Gizliliğinin Tanımlanması Mümkün mü? Gerekli mi?	36
III. ÖZEL YAŞAMIN GİZLİLİĞİ AÇISINDAN AVRUPA BİRLİĞİ ve A.B.D. HUKUKUNUN YAKLAŞIM FARKLILIĞI	38

İKİNCİ BÖLÜM

TÜRK HUKUKUNDA TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN GİZLİLİĞİ VE DENETİMİ

I. KAVRAMLAR	55
A. İletişim	56
B. Telekomünikasyon Yoluyla Yapılan İletişim	58
C. İletişimin Denetlenmesi	60
II. TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN DENETLENMESİNİN ÖZEL YAŞAMIN GİZLİLİĞİ VE İLETİŞİMİN GİZLİLİĞİ BAĞLAMINDA DEĞERLENDİRİLMESİ	67
A. Özel Yaşamın Gizliliği Bakımından	67
1. 1961 Anayasasında Özel Yaşamın Gizliliği	68
2. 1982 Anayasasında Özel Yaşamın Gizliliği	69
B. İletişimin Gizliliği Bakımından	79
C. 5397 Sayılı Kanun'un Özel Yaşamın Gizliliği ve İletişimin Gizliliği Hakkının Sınırlandırılması Açısından Değerlendirilmesi	85

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI

I. GENEL OLARAK	92
II. AVRUPA KONSEYİ VE AVRUPA BİRLİĞİ MEVZUATI BAĞLAMINDA KİŞİSEL VERİLER	93
A. Avrupa Birliği Yönergeleri	95
B. Avrupa İnsan Hakları Sözleşmesi	108
C. Avrupa Birliği Temel Haklar Şartı	114
III. KİŞİSEL VERİLERİN KORUNMASINA DAİR TEMEL İLKELER ...	119
A. Kişisel Verilerin Kaliteli Olması	120
B. Kişisel Verinin İşlenebilmesi İçin İlgilinin Rızasının Aranması İlkesi ...	121
C. Hassas Verilerin İşlenmesi	123
D. Kişisel Verinin İşlenmesi Sırasında İlgilinin Bilgilendirilmesi	126
E. Kişisel Verinin İşlenmesi Sırasında Veriye Ulaşma, Veriyi Düzeltme, Silme, Veriye Ulaşmayı Engelleme ve İtiraz Hakkının Korunması	128
F. Veri İşlemenin Gizliliği ve Veri Güvenliği İlkesi	131
G. Veri İşleme Faaliyetinin Açıklığı	132
IV. KİŞİSEL VERİLERİN KORUNMASI BAĞLAMINDA ÖZEL YAŞAMIN GİZLİLİĞİNE DAİR AVRUPA BİRLİĞİ YAKLAŞIMININ A.B.D. YAKLAŞIMIYLA GENEL BİR KARŞILAŞTIRMASI	133
V. TÜRK HUKUKUNDA ÖZEL YAŞAMIN GİZLİLİĞİ HAKKININ KORUNMASI BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI	139
A. 1982 Anayasası ve Yürürlükteki İlgili Diğer Mevzuat Bakımından	139
B. Kişisel Verilerin Korunması Kanunu Tasarısı	144

DÖRDÜNCÜ BÖLÜM

TÜRK HUKUKUNDA TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN ÖNLEME AMAÇLI DENETLENMESİNİN ŞARTLARI VE UYGULANMASI

I. TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN ÖNLEME AMAÇLI DENETLENMESİNİN AMACI, KAPSAMI VE TÜRLERİ	155
A. Genel Olarak	155
B. İletişimin Önleme Amaçlı Denetlenmesinin Amacı	156
1. Polis Bakımından	156
2. Jandarma Bakımından	157
3. Milli İstihbarat Teşkilatı Bakımından	157
C. İletişimin Önleme Amaçlı Denetlenmesinin Kapsamı	158
D. İletişimin Önleme Amaçlı Denetlenmesinin Türleri	159
1. Genel Olarak	159
2. İletişimin Tespiti	161
3. İletişimin Dinlenmesi	165
4. İletişimin Kayda Alınması	166
5. Sinyal Bilgilerinin Değerlendirilmesi	168
E. A.B.D. Hukukundaki İletişimin Denetlenmesi Tedbirlerinin Türk Hukukuyla Paralellik Kurularak Genel Olarak Değerlendirilmesi	170

1. Genel Olarak	170
2. Elektronik İletişimin Gizliliği Kanunu / The Electronic Communications Privacy Act (ECPA)	170
a. Tel İle Gerçekleştirilen İletişimin Dinlenmesine Dair Kanun / The Wiretap Act	171
b. Depolanmış İletişime Dair Kanun / The Stored Communications Act (SCA)	173
c. Teknik Bilgileri İçeren Kayıtlara Dair Kanun / The Pen Register Act	174
3. Yabancı İstihbarat Denetimi Kanunu / The Foreign Intelligence Surveillance Act (FISA)	175
II. TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN ÖNLEME AMAÇLI DENETLENMESİNİN KOŞULLARI VE UYGULANMASI	178
A. İletişimin Önleme Amaçlı Denetlenmesinin Koşulları	178
1. Genel Olarak	178
2. Tedbirin Uygulanacağı Kişiler	179
3. İletişimin Önleme Amaçlı Denetlenmesi Tedbirinin Uygulanmasıyla Önlenmesi Amaçlanan Suçlar	180
a. Polis ve Jandarma Bakımından	180
b. Milli İstihbarat Teşkilatı Bakımından	184
4. İletişimin Önleme Amaçlı Denetlenmesi Tedbirinin Uygulanmasında Suç İşleme İhtimali	186
5. İletişimin Önleme Amaçlı Denetlenmesi Tedbirinin Talep Edilmesi ve Karar	191
a. Hakimin Kararının Veya Yazılı Emrin İçeriği Ve Bulunması Gereken Bilgiler	197
b. Tedbirin Süresi	200
B. İletişimin Önleme Amaçlı Denetlenmesi Tedbirinin Uygulanması	205
1. Tedbirin Yerine Getirilmesi	205
2. Gizlilik	207
C. Tedbire Son Verilmesi	208
D. Kayıtların Yok Edilmesi	211
III. TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN ÖNLEME AMAÇLI DENETLENMESİ SONUCU ELDE EDİLEN VERİLERİN NİTELİĞİ ve KULLANIMI	213
IV. HUKUKA AYKIRI OLARAK TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN ÖNLEME AMAÇLI DENETLENMESİ VE YAPTIRIMI	218
A. Hukuka Aykırılık	218
B. Tazminat	220
1. Genel Olarak	220
2. İdarenin ve Kamu Görevlilerinin Sorumluluğu	221
3. Ceza Hukuku Açısından Sorumluluk	223
4. İdari Denetim	225
SONUÇ	227
KAYNAKÇA	230
ÖZGEÇMİŞ	258

KISALTMALAR LİSTESİ

a.e.	: aynı eser
a.g.e.	: adı geçen eser
a.g.m.	: adı geçen makale
a.y.	: yazara ait son zikredilen yer
AB	: Avrupa Birliği
A.B.D.	: Amerika Birleşik Devletleri
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
Bkz.:	: bakınız
bs.	: bası
C.	: Cilt
CIA	: Central Intelligence Agency
CMK	: 5271 sayılı Ceza Muhakemesi Kanunu
ÇAŞÖMK	: 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu
çev.	: çeviren
Doc.	: Document
DPT	:Data Protection Act
E.	: Esas Numarası
ECPA	: The Electronic Communications Privacy Act/
Ed. by	: editör/yayına hazırlayan

EU	: European Union
FAA	: Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008
FBI	: Federal Bureau of Investigation
FISA	: Foreign Intelligence Surveillance Act
GSM	: Global System for Mobile Communications
İletişimin Denetlenmesi Yönetmeliği	: Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik
IP	: İnternet protokol adresi
Jandarma Kanunu	: 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu
K.t.	: Karar tarihi
L. Rev.	: Law Review
L. J.	: Law Journal
MİT	: Milli İstihbarat Teşkilatı
MİT Kanunu	: 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu
OECD	: Organization for Economic Cooperation on the Protection of Privacy
para	: paragraf
PVSK	: 2559 sayılı Polis Vazife ve Selahiyet Kanunu
R.G.	: Resmi Gazete
s.	: sayfa
SCA	: Stored Communications Act

TBMM	:Türkiye Büyük Millet Meclisi
T.C.	: Türkiye Cumhuriyeti
TCK	: 5237 sayılı Türk Ceza Kanunu
TMK	: 4721 sayılı Türk Medeni Kanunu
TDK	:Türk Dil Kurumu
TİB	:Telekomünikasyon İletişim Başkanlığı
TİB Yönetmeliği	:Telekomünikasyon İletişim Başkanlığı'nın Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik
t.y.	: basım yeri yok
USA	: United States of America
U.S.	: United States
v.	: versus
v.d	: ve devamı

GİRİŞ

1890'da ilk ortaya atıldığından beridir tartışılan özel yaşamın gizliliği,¹ 21. yüzyılda, başka bir boyutuyla hala tartışılmaya devam edilmektedir. Tartışmaya ayrı boyut kazandıran ise teknolojik gelişmelerin, kişilerin sosyal ilişkilerini ve birbirleriyle olan iletişimini değiştirmiş olmasıdır. Kendimize ait bilginin sadece etrafımızda değil, kolaylıkla bizi tanımayan insanların etrafında dahi dolaşmasının mümkün olduğu,² özel yaşam dendiği zaman artık birçoğumuzun aklına bilgisayar ve telefonun geldiği böyle bir yaşam düzeninde,³ hukukun uzun zamandır içeriğini tanımlamaya çalıştığı bir temel hak ve özgürlük olan özel yaşamın gizliliği hakkına dair tartışmaların da artarak farklılık kazanması doğal karşılanmalıdır. Nitekim bu gelişmelerin ve sosyal yaşamın karmaşıklığının, modern demokratik düzenlerde kişiyi, toplumdan soyutlanmak yerine; kişisel ihtiyaçların ve sosyal değerlerin dengelenebildiği bir toplumsal yaşamla kaynaşmanın zorunlu olduğu bir ortamda yaşamaya; devletleri de bu konuda gerekli korumayı sağlamaya teşvik ettiği görülmektedir.⁴ Temel hak ve özgürlüklere dair ilke ve kuralların, toplumsal çıkarların ve düzenin göz önünde bulundurularak ortaya konulması zorunluluğu, bu yönüyle özel yaşamın gizliliği hakkı için de kendini göstermektedir. Nitekim örneğin, her toplumda, kişiye ait veya ona dair olan bilginin güvenlik, terörle veya suçla mücadele gibi kamusal çıkarlar nedeniyle devletlerce elde edilebilmesi belirli koşullar altında normal karşılanmaktadır.⁵ Fakat tüm bunlar kişinin rahatsız olduğu müdahale kimi zaman toplumsal düzenin korunması amacıyla mevcut hukuk

¹ Samuel D. Warren, Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review*, C.IV, No:5, 1890, s. 193-220.

² Abraham L. Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy*, USA, Cornell University, 2008, s. 1-3.

³ Michael S. Hyatt, *Invasion of Privacy: How to Protect Yourself in the Digital Age*, Washington, D.C., Regnery, 2001, s. 107.

⁴ Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, USA, Cornell University, 1992, s. 20; "The Right to Privacy in Nineteenth Century America," *Harvard Law Review*, C.XCIV, No:8, Haziran 1981, s. 1892-1894.

⁵ Richard F. Hixson, *Privacy in a Public Society*, USA, Oxford University, 1987, s. 215.

kurallarından kaynaklansa da, korumanın da tekrar hukuktan istendiği gerçeğini değiştirmemektedir.⁶

Özel yaşamın gizliliğinin korunması, özellikle dijital gelişmelerin de etkisiyle bazen modern problem⁷ olarak adlandırılrsa dahi, tüm toplumlar için, sosyal yaşam farklılıklarına rağmen, ortak olan sorunların en önemlilerinden bir tanesini oluşturmaktadır. Özel yaşamın gizliliği hakkının bazen A.B.D. Anayasası'nda⁸ olduğu gibi, özel yaşamın gizliliği hakkına açıkça yer vermeden evi kutsal mekan kabul eden temel kabul üzerinden hareket eden bir anlayışla; bazen ise Türkiye'de olduğu gibi Anayasa'da açıkça düzenlenerek;⁹ aslında belki farklı düzenleme anlayışlarıyla¹⁰ ama mutlaka koruma altına alındığı görülebilir.

Özel yaşamın gizliliğine ilişkin korumayı daha önemli kılan, çatıştığı kamusal değerlerin çoğunlukla, bu yeni iletişim olanakları ve dijital bilgi yoğunluğu içinde suçların önlenmesi ve ulusal güvenliğin sağlanması gibi esaslı değerler olmasıdır. Nitekim telekomünikasyon yoluyla yapılan iletişim de, bu dijital bilgi yoğunluğunun önemli bir parçasını oluşturmaktadır. Genel itibariyle iletişimin denetlenmesi, Türk hukukunda önleme (suç öncesindeki) ve adli (suç işlenmesinden sonraki) olmak üzere iki şekilde ortaya çıkmaktadır. Bu çalışma bakımından, suç işlendikten sonra

⁶ Fred H. Cate, **The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It**, USA, First Amendment Center, 2003, s. 3, 4.

⁷ Jemima Stratford, "Striking the Balance: Privacy v Freedom of Expression under the European Convention on Human Rights", **Developing Key Privacy Rights**, Ed. by. Madeleine Colvin, USA, Hart, 2002, s. 13.

⁸ The Constitution of the United States of America, English original text of the Constitution of 1789, together with Amendments I to XXVII (Ratified 5-7-1992), Doc. No 110-50, House of Representatives, United States Government Printing Office, Washington, 2007.

⁹ 1982 Anayasası'nın 20. maddesine göre, "herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakim onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar. (...)", 1982 Anayasası'nın 20. maddesinin 4709 sayılı Kanun'la değişen 1. ve 2. fıkrası, 4709 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinin Değiştirilmesi Hakkında Kanun, Resmi Gazete No. 24556 Mükerrer, 17 Ekim 2001.

¹⁰ Sibel İncoğlu, "ABD Anayasa Hukukunda Mahremiyet Hakkı," **İnsan Hakları Yıllığı**, C. XIX-XX, 1997-1998, s. 173-176.

delil elde etme amacıyla iletişimin (adli) denetimi şeklindeki koruma tedbiri konumuz dışında kalmakta ve asıl inceleme alanımızı istihbari faaliyet kapsamında, suç işlenmesinin önlenmesi amacıyla telekomünikasyon yoluyla yapılan iletişimin denetlenmesi oluşturmaktadır.

Çalışmada, iletişimin denetlenmesine ile ilgili prensipler bakımından bir ayrım yapılmamış olsa da, konunun değerlendirilmesi bağlamında ele alınan yargısal kararlar bakımından çoğunlukla telefon veya benzer iletişim araçlarıyla gerçekleştirilen iletişime dair olaylar ele alınmıştır. Zira örneğin internet üzerinden gerçekleştirilen iletişimin denetlenmesine ilişkin hususlar açısından ayrı bir çalışma konusu oluşturacak şekilde, internet hukukunun da gözetilmesinin gerektiği söylenebilir. Kaldı ki, telekomünikasyon yoluyla gerçekleştirilen iletişim kapsamında kabul edilen iletişim hallerinin tümü bakımından, temel prensipler aynı şekilde korunmaktadır. Bunun dışında, çalışmada, hemen her bölümde, ele alınan konular açısından A.B.D. ve Avrupa yaklaşımları değerlendirilirken; genel itibarıyla A.B.D. hukukunun temel anlayışı ile tek tek Avrupa devletlerinin değil, konuyu bu devletlerin de hukuklarını etkileyecek şekilde düzenleyen Avrupa Birliği mevzuatının temel yaklaşımı göz önünde bulundurulmaktadır.

Çalışmada, esas itibarıyla telekomünikasyon yoluyla yapılan iletişimin suçların önlenmesi amacıyla denetlenmesi, anayasal haklar bakımından özel yaşamın gizliliği hakkı ekseninde değerlendirilmiştir. Bu bağlamda çalışmanın birinci bölümünü, özel yaşamın gizliliği hakkı ve bu hakkın koruduğu değerlere ilişkin ayrıntılı bir değerlendirme oluşturmaktadır. Bu bölümde öncelikle, özel yaşamın gizliliğine ilişkin belirli bir tanım vermekten öte; her biri aslında bu hakkın farklı bir yönünü ortaya koyan farklı yaklaşımlar yansıtılmıştır. Bu bölümün getirdiği yenilik, özel yaşamın gizliliği kavramının koruduğu değerler ve gördüğü işlev bağlamında, ilk kullanıldığı yargısal kararlar göz önünde bulundurulurken tartışılmasıdır. Çalışmanın ikinci bölümünde ise, telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesine dair uygulamanın ve özel yaşamın gizliliği hakkıyla olan bağlantısının daha iyi anlaşılabilmesini sağlayacak şekilde; iletişim, telekomünikasyon ve iletişimin denetimi kavramları ulusal ve uluslararası

düzenlemeler ışığında ele alınmıştır. Bu bölümde ayrıca, iletişime denetim yoluyla müdahale edilmesinin özel yaşamın gizliliği ve iletişimin gizliliği hakkı açısından yarattığı sonuçlar, Anayasa Mahkemesi kararları ile 1961 ve 1982 Anayasası dikkate alınarak değerlendirilmiştir.

Çalışmanın üçüncü bölümünün konusunu, Avrupa Birliği mevzuatında ve Türk hukukunda telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sonucu elde edilen bilginin - kişisel verinin - niteliği ve korunması oluşturmaktadır. Bu bölümde, A.B.D. hukukundaki özel yaşamın gizliliği (**privacy**) kavramının, Avrupa yaklaşımında kişisel verinin korunması (**data protection**) olarak karşımıza çıkması hususundan yola çıkarak; kişisel verilerin korunmasına dair temel ilkeler, AB mevzuatı esas alınarak incelenmiştir. Bu bölümde Kişisel Verilerin Korunması Kanunu Tasarısı da, büyük oranda temellerini oluşturan AB mevzuatıyla ilişkilendirilerek değerlendirilmiştir. Fakat bununla birlikte, A.B.D. hukukunun konuya ilişkin normatif anlayışı da, daha düzenleyici bir yaklaşıma sahip olan AB hukukuyla karşılaştırmalı bir değerlendirmeye tabi tutulmuştur.

Çalışmanın dördüncü bölümü, telekomünikasyon yoluyla yapılan iletişimin Türk hukukundaki şartları ve uygulanması, gerek teorik çerçeve çizilerek gerek uygulama yansıtılarak tartışılmaya ayrılmıştır. Burada, iletişimin denetlenmesini oluşturan iletişimin dinlenmesi, kaydedilmesi, tespiti ve sinyal bilgilerinin değerlendirilmesi işlemlerinin uygulanmasına hakim ilke ve usuller açıklanmış ve bunlar Türk hukukunun ve AİHM düzeninin özel yaşamın gizliliği hakkının sınırlandırılması durumunda kişiler için öngördüğü güvenceler çerçevesinde ele alınmıştır.

BİRİNCİ BÖLÜM

ÖZEL YAŞAMIN GİZLİLİĞİ HAKKI ve KORUDUĞU DEĞERLER

I. ÖZEL YAŞAMIN GİZLİLİĞİ

A. Genel Olarak

Önleyici denetim yoluyla müdahale edilen özel yaşamın gizliliği hakkının ne şekilde korunabileceğinden bahsetmek için, öncelikle özel yaşam hakkının kapsam itibarıyla neyi koruduğu değerlendirilmelidir. Zira özel yaşamın gizliliği bir “hak” olarak, hukuken neyin özel yaşam olarak korunduğu ya da korunması gerektiğinin kapsamıyla doğrudan ilgilidir.¹¹

1890’da Özel Yaşamın Gizliliği makalesini yazdıklarında, Samuel D. Warren ve Louis D. Brandeis Boston’da yaşayan ve birlikte çalışan iki varlıklı avukattı. Brandeis, sonrasında Supreme Court hakimlerinden biri olarak da görev yapmıştır. 1883’de Samuel Warren varlıklı bir milletvekilinin kızı olan Mabel Bayard ile evlenir ve Boston’un en zengin semtlerinden birinde yaşamaya başlar. Samuel Warren ve eşi, Boston’un cemiyet hayatının saygın ve ünlü kişileri arasında kabul edilir. Kaldı ki, magazin haberlerini yayımlayan magazin dergi ve gazetelerinde de sık sık haberleri çıkan bir aile haline gelirler. Düzenledikleri partiler ve sosyal yaşamları gazetecilerin sürekli ve neredeyse düzenli olarak haber yaptıkları konular haline gelir. Aslında Warren’ın makaleyi yazma fikrinin tüm bu haberlerden dolayı değil de; kızıyla ilgili yapılan bir haber sonucu ortaya çıktığı ifade edilir. Buna göre,

¹¹ Daniel J. Solove, Paul M. Schwartz, **Privacy, Information, and Technology**, 2. bs., USA, Wolters Klower, 2009, s. 39; David H. Holtzman, **Privacy Lost, How Technology Is Endangering Your Privacy**, USA, Jossey-Bass, 2006, s. 3, 4; Charles J. Sykes, **The End of Privacy**, New York, St. Martin’s Press, 1999, s. 17; John Curtis Raines, **Attack on Privacy**, USA, Judson Press, 1974, s. 16, 17; Whitfield Diffie, Susan Landau, **Privacy on the Line, The Politics of Wiretapping and Encryption**, USA, MIT Press, 2007, s. 141-143; Elizabeth Neill, **Rites of Privacy and the Privacy Trade: On the Limits of Protection for the Self**, London, McGill-Queen’s University, 1984, s. 13, 14.

gazeteciler son olarak, Warren'ın kızının düğünü hakkında bir haber yapar. Fakat bu yalan haber Warren'ı makaleyi yazmak üzere motive eden en önemli haber haline gelir; çünkü haberi yapılan ve düğünü olduğu iddia edilen kızı henüz on yaşında bir çocuktur.¹²

Warren ve Brandeis, bu olaylar sonrasında bu makaleyi yazdıklarında,¹³ özel yaşamın gizliliğinin ihlaline ve bu ihlale ilişkin çözüm yollarına neredeyse ilk kez işaret etmişlerdi.¹⁴ Aslında çalışmanın esası, özel yaşamın gizliliği hakkının ilk kez hukuki olarak tanınması ve fark edilmesinin tartışılıyor olmasıydı. Çalışmalarını yayımladıklarında, özel yaşamı, yetersiz bir hukuki ve olgusal temele dayandırmış olmaları dolayısıyla eleştirilmiş olsalar da,¹⁵ gerek hukukçuların gerek Amerikan Yüksek Mahkemesi'nin ilgisini çekmiş olmaları bakımından, çalışmaları oldukça önemlidir. Nitekim özel yaşama ilişkin korumanın bu çalışma sonrasında kimi zaman kaygıyla, kimi zaman ilgiyle, hukukun temel düzenleme alanına çekildiğini ve temel konulardan birini teşkil ettiğini görmekteyiz. Bu bağlamda Warren ve Brandeis'in makalesi, birçok hukukçu tarafından A.B.D'deki ve diğer hukuk anlayışlarındaki özel yaşama ilişkin hukuki düzenlemelere ışık tutan düşüncelerin neredeyse başlangıcı olarak dahi kabul edilmektedir.¹⁶ Çalışma yayımlandığında, sürecin bugünkü tartışmalara kadar geleceği çok da dikkate alınmamıştı. Daha sonra ise, çalışmanın, bugünkü tartışmalara kadar uzanan bir sürece ışık tuttuğu görülmektedir.

Özel yaşamı korurken aslında neyi koruyoruz sorusunu cevaplamak bir başka deyişle özel yaşamı tanımlamaya çalışmak, özel yaşam kavramına ilişkin dört genel

¹² Solove, Schwartz, **Privacy, Information and Technology**, s. 12; Susan Dente Ross, **Deciding Communication Law: Key Cases in Context**, New Jersey, Lawrence Eri Baum Associates, 2004, s. 15.1.

¹³ Warren, Brandeis, a.e.; Solove, Schwartz, **Privacy, Information and Technology**, s. 13-23. Ayrıca bkz.: Madeleine Schachter, **Informational and Decisional Privacy**, USA, Carolina Academic, 2003, s. 9-15.

¹⁴ Solove, Schwartz, **Privacy, Information and Technology**, s. 12; Ross, a.g.e., s. 15.1.

¹⁵ "The Right to Privacy in Nineteenth Century America," a.g.m., s. 1892.

¹⁶ Daniel J. Solove, **Understanding Privacy**, USA, Harvard University Press, 2008, s. 15; Warren Freedman, **The Right of Privacy in the Computer Age**, USA, Greenwood, 1987, s. 1, 2; Ross, a.g.e., s. 15.1; Holtzman, a.g.e., s. 95; Randall P. Bezanson, "Privacy, Personality, and Social Norms," **Case Western Reserve Law Review**, C.XLI, 1990-1991; Fred H. Cate, **The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It**, USA, First Amendment Center, 2003, s. 3, 4. (Bundan sonra The Privacy Problem olarak kullanılacaktır.)

kategoriinin analizinin yapıldığı özel yaşama ilişkin özgün bir teori olarak ortaya atılmıştır.¹⁷ Kaldı ki, özel yaşamın kapsamının ne olduğunu ve hangi değerleri içerdiğini irdelemeden, tek ve genel geçer bir tanımlama yapmak çok da mümkün gözükmemektedir.¹⁸ Özel yaşamın gizliliğini, burada, kavramın ilk kullanıldığı çalışma ve özellikle onun yansıdığı Amerikan Yüksek Mahkemesi kararları ışığında incelemeye çalışacağız.

B. Özel Yaşam Kavramına İlişkin Çeşitli Yaklaşımlar

1. Tek Başına Olabilmek Hakkı

Özel yaşamı, tek başına kalabilmek olarak tanımlayan ilk çalışma, daha önce zikredilen Warren ve Brandeis'in 1890'da yayımladıkları "**The Right to Privacy**/Özel Yaşamın Gizliliği Hakkı" isimli çalışmaydı. Yazı yayımlandığında, bugünkü tartışmaları daha şekillendireceği göz önünde bulundurulmamıştı. Zira ilk başlarda, iki akademisyenin, dedikoduyu kar amaçlı ticari bir iş haline dönüştürdüklerine inandıkları A.B.D'deki gazetecilere yönelik tepkileri sonucu ortaya çıkmış bir yazıydı.¹⁹ Aslında bu çalışmada, özel yaşamın korunması bir hak olarak adeta ilk defa ortaya atılıyordu.²⁰ Nitekim sözleşme, mülkiyet ve telif hakkına ilişkin o ana kadarki mahkeme kararlarında yargıçların uyguladıkları ve dönemin hukukunu oluşturan kurallardan (**common law**) kaynaklanan korumanın yeterli olmayacağı ve özel yaşamın ayrı bir korumayı zorunlu kıldığı vurgulanıyordu.²¹

Teknolojik gelişmeler ve medya gibi gündelik yaşamı etkileyen yeni etkenler ve modern aletler yaşamın birçok alanında yer almaktaydı ama Warren ve Brandeis'in asıl kaygısı ve katkısı, bu yeni gelişmelere mevcut kuralları ve korumaları uygulamak değil; "özel yaşamın gizliliğinin korunması" şeklinde yeni bir prensip

¹⁷ Solove, **Understanding Privacy**, s. 12.

¹⁸ Neill, **a.g.e.**, s. 13; Neil M. Richards, "Reviewing the Digital Person: Privacy and Technology in the Information Age by Daniel J. Solove," **Georgetown Law Journal**, C.XCIV, Nisan 2006, s. 20.

¹⁹ Warren, Brandeis, **a.e.**; Serge Gutwirth, **Privacy and the Information Age**, Çev. Raf Casert, USA, Rowman&Littlefield, 2002, s. 5.

²⁰ Fred H. Cate, **The Privacy Problem**, s. 3; Bennett, **a.g.e.**, s. 25.

²¹ Robert C. Post, "Rereading Warren and Brandeis: Privacy, Property, and Appropriation," **Case Western Reserve Law Review**, C.XLI, 1990-1991, s. 647-653.

yaratmaktı. Kaldı ki, henüz sadece fotoğraf çekmenin popüler olduğu bir dönemde yazılmış olmasına rağmen, teknolojiye yeni teknolojilerin, özel yaşama karşı potansiyel bir tehdit oluşturduğu vurgulanıyor; mahremiyete ilişkin uygunluk sınırlarının medya tarafından gazeteler yoluyla dahi fazlasıyla aşıldığı ifade ediliyordu. İşte bu noktada, Warren ve Brandeis'in özel yaşamı tek başına olabilmek hakkı olarak açıklayan yeni anlayışı bir özellik arz etmekteydi.²²

Konuya belki de kişinin düşüncelerine, yazdıklarına, ifadelerine bir başka anlatımla yaşamına bu müdahaleye, mülkiyet hakkının ihlaline, bir kişinin malını izinsiz kullanmaya veya hırsızlığa ilişkin yasal korumalardan yararlanılarak da yaklaşılabilirdi. Fakat bu yeni anlayış, kişisel yaşama müdahaleyi kişinin tek başına olabilmek şeklinde ayrı bir hakkı olması gerektiğiyle açıklamakta ve ancak bu şekilde tam bir korumanın sağlanabileceğini kabul etmektedir. Çünkü günlük yaşamın o dönemin neredeyse sadece fotoğraf çekmeyle sınırlı olan teknolojik gelişmeleri karşısında dahi, bir kişinin özel yaşamının hiçbir fiziksel müdahalede bulunmadan ihlal edilebileceği göz önünde bulunduruluyordu.²³ Bu bağlamda, güvenin ve sözleşmenin ihlaline dair mevcut kurallar çerçevesinde sağlanamayacak korumanın, bu şekilde kişiliği merkeze koyan “kişinin tek başına olabilmek hakkı” ile sağlanabileceği ifade ediliyordu.²⁴

En geniş anlamıyla bu anlayışta özel yaşamın gizliliği, kişinin duygu ve düşüncelerini başkalarıyla hangi kapsamda paylaşmak istediğiyle ilgilidir. Bu bağlamda kişiye yönelik duygusal zarar; bedensel zarar ve hakaret ile aynı seviyede ve hatta kişiliğe yönelik olarak daha zararlı görülmüş ve fakat ayrı bir korumayı gerekli kıldığı da vurgulanmıştır. Nitekim Warren ve Brandeis'in bir makalesiyle ortaya atılan ve kişinin tek başına olabilmek hakkı çerçevesinde ifade edilen özel yaşamının gizliliği hakkı ve korunması, sadece teorik çerçevede kalan kavramsal bir

²² Amita Etzioni, **The Limits of Privacy**, USA, Basic Books, 1999, s. 190.

²³ Cate, **The Privacy Problem**, s. 3, 4.

²⁴ Andrew T. Kenyon, Megan Richardson, “New Dimensions in Privacy: Communications Technologies, Media Practices and Law”, **New Dimensions in Privacy Law: International and Comparative Perspectives**, Ed. by. Andrew T. Kenyon, Megan Richardson, UK, Cambridge University, 2006, s. 4; Etzioni, **a.g.e.**, s. 190.

tartışma olmaktan çıkmış, Amerikan Yüksek Mahkemesi'nin ve anayasa hukukunun özel yaşama ilişkin yaklaşımını da şekillendirmiştir.²⁵

Brandeis'in, çalışmanın yayımlanmasından yaklaşık kırk yıl sonra, 1928'de, Olmstead v. U.S. kararında,²⁶ bu sefer yargıç olarak kaleme aldığı karşı oy gerekçesinde, kişinin özel yaşamının gizliliğinin/tek başına olabilmek hakkının uygar bir kişiyi en anlamlı kılan ve onun en kapsamlı haklarından biri olduğunu bir kez daha vurguladığı görülür. Mahkeme bu kararında, A.B.D. Anayasası'nın²⁷ arama ve el koymaya ilişkin hükmünün (**Fourth Amendment**) ihlal edilmediğini çünkü davacıların şahsi eşyalarının veya belgelerinin arama amacıyla veya evlerine fiziksel olarak girerek aranmadığını ve el konulmadığını ileri sürmüştür. Davacıların evlerine veya iş yerlerine girmeden, sadece dinleme yönteminin kullanılmasının ise A.B.D. Anayasası'nı ihlal etmediği ve arama veya el konulmaya ilişkin bir korumadan yararlanamayacağı ifade edilmiştir.²⁸ Mahkemenin bu kararına karşı oy bildiren Brandeis ise gerekçesinde, kişinin sahip olduğu belge veya yazı gibi maddesel şeylere ilişkin ihlalin, anayasanın koruduğu kişi yaşamının sadece bir bölümünü oluşturduğunu ifade etmiştir. Brandeis'e göre, anayasayı hazırlayanlar, kişinin duygu ve düşünceleri, hissettikleri ve bu hislerini yaşama geçirmesi bağlamında tam bir özgürlük içinde olduğu anlayışıyla anayasayı şekillendirmişlerdir. Buna göre, görevlileri aracılığıyla kişilerin telefon konuşmalarını dinleten devletin ise bunun tam aksine bir anlayış benimsediğini ve bu bağlamda bir eve girmeden dahi yapılan dinlemenin Anayasa'nın (**Fourth Amendment**) ihlali sayılarak, bu işlem karşısında bireye tam korumanın sağlanması gerektiği savunulmuştur.²⁹

²⁵ Solove, **Understanding Privacy**, s. 17; Schachter, **a.g.e.**, s. 15-20.

²⁶ Olmstead v. United States, 277 U.S. 438 (1928); Cate, **The Privacy Problem**, s. 3.

²⁷ The Constitution of the United States of America, English original text of the Constitution of 1789, together with Amendments I to XXVII (Ratified 5-7-1992), Doc. No 110-50, House of Representatives, United States Government Printing Office, Washington, 2007.

²⁸ Olmstead v. United States, 277 U.S. 438 (1928). Ayrıca bkz.: Robert Gellman, "Does Privacy Law Work", **Privacy and the Representation Technology and Privacy: The New Landscape**, Ed. by. Philip E. Agre, Marc Rotenberg, London, England, The MIT Press, 1997, s. 203; F. Lawrence Street, Mark P. Grant, **Law of the Internet**, USA, Lexis Law, 2000, s. 116; Diffie, Landau, **a.g.e.**, s. 149.

²⁹ Olmstead v. United States, 277 U.S. 438 (1928), Brandeis dissenting.

1920’li yıllarda karşı oy olarak kalan Brandeis’in özel yaşamın, tek başına olabilmek imkanı şeklinde, ayrı bir hak olarak korunması gerektiği anlayışının 1960’lara gelindiğinde, yaklaşık üç yüz kararda farklı şekillerde yer bulduğu görülür.³⁰ Nitekim, Supreme Court’un halen geçerliliğini ve uygulanabilirliğini koruyan 1967’deki Katz v. U.S. kararında, 1920’de azınlık görüşü kalan tek başına olabilmek anlayışının, hakim anlayış olarak benimsendiği görülür. Herkesin kullanımına açık bir telefon kulübesine yerleştirilen cihazla yapılan dinleme, konuşmanın yapıldığı yere fiziksel olarak girilip dinleme yapılmasa dahi, Anayasa’yı ihlal olarak kabul edilir.³¹ O kadar ki Mahkeme, bu kararında, Anayasa’nın koruduğu özel yaşamın gizliliği hakkının, aslında kişinin tek başına kalabilmek hakkını ifade ettiğini ve “tek başına kalabilmek” hakkını bir formülasyon olarak benimsediğini açıkça vurgular. Bir kişinin gizlice dinlenmesinin kişiliğine, açıkça ve izinle ev veya işyerinin aranmasından daha az zarar vermeyeceği de bu formülasyonun benimsenmesindeki başlıca etkenlerden biri olarak gösterilmiştir.³²

Özel yaşamın gizliliğinin korunmasını, kişinin duygu ve düşüncelerini hangi kapsamda paylaşacağını kendisinin belirlemesini de içerecek şekilde ve fakat tek başına olabilmek hakkı bağlamında ifade eden en iyi açıklamalardan biri yargıç Douglas’ın, Doe v. Bolton kararında yazdığı gerekçesinde görülür: Tek başına olabilmek hakkı, kişinin kendi ilişkilerini kendi isteği doğrultusunda kendisinin tasarlaması olanağını kapsar. Sosyal yaşama yönelik zarar verici davranışlar bakımından ise, her birey en doğru olduğunu düşündüğünü ve onu en memnun edeni seçerek yaşamını şekillendirebilmesi açısından, tek başına, tek belirleyen olarak bırakılmıştır.³³ Bu bağlamda, özel yaşamın gizliliği hakkı, “tek başına olabilmek”

³⁰ William Prosser, “Privacy,” *Cal. L. Rev.*, C. XLVIII, No:3, 1960, s. 388, 389.

³¹ Katz v. United States, 389 U.S. 347 (1967). Ayrıca bkz.: Philip E. Agre, “Beyond the Mirror World: Privacy and the Representational Practices of Computing”, **Privacy and the Representation Technology and Privacy: The New Landscape**, Ed. by. Philip E. Agre, Marc Rotenberg, London, England, The MIT Press, 1997, s. 7; Janlori Goldman, “Privacy and Individual Empowerment in the Interactive Age”, **Privacy: New Risks and Opportunities**, Ed. by. Yves Poulet, Cecile de Terwangne, Paul Turner, Belgique, Centre de Recherches Informatique et Droit, 1997, s. 70.

³² Katz v. United States, 389 U.S. 347 (1967).

³³ Doe v. Bolton, 410 U.S. 179 (1973). Supreme Court’un 1960’lı yılların sonuna kadar özel yaşamın gizliliği hakkının ihlalini oluşturabilecek müdahalelere ilişkin genel yaklaşımıyla ilgili ayrıntılı bilgi için bkz.: Susan Freiwald, “Online Surveillance: Remembering the Lessons of the Wiretap Act,” *Alabama Law Review*, C.LVI, 2004-2005, s. 22.

bağlamında bir kişiye ait, yaşamını kendince en iyi bulduğu düşünce doğrultusunda şekillendirebilmesi, onu memnun kılan davranışı yapabilmesi ve onu memnun kılan yere gidebilmesi üzerine kurulu bir ayrıcalık olarak kabul edilebilir.³⁴

Özel yaşamın gizliliğinin, kişinin yaşamında kararlarını ve davranışlarını tek başına oluşturabilmesi olarak kabul edilmesinin,³⁵ özel yaşamın hiçbir müdahaleyi içermeyecek bir şey olduğu yönündeki genel algılamayı da yansıtmadığı söylenebilir. Buna göre, Warren ve Brandeis'in özel yaşamın gizliliğinin korunmasına yönelik altı sınırlama belirlediği görülür: (i) Özel yaşamın gizliliği, kamunun çıkarlarını ilgilendiren belgelerin yayımlanmasını engellemez. (ii) Özel yaşamın gizliliği, yargı organlarında veya kamusal bir makamda, bir konuyla ilgili gerekli görüşmelerin yapılmasını veya bunların gerekli ise yayımlanmasını yasaklamaz. (iii) Konuşma özgürlüğü (**free speech**) çerçevesinde gerçekleştirilen sözlü iletişim, kendiliğinden özel yaşamın gizliliğinin ihlali doğurmayacaktır. (iv) İlgilinin rızasıyla veya kendi tarafından yapılan yayınlar, özel yaşamın gizliliğinin ihlali konuyu oluşturmayacaktır. (v) Özel yaşama ilişkin sızdırılan veya elde edilen bir bilginin, gerçek olması veya gerçeğe ulaşmak için gerekli tüm çabanın gösterilmiş olması ise, özel yaşamın gizliliğinin ihlali savunmasını neredeyse etkisiz bırakabilecektir. (vi) Son olarak da, herhangi bir kasıt gösterilmesi zorunluluğunun, özel yaşamın gizliliğinin ihlali edildiğinin ileri sürülebilmesi için gerekli görülemeyeceği ifade edilmiştir.³⁶

Warren ve Brandeis kişinin tek başına kalabilmek hakkının ihlali durumunda başvurulabilecek çözüm yolları bakımından, hakarete ilişkin ceza hukuku koruması ve mülkiyet hakkına ilişkin özel hukuk koruması gibi mevcut hukuki korumaların tamamen dışlanması yerine; onlardan da yararlanılarak ve fakat ayrı ve tam bir

³⁴ Jacqueline Klosek, **Data Privacy in the Information Age**, London, Quorum, 2000, s. 127, 128; Warren, Brandeis, **a.e.**; Solove, Schwartz, **Privacy, Information and Technology**, s. 13-23; Schachter, **a.g.e.**, s. 9-15; Goldman, **a.g.m.**, s. 67.

³⁵ Diffie, Landau, **a.g.e.**, s. 142.

³⁶ Warren, Brandeis, **a.e.**; Solove, Schwartz, **Privacy, Information and Technology**, s. 13-23; Schachter, **a.g.e.**, s. 9-15.

koruma anlayışıyla hareket edilmesi gerektiğini savunmuşlardır.³⁷ Bu açıdan, kişinin tek başına kalabilmek hakkına - özel yaşamının gizliliğine - müdahale edilmesi halinde, özel bir zarar mevcut olmasa da, esaslı bir tazminatın veya ceza hukuku yaptırımlarına ek olarak bir yasaklamanın uygulanması bu anlayış çerçevesinde göz önünde bulundurulmuş çözümler olmuştur.³⁸ Böylece kişiye yönelik zarar verici herhangi bir fiil veya haksızlık da, özel yaşamın gizliliği hakkının ihlali olarak nitelendirilebilecektir ve korunması sadece ceza hukukuyla sınırlanmış olmayacaktır.

Yayımlandığı ve yansıdığı mahkeme kararlarının yazıldığı dönem itibariyle yeni bir bakış açısıyla, kişinin korunmaya yönelik yaşamının sadece sahip olduğu maddesel şeylerden ibaret olmadığı, kişinin tek kalesinin evi olmadığı ve yeni bir hak yaratma anlayışıyla sunulan “tek başına olabilmek hakkı” yaklaşımının özel yaşamın her alanına ilişkin sorunları aydınlatmadığı ileri sürülebilir. Özellikle nelerin kişinin tek başına olacağı konuları oluşturacağı belirsizlik yaratmaya müsaittir. Nitekim bu yaklaşıma yönelik eleştirilerin başlıca iki noktada toplandığı söylenebilir. Bunlardan biri, Warren ve Brandeis’in özel yaşamı kişinin tek başına kalması olarak tanımlamalarının çok geniş ve fakat bir o kadar da belirsiz olduğu yönündedir.³⁹ Diğeri ise, Warren ve Brandeis’in bu anlayışı ileri sürerken bir özel yaşamın gizliliği tarifi yapmadıkları; onun yerine sadece özel yaşama ilişkin ileri bir konsept ileri sürdükleri yönündedir. Nitekim ‘kişiliğe’ ve özel alana müdahale bir ihlal olarak değerlendirilmekte⁴⁰ ve fakat Warren ve Brandeis’in yaklaşımında, bu özel alanın ne olduğu tam bir açıklığa kavuşmamaktadır.⁴¹

Bununla birlikte, özel yaşam tek başına bırakılma şeklinde bir ayrıcalık olarak ifade edilirse, başka bir kişiye yönelik her türlü davranış aynı kapsamda değerlendirilebilecektir.⁴² Bu bağlamda, burnuna yumruk atılmış bir kişi de evine

³⁷ Warren, Brandeis, **a.e.**; Solove, Schwartz, **Privacy, Information and Technology**, s. 13-23; Schachter, **a.g.e.**, s. 9-15.

³⁸ Warren, Brandeis, **a.e.**

³⁹ Kenyon, Richardson, **a.g.m.**, s. 4.

⁴⁰ Bennett, **a.g.e.**, s. 25.

⁴¹ Solove, **Understanding Privacy**, s. 18.

⁴² Bu görüş bakımından özellikle, özel yaşamın gizliliğini tartışırken, konseptin, mevcut koşulların da önemi olduğunu ifade eden anlayış için bkz.: Sykes, **a.g.e.**, s. 17.

kamera yerleştirilmiş bir kişi de; kendisinin yönlendirmediği zarar verici bu davranışı, ‘aynı özel yaşam’ kavramı içerisinde nitelendirebilecektir.⁴³ Hakikaten tek başına bırakma anlayışı bu yönüyle fazlasıyla soyut ve geniş bir tanımlama olarak değerlendirilebilir.⁴⁴ Fakat kanımızca bu eleştirilere de, bu yaklaşımın kapsama ilişkin yetersizliği yanında bir diğer yönüyle de, özellikle kişinin yaşama dair tek başına karar alabilme ve davranabilme algısını da kabul ederek, özel yaşama ilişkin yasal korumayı mümkün kılabileceği ve hatta genişletebileceği vurgulanarak karşılık verilebilir.

Kişiyi tek başına bırakma anlayışının asıl eksikliği, dönemin etkisiyle ve Mahkeme’nin önüne gelen mevcut olaylara yoğunlaşmanın kaygısıyla, neredeyse sadece devlet organlarının müdahalelerinin yarattığı özel yaşamın gizliliği ihlaline odaklanmasındadır.⁴⁵ Zira kişiyi tek başına bırakma, bu anlayışta daha çok devletin müdahale etmemesi ve bu alana karışmaması üzerine yoğunlaşmıştır. Fakat tam ve kapsamlı bir özel yaşamın gizliliği anlayışı, kişinin hukuksal düzenin getirdiği zorunluluklar veya başka bireylerin gerçekleştireceği özel yaşam ihlalleri karşısında da özgür olmasını ve kendi seçimlerini yapabilmesini de gerekli kılar. Nitekim özel yaşam başkalarının veya özellikle devletin bize bıraktığı alandan daha geniş olmalıdır; çünkü özel yaşam aynı zamanda bir reddediş, özgür karar alış, başkalarının değil kendimizin belirlediği kimlikleri benimseyiş olanağı sağlıyor ve tek başına kalacağı alanı da kişinin kendisinin belirlemesini mümkün kılıyorsa anlamlıdır.⁴⁶

Tüm eleştirilere rağmen, özellikle Anglo Sakson hukuku bakımından, Warren ve Brandeis’in özel yaşamı tek başına olabilmek hakkı bağlamında ele alan yaklaşımının, ortaya atıldığı dönem ve daha sonra mahkeme kararlarında da ağırlıklı olarak yer verildiği dikkate alındığında; geliştirilmeye açık yeni bir bakış açısı

⁴³ Solove, **Understanding Privacy**, s. 18.

⁴⁴ Warren ve Brandeis’in tek başına bırakma anlayışına yönelik diğer eleştirilerle ilgili ayrıntılı bilgi için bkz.: “The Right to Privacy in Nineteenth Century America,” **a.g.m.**, s. 1891-1893.

⁴⁵ Ruth Gavison, “Privacy and the Limits of Law,” **The Yale Law Journal**, C.LXXXIX, No: 3, 1980, s. 438, 439.

⁴⁶ Anita L. Allen, “Coercing Privacy,” **William and Mary Law Review**, C. XL.III, Mart 1999, s. 723; Solove, Schwartz, **Privacy, Information, and Technology**, s. 43; Fred H. Cate, **Privacy in the Information Age**, Washington, DC, Brookings Institution, 1997, s. 25, 26.

kazandırdığı ifade edilebilir. Zira kimi zaman özel yaşama ilişkin ayrı bir yaklaşım olarak ifade edilen,⁴⁷ fakat kanımızca Warren ve Brandeis'in kişinin yaşamında kararlarını ve davranışlarını tek başına oluşturabilmesi olarak gördükleri bu anlayış üzerine kurulan “kişiliğin (**personhood**) korunması” anlayışının da ortaya çıkmasını sağlar. Nitekim Warren ve Brandeis kişinin yaşamına dair seçim yapan, tek belirleyen olmasındaki temel unsuru kişiliğinin ihlal edilmemesi/zarar görmemesi olarak belirler ve kişiliğin bütünlüğünden yola çıkar. Freund korunması gereken bir şey olarak kişiliği ilk defa tanımlarken; bunu kişinin sadece kendisine indirgenebilecek nitelikleri olarak kabul eder.⁴⁸ Fakat gerek kişilik gerek bu ifadesinde içermek istediği bireysellik, bağımsızlık ve gizlilik kavramları kapsamı belirlenmemiş ucu açık kavramlar olarak bırakıldığından, aslında, Warren ve Brandeis'in ortaya attığı zaman çok da ayrıntılandıramadığı “tek başına olabilmek” kavramı bu unsurları da içeren, daha bütünlükçü bir bakış açısı ortaya koyar.

Kişiliğin korunmasını tek başına olabilmek anlayışının içinde düşününlerin de,⁴⁹ ikisini ayrı yaklaşım olarak ele alan görüşün de,⁵⁰ özel yaşamın gizliliğinin korunmasını, kişinin kişiliğini oluşturma ve onu o şekilde devam ettirmedeki temel yararını koruduğu ve bu kişiliği zayıflatacak etkenlere karşı da koruma sağladığı düşüncesi üzerine dayandığı görülür.⁵¹ Kısacası üzerinde durulan temel soru özel yaşamın ‘kişinin’ hangi temel yararına hizmet ettiğidir.⁵² Aynı zamanda şu da görülebilir ki, ayrı bir yaklaşım olarak değerlendirilmek yerine; kişilik ve kişiliğin bütünlüğü kavramı, ileride incelenecek diğer bütün yaklaşımlar açıklanırken de yararlanılabilecek bir unsur olarak karşımıza çıkacaktır. Bu yönüyle de, özel yaşamın gizliliğini korumanın, hangi davranışların yapılmasına karşı bir koruma sağlayacağını tartışırken kullanılabilecek daha anlamlı ve tutarlı bir değerlendirme sunmuş olur. Örneğin, özel yaşamın neden önemli olduğu, kişinin hangi yönüne

⁴⁷ Solove, **Understanding Privacy**, s. 29-30.

⁴⁸ Paul Freund, **Address at the American Law Institute, 52nd Annual Meeting**, Aktaran J. Braxton Craven, Jr., “Personhood: The Right to be Let Alone,” **Duke L. J.**, C.1976, 1976, s. 702-703.

⁴⁹ Craven, **a.g.m.**, s. 702.

⁵⁰ Solove, **Understanding Privacy**, s. 30.

⁵¹ Aaron J. Rappaport, “Beyond Personhood and Autonomy: Moral Theory and the Premises of Privacy,” **Utah Law Review**, C.II, 2001, s.453-454; Edward Blousten, **Privacy as an Aspect of Human Dignity**, Aktaran Solove, **Understanding Privacy**, s. 30.

⁵² Rappaport, **a.g.m.**, s. 452-454, Solove, **Understanding Privacy**, s. 30.

sınırlı ulaşılacağı veya hangi bilgiyi kontrol etmemiz gerektiği - bu soruların her biriyle aşağıda incelenecek olan farklı bir anlayışın ilgilendiği dikkate alınır - açıklanırken de, kişiliğin bütünlüğü kavramından yararlanılabilir ve özel yaşamın aslında kişiye dair neyi koruduğu açıklanabilir.

Kişinin tek başına, tek belirleyen olarak kişiliğinin korunması anlamında özel yaşamın gizliliğini açıklayan Warren ve Brandeis ile başlayan ve gelişen bu yaklaşımda, özel yaşamın gizliliğinin korunmasının, kişiliğe aynı zamanda saygıyı da ifade ettiği ileri sürülür. Bu saygı, kimi zaman kişiye kendisiyle ilgili 'seçim yapan' biri olarak duyulan saygı bağlamında görülmektedir. Bu bakış açısının özel yaşamın gizliliğine etkisi bakımından bir anlamı vardır. Nitekim bu yönüyle kişiye saygı, aslında kişinin kendi iradesiyle adeta bir kuruluş yaratır gibi kendi kişiliğini ve kişisel bütünlüğünü yaratma yönünde iradesini kullanırken, izlenerek, dinlenerek veya başka yollarla denetime tabi olursa, bu iradesine zarar verilebilecek, zayıflatılabilecek ve rahatsız edilebilecek biri haline gelebilecek bir kişi olarak da saygı duyulmasını ifade eder.⁵³ Bu saygı, bu şekillerde veya daha da sınırlı olarak başka birinin denetimine konu olmuş birinin, gözetlenen (**observed**) olarak, seçim yapma olasılığının sınırlanabileceği niteliğinden kaynaklanır.⁵⁴

2. Kişisel Bilgi Üzerindeki Kontrol İmkanı

Özel yaşamı, kişinin, kendisine ait, onu belirlenebilir kılan bilgisi üzerindeki kontrolü olarak gören yaklaşım,⁵⁵ başkalarının bize ilişkin sahip olduğu bilgilerin varlığının değil; aksine bizim kendimize ait bilginin üzerindeki kontrolün belirleyici

⁵³ Paul Schwartz, "Privacy and Democracy in Cyberspace," **Vand. L. Rev.**, C. LII, 1999, s. 1653-1658; Bennett, **a.g.e.**, s. 19-21.

⁵⁴ Solove, **Understanding Privacy**, s. 30.

⁵⁵ Randall P. Bezanson, "The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990," **California Law Review**, C.LXXX, Ekim 1992 (Bundan sonra The Right to Privacy Revisited olarak kullanılacaktır.); Solove, Schwartz, **Privacy, Information, and Technology**, s. 44, 45; Solove, **Understanding Privacy**, s. 24-29; Cate, **Privacy in the Information Age**, s. 21; Bennett, **a.g.e.**, s. 25; Richard S. Murphy, "Property Rights in Personal Information: An Economic Defense of Privacy," **The Georgetown Law Journal**, C.LXXXIV, 1995-1996; Goldman, **a.g.m.**, s. 67.

olduğunu ifade eder.⁵⁶ Buna göre özel yaşamın gizliliği, kişinin başkalarıyla nerede ve ne zaman iletişim kuracağı ve hangi kapsamda bilgi alacağı veya aktaracağını belirlemeyi talep edebilmesidir.⁵⁷

Özel yaşam söz konusu olduğunda, bir “koruma”nın da bu bağlamda göz önünde bulundurulması ve tartışılması gerektiğini vurgulaması, bu anlayışın diğerlerinden en belirgin farkını oluşturur. Çünkü özel yaşamın gizliliğinin, kişinin hangi bilginin kendisine ait olduğu ve ne kadar kontrol kurmak istediğine ilişkin sahip olduğu bir ayrıcalıktan ibaret bir şey olmadığı kabul edilir ve iki yönlü içiçe geçmiş bir algılamayla açıklanır. Bunlar, toplumun neyin korunmasını uygun gördüğü ve kişinin kendisine ait hangi bilgiyi başkalarına ulaşılabılır kılma şeklindeki kişisel hareket alanıdır.⁵⁸

Bu yaklaşımın, her ne kadar koruma kavramının özel yaşam kavramıyla birlikte düşünülmesine dair adeta ilk çağrışımları yapan bir görüş olduğu görülse de, üzerinde kontrol sağlanacak olan bilginin ne tür bir bilgi olursa, kişisel bilgi olacağı ve üzerinde kontrol imkanı sağlayacağı konusunda belirleyici ve net bir değerlendirme yapamadığı görülmektedir.⁵⁹ Bu yönüyle hem geniş hem de dar bir değerlendirmeye sahip bir anlayış olması nedeniyle eleştirilebilir. Nitekim bu anlayış çerçevesinde özel yaşamın gizliliğini kontrol bağlamında yorumlayan görüşlerden bir tanesi, son derece geniş ve ucu açık bir şekilde, kişinin onu kimin duyacağı, ona kimin dokunacağı ve hatta kiminle aynı ortamda bulunacağı gibi belirlemelerin dahi özel yaşamın özünü oluşturduğunu ileri sürmektedir.⁶⁰ Diğer bir görüş ise, kişiye ait, onu belirli kılan bilginin üzerindeki kontrol imkanının bu anlayışı şekillendirdiğini

⁵⁶ Solove, Schwartz, **Privacy, Information, and Technology**, s. 44, 45; Solove, **Understanding Privacy**, s. 24, 25; Allen, **Coercing Privacy, a.e.**

⁵⁷ Alan Westin, **Privacy and Freedom**, Aktaran Solove, Schwartz, **Privacy, Information, and Technology**, s. 41.

⁵⁸ Solove, **Understanding Privacy**, s. 25; Solove, Schwartz, **Privacy, Information, and Technology**, s. 44, 45.

⁵⁹ Bu konuda, konuşma özgürlüğü de belirli bir bilgi üzerinde kontrol imkanı sağladığından dolayı, konuşma özgürlüğü ile kontrol bağlamında anlaşılan özel yaşamın gizliliği hakkının çatışabileceğine dair görüş için bkz.: Eric Barendt, “Privacy and Freedom of Speech”, **New Dimensions in Privacy Law: International and Comparative Perspectives**, Ed. by. Andrew T. Kenyon, Megan Richardson, UK, Cambridge University, 2006, s. 11.

⁶⁰ Solove, **Understanding Privacy**, s. 25.

kabul etmektedir. Görülüyor ki, bu anlayış bağlamında kişisel bilgi olsun veya olmasın, üzerinde kontrol sağlayabileceğimiz pek çok şey olduğu noktasından bir tanımlama yapılabilir. Böylece Warren ve Brandeis'in anlayışındaki 'tek başına kaldığımız alan'a ilişkin belirsizliğin bir benzerinin bu anlayışta da, bu defa 'kontrol'den ne anlaşıldığı noktasında varolduğu söylenebilir.

Tüm bu belirsizlikler karşısında, kişinin kendi kişiliğine dair karar almaya ilişkin düşüncesi üzerinde mülkiyet hakkı olduğu görüşü dahi ileri sürülmüştür.⁶¹ Gerçi bu yöndeki kabulün temellerini, John Locke'un herkesin 'kendisi' üzerinde (fikri) mülkiyet hakkı olduğu görüşünde bulduğu da söylenebilir. Zira kişinin sadece kendisinin kişiliği ve emeği üzerinde bir hakkı olduğunu belirten Locke; bir kişiyi diğerlerinden ayıran özelliğinin, kendi emeğiyle bütünleşince ortaya kendisine ait bir şey çıkarması olduğunu ifade eder.⁶² Özel yaşamın gizliliği bağlamında, birbiriyle karışıp bütünleşen bu iki şeyin kişinin düşünceleri ve kendine özgü kişiliği olduğu söylenebilir. Locke'un görüşüne kadar uzanan bu anlayışta, asıl korunan 'kişiye ait' olan, ondan ortaya çıkan düşünce ve bilgidir. Bu açıdan, bu bilgi de kişiliğin bir parçası ve uzantısı olarak kabul edilir. Kişinin kendi duygularının, benliğinin ve özgeçmişinin, sonunda da kendisine ait bu kişisel bilgiyi yarattığı vurgulanır. Şu da unutulmamalıdır ki, mülkiyet hakkı anlayışıyla paralellik kurularak açıklanan bu yaklaşımın da kendi içinde birtakım sorunlara neden olacağı görülebilir. Nitekim en yalın yaklaşımla, aslında yaşam ilişkisi kurmamızı sağlayacak bilginin,⁶³ bu yönde korunma ve üzerinde kontrol imkanı sağlayacak bilgi olduğu görülebilir. Zira başka kişilerle ilişki kurarken kullandığımız bilgi çoğunlukla onlarla olan iletişimle de şekillenmekte ve bu da hangi bilgi üzerinde aitlik ileri sürüleceği belirsizliğini de beraberinde getirmektedir.⁶⁴ Örneğin bir kişinin eşiyle olan ilişkisi dahilinde ileri sürülen, eşinin alkolik olduğu bilgisi onun kişiliğine zarar vermesi bakımından üzerinde kontrol sağlayabileceği kişisel bir bilgi midir yoksa kişinin yaşam

⁶¹ Westin, a.e.

⁶² John Locke, **Second Treatise on Government**, 1690, para 26, 27, aktaran Solove, **Understanding Privacy**, s. 26. Ayrıca bkz.: C M Millen, **The Right to Privacy and its Natural Law Foundations in the Constitutions of the United States and Ireland, Ireland**, Blackhall, 1999, s. 91.

⁶³ Charled Fried, "Privacy," **Yale L. J.**, C.LXXVII, 1967-1968, s. 484.

⁶⁴ Jerry Kang, "Information Privacy in Cyberspace Transactions," **Stanford Law Review**, C.L, 1997-1998, s. 1202-1212.

ilişkisinden kaynaklanmış ve kontrol iddiasında bulunamayacağı genel bir bilgi midir?⁶⁵

Sadece ‘kontrol’ün tanımlanması bir zorluk teşkil etmemekte; aynı zamanda kişisel bilgi üzerindeki kontrol anlayışı da oldukça ucu açık kalmaktadır. Kişisel bilgi üzerindeki kontrol, daha önce ifade edildiği gibi bazen başkalarıyla ilişki kurarken kullanılan bilgi olarak ortaya çıktığı için, başka kişi veya gruplara ait bilgi üzerinde kontrolü de mümkün kılma gibi sakıncalar veya belirsizlikler doğurabilir. Bu nedenle, bilgi üzerindeki kontrol anlayışını, kişinin arkadaşlık, sevgi ve güven gibi yaşamını devam ettirmesi için gerekli ilişkilere dair ve doğrudan kendisiyle ilgili bilgi üzerinde kontrol hakkı ile sınırlamak mümkün görülebilir.⁶⁶

Görülüyor ki, bu yönleriyle kişisel bilgi üzerindeki kontrol anlayışı geniş, ama tercihi adeta kişiye bırakması yönüyle bir o kadar da dar bir yaklaşım olarak karşımıza çıkmaktadır. Nitekim bu anlayış, özel yaşamın gizliliğini sadece bilgidan ibaret kabul etmesi yönüyle de eleştirilmiştir.⁶⁷ Hakikaten bir kişinin özel yaşamının gizliliğinin, başka biriyle kendisine ait yeni bir bilgi paylaşmasa da ihlal edilebileceği açıktır. Bir kişinin yapılan yayın veya reklamlarla istemediği bir görüşü benimsemek zorunda bırakılması veya iletişiminin dinlenerek kendi görüşünü paylaşamayacak duruma getirilmesi de, özel yaşamının gizliliğine müdahale olarak nitelendirilebilir. Bu bağlamda, özellikle özel yaşamın gizliliğini, kişinin kendi seçtiği düşünce ve davranışlar doğrultusunda yaşamını şekillendirebilmesi ve böylece kendi belirlediği alanda tek başına bırakılması olarak gören anlayışı savunanlar, kontrol anlayışını, ‘özel’ olarak kabul ettiğimiz yaşamı anlamlı kılan birçok alanı görmezden gelmesi nedeniyle eksik bulmaktadırlar.⁶⁸

⁶⁵ A.B.D’de Haynes v. Alfred A. Knopf, Inc davasında, yargıç Posner, bir kişinin eski eşinin alkolik olduğu, bencil ve sorumsuz davranışlar içinde olduğunu içeren bir kitabın yayımlanmasının özel yaşamın gizliliğinin ihlalini oluşturmayacağını; böyle bir davranışla gerçeğin ifşası şeklinde gerçekleşen, kamuyu ilgilendiren bir konunun kaleme alındığını ifade etmiştir, Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222 (7th Circuit 1993).

⁶⁶ Solove, Schwartz, **Privacy, Information, and Technology**, s. 44, 45; Solove, **Understanding Privacy**, s. 27-29; Cate, **Privacy in the Information Age**, s. 21; Bennett, **a.g.e.**, s. 25.

⁶⁷ Solove, **Understanding Privacy**, s. 29.

⁶⁸ Anita Allen, “Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm,” **Conn L. Rev.** C.XXXII, 1999-2000, s. 865-869.

Kaldı ki, kontrol anlayışının, gerek sahip olduğu bilgiye dair seçimler yapabilmesinde gerek bilginin sosyal yaşamda iletişimi sağlayacak şekilde düzenlenmesinde, bir başka ifadeyle neredeyse her durumda kişinin bir kontrole sahip olduğu varsayımı üzerine kurulu olduğu görülebilir. Oysa yaşamsal ilişkinin birçok boyutunda kişinin kendi belirlemeleri dahi, kişisel bilginin sosyal ortamda şekillenmesiyle ortaya çıkabilir. Zira özel yaşam, sadece bir kişisel kontrol mekanizması olarak karşımıza çıkmaz; sosyal yönü ve özellikle yaşamsal ilişkiler de dikkate alınarak sahip olunan bilgilerin kullanılması yönü de bulunmaktadır.⁶⁹ Fakat bu yönüyle dahi, kontrol anlayışı, John Stuart Mill'in klasik, bir kişi istediğini yapmaya, başkasına zarar vermeyecek sınırlar içerisinde serbesttir tanımlamasıyla sınırlı olarak anlaşılmamalıdır.⁷⁰ Çünkü kontrol anlayışını savunanlar esas itibariyle, kişinin dışarıda bırakılmadığı; tam tersine kendisinin şekillendireceği ve fakat kendi bilgi kullanımı olanağının da şekilleneceği sosyal ilişkilerde bulunmasını mümkün kılan ve bu bağlamda düzenleme yetkisinin de kendisinde olduğu bir konsept ileri sürmektedirler.⁷¹

Kontrol anlayışının, özel yaşamın gizliliğini indirgediği kapsamın belirsizliğine, genişliğine veya kişisel tercihe fazlasıyla odaklanmasına ilişkin eleştiriler daha da artırılabilir. Fakat tüm bunlara rağmen bu yaklaşımın, kişisel bilginin hukuki korumasına zemin oluşturması özelliği de göz ardı edilmemelidir. Zira hukukun, sadece kişinin özgürce karar almasını, uygulamasını veya bilgilendirilmesini değil; aynı zamanda bu bilgiyi kişisel olarak görüp açıklamak veya kimseyle paylaşmak istemediği zaman bu kararını ve buna ilişkin yararını da koruduğu kabul edilir.⁷² Örneğin, Amerikan Yüksek Mahkemesi, kişinin paylaşmak istemediği kişisel bilginin bir şekilde açığa çıkmasının önlenmesindeki yararının da özel yaşamın gizliliği hakkının bir parçası olduğunu ifade eder. Kaldı ki, bu bağlamda, sosyal güvenlik, sağlık veya vergileme gibi konulara ilişkin olarak kişisel bilgilerin toplanması hususunu, 1970'li yıllardaki kararlarında dahi, özel yaşamın gizliliğine

⁶⁹ Paul M. Schwartz, "Property, Privacy, and Personal Data," **Harvard Law Review**, C.CXVII, No: 7, 2004, s. 2087-2089.

⁷⁰ Schwartz, **Property, Privacy, and Personal Data**, s. 2088.

⁷¹ Bezanson, "The Right to Privacy Revisited," s. 1142, 1143; Fried, **a.g.m.**, s. 482; Solove, **Understanding Privacy**, s. 26.

⁷² Jon L. Mills, **Privacy: The Lost Right**, New York, Oxford, 2008, s. 16, 17; Fried, **a.g.m.**, s. 483.

zarar verecek potansiyel tehlikeler olarak görür.⁷³ Bu tartışmanın, teknolojinin ve telekomünikasyonun sağladığı yollarla kişisel bilgiye ulaşılması konusu da eklenerek devam ettiği açıkça görülmektedir.

3. Mahremiyet (Intimacy)

Özel yaşamı kontrol bağlamında açıklayan anlayış, zamanla, özel yaşamın değerini belirlemek ve özellikle üzerinde kontrol sağlanacak bilginin kapsamını sınırlamak için bir mahremiyet görüşünü de geliştirir⁷⁴ ve bu son zamanlarda kabul gören görüş olarak da karşımıza çıkar. Buna göre, yaşam ilişkilerimiz ve yaşam ilişkilerimizi belli bir yakınlık ve gizlilik üzerine kurmamız da, özel yaşam hakkına biçtiğimiz değer ve önem bakımından belirleyicilik arz eder. Bir başka deyişle özel yaşam kavramı sadece kişinin kendisi ve kişiliği açısından değil, sosyal yaşamın bir yönü olarak insan ilişkileri bakımından da esaslı bir unsur olarak göz önünde bulundurulur.⁷⁵ Bu anlayışın savunucularının asıl kaygısı, özel yaşamın, başkalarından ayrı/tek başına olmanın ve gizliliğinin dışında bir şey olduğunu açıklayabilmektir.⁷⁶ Bu bağlamda, özel yaşamın gizliliği hakkını koruma isteğimiz devam etmeseydi, yakın ve özel yaşam ilişkilerimizin de varolmayacağı dahi ileri sürülür.⁷⁷

Bu yaklaşımın, en genel anlatımıyla özel yaşamı, başkalarıyla kurduğumuz ilişkiyi yakınlık veya uzaklık derecelerine göre nasıl şekillendirdiğimiz ekseninde açıkladığı söylenebilir. Aslında bunu yaparken, bir bakıma, yukarıda sayılan diğer her bir anlayışın tek tek açıklamaya çalıştığı kavramı da kapsayarak bir anlayış geliştirdiği görülebilir. Zira yaşamın hangi yönüne sınırlı ulaşımı sağlayabiliyoruz veya hangi bilgiyi kontrol edebiliyor veya gizli tutabiliyoruz sorularını da kapsar bir tanımlama

⁷³ Whalen v. Roe, 429 U.S. 589, February 22, 1977, No. 75-839, (Çevrimiçi) <http://www.caselaw.lp.findlaw.com>, 23 Mayıs 2010.

⁷⁴ Charles Fried, **a.g.m.**, s. 475-489. Özel yaşamın gizliliği hakkının mahremiyet bağlamında, AİHS kararlarına nasıl yansıdığı konusunda ayrıntılı bilgi için bkz.: Gülay Arslan Öncü, **Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması Hakkı**, İstanbul, Beta, 2011, s. 184-191.

⁷⁵ Solove, **Understanding Privacy**, s. 34.

⁷⁶ Daniel Farber, "Book Review/Privacy, Intimacy, and Isolation by Julie C. Inness," **Constitutional Commentary**, C.X, 1993, s. 514

⁷⁷ Fried, **a.g.e.**, s. 484-486.

verilmeye çalışılmaktadır.⁷⁸ Nitekim bu yaklaşımın en büyük savunucularından Inness, özel yaşamı sadece bilgi, ulaşım ve kendimize ait karar alanlarına yoğunlaşarak açıklayamayacağımızı; çünkü özel yaşamın bu üç unsuru da kapsayan ve bir yönüyle de farklılaşan bir kavram olduğunu vurgular. Bu farklılaşan nokta ise, ‘mahrem’dir: Mahrem bilgi, mahrem bağlantı ve mahrem kararlar.⁷⁹ Bu noktada Inness, mahrem kavramının da açıklanması gerektiğini ve bunun ya davranışlara ya da bu davranış motive eden duygusal nedene bakmak şeklinde iki yolla olabileceğini ifade eder. Bu iki yoldan da ‘davranışa’ değil; ondan önce gelen, insanı belli bir davranış için ‘motive’ eden nedenlere dayanarak, mahremi açıklamaya çalışır; aslında bireyin motivasyonunun esas teşkil ettiğini kabul eder.⁸⁰

Bu bağlamda, mahrem alanlar, ilişkide veya iletişimde olduğumuz kişinin - biz ve sosyal yaşam arasındaki kişinin - hoşlanması veya ilgi duymasından dolayı anlamlı ve değerli olan konulardır. Ona göre bu tanımlama ‘mahrem’in kapsamını ifade eder; özel yaşamın gizliliği ise bu tanımla ilişkili ve fakat farklıdır. Özel yaşamın gizliliği, iletişimde olduğumuz kişinin, onun sevgi, hoşlanma veya ilgi duymasından dolayı anlam kazanan konular üzerindeki kontrolü olarak tanımlanabilir.⁸¹ Görülüyor ki, bu açıklamada, mahrem açısından belirleyici olan, diğer kişi için ifade ettiği anlam veya değerdir ve böylelikle özel yaşam çoğunlukla duygusal ilişkiler bazında nitelenir. Diğer yandan ise, mahremiyeti, sadece hayatta bizim için çok büyük önem taşıyan kişilere karşı göstereceğimiz davranışlarımız veya duygularımız olarak tanımlamak da düşünülebilir. Bu açıdan bakıldığında özel yaşam ise, bir süreçtir; bir anlatma sürecidir ve hem başkaları hem de kendimizle ilgili bilgilere dair içeriğin yansıtılmasıdır. Fakat şu da unutulmamalıdır ki, özel bilginin paylaşılmasının tek nedeni de mahremiyet ve mahrem ilişkiler değildir.⁸²

⁷⁸ Solove, *Understanding Privacy*, s. 34.

⁷⁹ Inness, *Privacy, Intimacy, and Isolation*, Aktaran, Farber, *a.g.m.*, s. 514.

⁸⁰ Solove, *Understanding Privacy*, s. 34, 35; Farber, *a.g.m.*, s. 517.

⁸¹ Tom Gerety, “Redefining Privacy,” *Harvard Civil Rights-Civil Liberties Law Review*, C.XII, No: 2, 1977, s. 268; Solove, Schwartz, *Privacy, Information, and Technology*, s. 45; Fried, *a.g.e.*, s. 483, 484.

⁸² Sandra Petronio, *Boundaries of Privacy, Dialectics of Disclosure*, New York, State University of New York Press, 2002, s. 6.

Özel yaşamı böyle bir mahrem anlayışıyla, bir başka deyişle kişinin motivasyonuna göre mahrem niteliği kazanan konular ekseninde açıklamak,⁸³ yukarıda açıklanan özel yaşamı “kişinin bilgi üzerindeki kontrol imkanı” olarak açıklayan görüş ile de belli noktalarda kesişebilir. Daha doğrusu bu yönüyle bakılınca, o görüşü savunanların da mahrem bilgi tanımlaması yaptıkları ve bu tanımlamadan yola çıktıkları söylenebilir. Özel yaşamı “bilgi üzerinde kontrol imkanı” olarak açıklayanlar için de mahremiyetin ihlali, bir kişinin başkalarıyla paylaşmayacağı veya paylaşmamaya hakkı olduğu davranışlarının, duygularının veya inandıklarının bir başkasıyla paylaşılmasıdır. Bu da daha çok, sevgi ve arkadaşlık çerçevesinde sürdürülen ahlaki durumu ifade eder.⁸⁴

Aslında yukarıda da ifade edildiği gibi, kontrol yaklaşımı, tam da bu noktada Inness’in duygusal ilişki ve motivasyon bazında açıkladığı mahrem anlayışıyla kesişir. Nitekim iki yaklaşım arasındaki farklılık ise en açık şekilde, özel yaşamın hangi iki unsur arasındaki ilişkiye dayandığı açıklanarak belirtilebilir. Bu bağlamda, özel yaşamı anlamlı kılanın, bireyin kendisine ve kendisiyle ilgili bilgiye kimin ulaştığını kontrol edebilme kabiliyeti ile farklı kişilerle farklı düzeyde sosyal yaşam ilişkileri kurabilme kabiliyeti arasındaki ilişki olduğu ileri sürülür.⁸⁵

Kanımızca, aslında bu açıklamayla dahi, iki yaklaşım arasındaki farkın değil; ikisinin ortak ilişkisinin ifade edildiği söylenebilir. İki yaklaşım arasındaki bu ikili ilişkiyi kurarak özel yaşamı açıklayanların mahrem bilgiyi tanımlarken, dar bir kapsamda, paylaşmak istediğimiz veya aksi takdirde saklayacağımız bilgiye dayanmadıkları gözden kaçmamalıdır.⁸⁶ Eğer sadece bu paylaşım kontrolüne dayansalardı, kişisel bilgi üzerindeki kontrol anlayışından pek de ayrılmadıkları dahi söylenebilirdi. Özel yaşamın gizliliğini mahremiyet olarak açıklayan yaklaşımın asıl üzerinde durduğu,

⁸³ Gerety, **a.g.m.**, s. 268.

⁸⁴ Fried, **a.g.e.**, s. 480-484.

⁸⁵ Jeffrey Rosen, “Purposes of Privacy: A Response,” **The Georgetown Law Journal**, C.LXXXIX, s. 2122; Jeffrey Rosen, **The Unwanted Gaze: The Destruction of Privacy in America**, s. 8, 9, Aktaran, Solove, Schwartz, **Privacy, Information, and Technology**, s. 46; Gerety, **a.g.m.**, s. 265, 266; Solove, Schwartz, **Privacy, Information, and Technology**, s. 45; Solove, **a.e.**, s. 35.

⁸⁶ Inness’in mahrem anlayışını eleştiren ve bu anlayışı yaşamın mahrem alanlarını, mahrem bilgiyi kontrol imkanı olarak gören yaklaşım için bkz.: Farber, **a.g.m.**, s. 510-514.

karşıdaki diğer kişiye karşı sevgi, ilgi veya özen şeklinde ortaya çıkan duygusal motivasyon ve bunun basit bir şekilde özel bilgilerin başkasıyla paylaşılması olmadığı hususudur.⁸⁷ Bu nedenle, bu anlayışta, başkalarının bize ulaşması imkanını yaratmak her zaman özel yaşamın gizliliğinin ihlalini teşkil etmez; örneğin bir doktorun bize ve bize ait bilgiye ulaşabiliyor olması, bu yakınlığı mahrem olarak nitelendirmemizi sağlamaz.

En çok kabul gören anlayışlardan biri olsa da,⁸⁸ sadece ilişki kurduğumuz kişiye bir ilgi veya yakınlık gibi farklı duygusal bağ hissettiğimizde, mahrem bir ilişki ve bilgi paylaşımı içine girdiğimizi kabul eden ve özel yaşamı böyle bir mahremiyet temeline dayandıran bu anlayış da, diğer yaklaşımlar için ileri sürdüğümüz fazla geniş ama aynı zamanda fazla sınırlı şeklindeki eleştirilerden kurtulamamaktadır. Nitekim en başta, özel yaşamı sadece özel bir duygusal ilişki içine girdiğimiz kişilerle oluşturduğumuz ilişki çerçevesinde yaptıklarımız olarak nitelendirmek ve bu şekilde ‘güven, ilgi ve sevgi’ üçlemesi üzerinden duygusal motivasyon temeline dayandırmak⁸⁹ son derece ucu açık bir niteleme olarak görülebilir. Zira ilk göze çarpan haklı eleştirilerden biri, ilgi veya sevgi çerçevesinde yapılan her hareketin mahrem bir davranış teşkil etmeyeceğidir. Başkasına bir hediye almak veya onun için yemek pişirmek de belli bir duygusal motivasyon ile yapılabilir ama her durumda mahrem davranış oluşturmayacağı ortadadır.⁹⁰ Bununla beraber, duygusal motivasyon temelli bir açıklamanın kapsam açısından çok da anlamlı bir sınırlama yaratamayacağı nedeniyle ucu açık, belirsiz olduğu da ileri sürülmüştür.⁹¹

Bu anlayışın diğer yönüyle özel yaşama aslında dar kapsamlı, sınırlı bir açıklama getirdiği;⁹² güven, ilgi ve sevgi konseptinin özel yaşamı açıklamada yeterli olamayacağı söylenebilir.⁹³ Yukarıda verilen, belli bir motivasyonla yapılan ama her

⁸⁷ Solove, *Understanding Privacy*, s. 34, 35.

⁸⁸ Solove, *Understanding Privacy*, s. 34.

⁸⁹ Farber, *a.g.m.*, s. 510.

⁹⁰ Farber, *a.g.m.*, s. 514, 515.

⁹¹ Solove, *Understanding Privacy*, s. 36.

⁹² Gavison, *a.g.m.*, s. 446; Solove, *Understanding Privacy*, s. 36, 37.

⁹³ Judith W. DeCew, “Review the book ‘Privacy, Intimacy, and Isolation’ by Julie Inness,” *Ethics*, C.CIV, Ekim 1993, s. 206.

zaman özel yaşamı tanımlayamayacak ve mahrem sayılamayacak sosyal davranışlar buna örnek gösterilebilir. Bunun dışında, özel yaşamın her zaman sadece kişinin başkalarıyla olan ‘yakın’ ilişkisinden ibaret sayılamayacağı da söylenebilir; çünkü bu durumda kişinin sadece kendisine ait olan ‘özel’ yaşamı korumasız kalır.⁹⁴ Örneğin, bilgisayar ortamında kişisel bilgilerin toplanması, özel yaşama müdahale olarak nitelendirilirken; bu ihlalin sosyal yaşantımızdaki arkadaşlığa, hoşlanmaya veya sevgiye dayalı ilişkilerimizi etkilemesi gerekmez. Kaldı ki, bu müdahale çoğu kez, bu duyguları beslediğimiz ve bu duygularla ilişkide olduğumuz kişilerden değil; devlet, özel sektör veya çeşitli kuruluşlardan kaynaklanır.⁹⁵ Aslında bu nedenledir ki, özel yaşamın korunması kavramı da zamanla değişmiş; kişilerin duygusal motivasyonu gibi statik bir temelle açıklanmak yerine, teknolojinin ve hatta günlük yaşamın değişen boyutlarını da göz önünde bulunduran, nelerin özel yaşamın gizliliğinin ihlalinin oluşturacağını da geliştiği ve değiştiği gibi bir yaklaşım benimsenmeye başlanmıştır.

Kanımızca da hakikaten, özel yaşamı mahrem kavramıyla açıklarken, mahrem tanımlamasını da sadece sevgi, hoşlanma veya ilgiye dayalı duygusal motivasyon temelinde yapmak;⁹⁶ özel yaşamın sadece bu duygular dahilinde birlikte olduğumuz insanlar etrafında şekillenebileceği ve özel yaşamın gizliliğine müdahalenin de sadece bu ilişkinin taraflarından gelebileceği kabulü gibi sınırlı ve kişiyi esas almayan⁹⁷ bir yaklaşıma götürebilir. Nitekim bu yaklaşımı benimseyen ve özel yaşamı mahrem anlayışının bu dar yönüyle değerlendirenler de olmuştur. Jeffrey Rosen, mahrem bilginin etrafımızdaki sadece belli insanlarla değiş tokuşunu yapabileceğimiz bir bilgi olduğunu ifade eder. Bu yönüyle de, sadece uzun bir zaman zarfında yakın, güvene ve ilgiye dayalı mahrem bir ilişki kurduğumuz bu kişilerin

⁹⁴ Lawrence Lessig, “Privacy and Attention Span,” *The Georgetown Law Journal*, C.LXXXIX, 2000-2001, s. 2065.

⁹⁵ Priscilla M. Regan, “Privacy, Government Information, and Technology,” *Public Administration Review*, C.XLVI, No:6, Kasım-Aralık 1986, s. 629, 630.

⁹⁶ DeCew, a.g.m., s. 206; Farber, a.g.m., s. 514; Solove, *Understanding Privacy*, s. 34.

⁹⁷ Solove, *Understanding Privacy*, s. 36, 37.

bize ait mahrem bilgiye sahip olduğunu⁹⁸ ve ancak bu bilginin onlar tarafından başkalarıyla paylaşılması durumunda bize zarar verebileceğini vurgular.⁹⁹

Inness'in arkadaşlık, sevgi ve ilgi üzerinden duygusal motivasyona dayalı özel yaşam anlayışına dair en önemli eleştiri, bizce, bu yaklaşımın anayasal özel yaşamın gizliliği hakkına (**constitutional privacy**) dair ayrı bir koruma sağlayabilecekken; iletişimin gizliliğine (**informational privacy**) dair esaslı bir koruma oluşturamayacağı noktasında toplanabilir. Fakat bu bakış açısı Rosen'in son ifade edilen yaklaşımıyla da birlikte düşünülerek farklı bir değerlendirmeye de tabi tutulabilir ve o zaman mahrem anlayışının özel yaşamı o kadar da dar çerçevede görmediği söylenip, bu eleştiriye cevap verebilir. Buna göre, özel yaşam ve mahrem arasındaki bu etkileşim, ikisinin arasındaki farkı da ortaya koymaktadır. Örneğin, kişiye ait gizli bir bilginin, onu tanıyanlar arasında yayılmasıyla hiç tanımayanlar arasında yayılması farklı sonuçlar doğuracaktır.¹⁰⁰ Yayılan aynı bilgi olsa dahi, kişiyi tanımayanlar arasında yayılması, o kişiyi yaşamı, zevkleri ve ilgileri hakkında önyargı yaratılabilecek bir etkiye maruz bırakmaktadır. Her iki durumda da aynı bilgi yayılmıştır; fakat görülmektedir ki, bu yaklaşım, mahrem bilgiyi tanımlarken bu yönüyle özel yaşamın koruma işlevi açısından bir ayrım yaparak tanım getirmektedir. Bu bağlamda, mahrem bilgi, kişinin sadece kendisinin belirleyeceği, istediği kişilerle paylaştığı bilgidir. Özel yaşamın gizliliği ise, bilinmesi zarar verecek olsun veya olmasın, kişiye, o bilgiyle olan ilişkisini kendisinin düzenleyebilmesine imkan veren unsurdur.¹⁰¹ Bu açıdan bakıldığında, özel yaşamın gizliliğinin korunmasının işlevi de, kişiyi doğruluğu zedelenmiş mahrem bilgidен değil; o kişi hakkında yanlış anlaşılmaya neden olacak bilginin yaratacağı, kişiye zarar verecek sonuçtan korumaktır.

⁹⁸ Rosen, *The Unwanted Gaze: The Destruction of Privacy in America*, s. 8, 9, Aktaran, Solove, Schwartz, **Privacy, Information, and Technology**, s. 46.

⁹⁹ Jeffrey Rosen, "Privacy in Public Places," *Cardozo Studies in Law and Literature*, C.XII, No:1, 2000, s. 176; Rosen, **Purposes of Privacy: A Response**, s. 2120.

¹⁰⁰ Rosen, *The Unwanted Gaze: The Destruction of Privacy in America*, Aktaran Solove, Schwartz, **Privacy, Information, and Technology**, s. 46.

¹⁰¹ Gerety, *a.g.m.*, s. 284; Fried, *a.g.e.*, s. 484; Inness, **Privacy, Intimacy, and Isolation**, Aktaran, Farber, *a.g.m.*, s. 514; Solove, **Understanding Privacy**, s. 35.

4. Kişiyeye Sınırlı Ulaşım

Özel yaşam kavramına ilişkin bir diğeryaklaşım, özel yaşamı “sınırlı ulaşım” olarak kabul eder¹⁰² ve özel yaşamı kişinin tek başına olabilmek hakkı olarak da gören yaklaşımla yakından bağlantılıdır. Nitekim kişilerin, başkalarının onlar hakkında ne kadar bilgilerinin olduğuna ve ne kapsamda onlara ulaşabileceklerine ilişkin kaygıları aslında özel yaşamın gizliliği konusundaki ilgi ve kaygılarını da belirlemede büyük rol oynar. Zira özel yaşam kavramı başlı başına, kişinin başkalarından ayrı ve bağımsız olabilmeye ilişkin ihtiyaç ve isteği doğrultusunda şekillenir. Kişinin başkalarının ona sınırlı ya da kendi istediği kadar ulaşması isteği ise, özel yaşama ilişkin bu beklentinin dahi kapsamını genişletir. Böylelikle, örneğin, sadece medya veya kamunun çeşitli kesimleri tarafından özel yaşama yapılan müdahaleler değil; devletin özel yaşama karışması veya müdahalesi de özel yaşama ilişkin tam koruma isteğini mümkün kılar. Çünkü bu “sınırlı ulaşım”, kişinin istemediği bilgilerin, kişilerin ve hatta istemediği düzeyde bir bilginin muhatabı olmasını engeller.¹⁰³

Özel yaşamın gizliliğini sınırlı ulaşım olarak kabul edilen görüşler aslında iki noktada toplanabilir. Bunlardan ilki, kişinin kendisine ulaşılması bakımından sahip olduğu kontrol yetkisi olarak ifade edilebilir; diğeryise, kişiyeye sınırlı ulaşılmasının zaten var olduğu olgusundan yola çıkar.¹⁰⁴ Bu ikinci yaklaşımın esasını, aslında her ‘sınırlı’ iletişim durumunun kişinin kendi tercihiyle gerçekleşmediği gerçeği oluşturur. Nitekim bazen bu durum kişinin istemeden yalnız kaldığı koşulları dahi kapsar. Fakat böyle bir değerlendirmeye, kişinin fiziken tek başına olduğu bir yerde veya sosyal olarak toplumdan soyutlandığı bir ortamda bir başka ifadeyle yalnız olduğu bir durumda, özel yaşam tartışmasının anlamsız kalacağı da açıktır.

¹⁰² Cate, *Privacy in the Information Age*, s. 27; Gavison, a.y.; Solove, Schwartz, *Privacy, Information, and Technology*, s. 45; E. L. Godkin, *Libel and Its Legal Remedy*, Aktaran Solove, *Understanding Privacy*, s. 19; “The Right to Privacy in Nineteenth Century America,” s. 1909; Bennett, a.g.e., s. 25; Gavison, a.g.m., s. 428, 429; Diffie, Landau, a.g.e., s. 142.

¹⁰³ Solove, Schwartz, *Privacy, Information, and Technology*, s. 45; Solove, *Understanding Privacy*, s. 18-21.

¹⁰⁴ Solove, *Understanding Privacy*, s. 18-20.

Bu açıdan, kişi bakımından, neyin onun için ‘özel’ olduğunun belirlenmesi önemlidir. Zira bu belirleme yapılmazsa, sadece sınırlı ulaşma kavramı özel yaşamın kapsamı bakımından çok da açıklayıcı değildir.¹⁰⁵ Çünkü unutulmamalıdır ki, bir kişiye ait her unsura ulaşmak, her durumda istenmeyen bir müdahale veya karışma olarak nitelendirilemez. Böyle bir müdahale veya karışma, o kişinin onu belirli kıldığına inandığı unsurlara veya bilgiye ve hatta dış dünyadaki istemediği unsurlara ulaşma şeklinde ise, belirleyicilik kazanarak bir ihlal olarak değerlendirilebilir.¹⁰⁶ O halde şu soruyu sormak gerekmektedir: Bir kişinin sadece dikkatlice izlenerek veya bir arkadaşıyla yaptığı konuşma dinlenerek ona veya arkadaşına ait yaşı, mesleği hatta saç rengi, yüz şekli gibi kişisel görünümü hakkındaki bir bilgiye ulaşılması; özel yaşamı etkileyecek şekilde bir kişisel bilgiye ulaşım olarak nitelendirilecek midir?

Kanımızca bu yaklaşım çerçevesinde şu ana kadar ileri sürülen ilkeler, sorduğumuz bu soruyu kesin olarak cevaplamaya yetmemektedir. Bu bağlamda, Gavison’un sınırlı ulaşma dair belki de en açıklayıcı nitelendirmeyi yaptığı söylenebilir. Buna göre, özel yaşamımızın korunmasına olan ilgimiz, aslında insanların bizim hakkımızda ne kadar şey bildiği, ne kadar onların ilgi konusu olduğumuz ve onların bize fiziksel olarak ne kadar ulaşabildikleri ile alakalıdır.¹⁰⁷ Bu görüş, kişinin tek başına olduğu veya başkalarıyla paylaştığı fiziksel mekan tanımlaması kaygısından uzaktır. Aksine, kişiye ilişkin hangi unsura, neye, ulaşım sağlanırsa, özel yaşamın gizliliğinin ihlal edileceği hususuyla ilgilenilmelidir.¹⁰⁸

¹⁰⁵ Solove, *Understanding Privacy*, s. 20.

¹⁰⁶ Julie C. Inness, *Privacy, Intimacy and Isolation*, Oxford, New York, 1992, s. 29; Solove, *Understanding Privacy*, s. 20.

¹⁰⁷ Gavison, *a.g.m.*, s. 423, 424.

¹⁰⁸ Inness, *a.g.e.*, s. 63, 64.

5. Kişisel Özerklik / Bağımsızlık

Kişisel özerklik, bireyin sosyal yaşamda varolduğu görüntüyle gerçekte nasıl olmak istediği arasında çoğu kez farklılık olduğu noktasından hareket eder.¹⁰⁹ Aslında bu farklılık sosyal yaşamda insanların maskeyle gezdiğine dair klasik nitelemeyle paralel görülebilir. Nitekim insan sözcüğünün etimolojik anlamının, bir kişinin kendisini sosyal yaşamdaki aktörlere doğrudan ve dolaylı sunum şekli bağlamında ‘maske’ olduğu dikkate alınır,¹¹⁰ bu saptamanın çok da isabetsiz olmadığı ileri sürülebilir.

Her birey, özel yaşamının gizliliğini, kişisel gelişimini ve hatta bağımsızlığını sürdürebilmek için gerekli görür. Kaldı ki, demokrasilerde kişisel bütünlüğü korumaya ve kişisel özerkliğe saygının esaslı unsurlar olduğu da yadsınamaz bir gerçektir. Bu özerklik, kişinin düşüncelerini ve hayata bakışını özgürce oluşturması, geliştirmesi ve her şeyden önemlisi özgür ve bağımsız bir muhakeme gücüne kavuşması olarak kendini gösterir ve vazgeçilmezdir.¹¹¹ Çünkü bu kişisel yetkinlik ve bütünlük, demokratik bir hukuk devletinde varolması gereken düşünce, inanç, siyasi düşünce ve hatta biraraya gelme çeşitliliğini de beraberinde getirecektir. “İzlenmeyen ve gözetlenmeyen tercihler (**unmonitored choice**)”, özel yaşama saygıyı artırırken, gerekli hukuksal korumayı da pekiştirebilecektir.¹¹² Kişinin bu şekildeki bağımsızlığı, onun bir düşüncesini veya davranışını toplumla paylaşmadan önce belirli bir zamana da ihtiyacı olduğunu ortaya çıkarır. Bu özerkliğin önemli bir kısmını ise, bireyin kendisinin ne zaman sosyal yaşama karışmayı doğru buluyorsa o zaman karışması oluşturmaktadır. Bu husus, sosyal yaşama dair başkaları tarafından belirlenmiş ve dikte ettirilmiş kararlar çerçevesinde hareket etmeme serbestliği olarak da değerlendirilebilir.¹¹³

¹⁰⁹ Julie Cohen, “Examined Lives: Informational Privacy and the Subject as Object,” Aktaran Solove, Schwartz, **Privacy, Information, and Technology**, s. 46-48; Gavison, **a.g.m.**, s. 449, 450; Diffie, Landau, **a.g.e.**, s. 142.

¹¹⁰ Westin, **Privacy and Freedom**, Aktaran Aktaran Solove, Schwartz, **Privacy, Information, and Technology**, s. 43.

¹¹¹ Cate, **Privacy in the Information Age**, s. 23, 24.

¹¹² Solove, Schwartz, **Privacy, Information, and Technology**, s. 47; Mills, **a.g.e.**, s. 15, 16.

¹¹³ “Engaging Privacy and Information Technology in a Digital Age”, Ed. by. James Waldo, Herbert S. Lin, and Lynette L. Millett, Washington, DC, The National Academic Press, 2007, s. 66, 67.

Şu da unutulmamalıdır ki, bu yaklaşım birey ve toplum arasında her durumda otomatik bir kademelenme yaratılması gerektiği varsayımından yola çıkmaz; biri diğerine ait değerleri korumayı engellemez.¹¹⁴ Görülüyor ki, kişinin kendi kararlarını kendisinin alması, istemediklerini paylaşmaması şeklindeki kişisel yetkinliği, özel yaşamın koruduğu bir değer olarak karşımıza çıkarken; aslında karşılıklı bir etkileşime de kaynak oluşturmaktadır. Nitekim iki taraflı bu ilişkiyle, kişisel özerklik özel yaşamın gizliliğinin sağlanmasıyla böylece korunurken; özel yaşam ve ilgili hukuksal koruma da bir yönüyle değer kazanmaktadır.

II. ÖZEL YAŞAMIN GİZLİLİĞİ KAVRAMININ KAPSAM İTİBARIYLA DEĞERLENDİRİLMESİ

A. Özel Yaşamın Gizliliği Kavramının Koruduğu Değerler

Özel yaşam kavramına ilişkin yapılacak tanımlamanın içinde birden fazla faktörü barındıracak, karmaşık ve içiçe geçmiş bir kavramsallaştırma olacağı açıkça ifade edilebilir. Özellikle özel yaşamın korunmasının gerçekleştirdiği işlevler, koruduğu değerler açıklandıktan sonra, yukarıda açıklanan özel yaşamın tanımlanmasına ilişkin yaklaşımların her birinin farklı ama birbiriyle bir o kadar da üst üste geldiği görülebilecektir.¹¹⁵ Bu açıdan, genel, ortak bir payda bulmaya çalışmak ve onun üzerinden bir tanımlama yapmak hem çok sınırlı hem de çok geniş olabileceği nedeniyle çok da belirleyici gözükmeyebilir.¹¹⁶ Kaldı ki, birebir örtüşen özel yaşamın gizliliği anlayışına sahip olmasalar da, hem Amerikan Yüksek Mahkemesi'nin hem

¹¹⁴ Daniel Ortiz, "Privacy, Autonomy, and Consent," *Harvard Journal of Law and Public Policy*, C.XII, 1989, s. 92.

¹¹⁵ Diffie, Landau, *a.g.e.*, s. 142; Solove, *Understanding Privacy*, s. 12, 13.

¹¹⁶ Cate, *The Privacy Problem*, s. 2; Goldman, *a.g.m.*, s. 67. Bu noktada yaşam koşullarındaki teknolojiye bağlı değişikliğin getirdiği farklılıkların da belirli ve sınırlı bir özel yaşamın gizliliği tanımı yapılmasını çok da mümkün kılmadığı belirtilmektedir. Zira sınırsız bir özgürlük yaratan iletişim ağları ve kişinin bu imkanları sınırsız kullanma isteğinin; kişisel ve toplumsal çıkarlar arasındaki denge tartışmalarını beraberinde getirdiği ve bu sınırsızlıkta ne zaman ve hangi sınırdaki özel yaşamın gizliliği problemini ve tanımını ortaya çıkaracağını da belirsiz kıldığını ifade eden görüş için bkz.: Stefano Rodota, "Beyond the EU Directive: Directions for the Future, Privacy: New Risks and Opportunities", Ed. by. Yves Poullet, Cecile de Terwangne, Paul Turner, Belgique, Centre de Recherches Informatique et Droit, 1997, s. 209, 210; Post, *a.g.m.*, s. 652.

de AİHM'nin¹¹⁷ özel yaşamın gizliliği tanımı yapmak kaygısıyla kendilerini ve kavrama ilişkin korumayı sınırlamadığı ifade edilebilir.

İşte tam bu noktada, öğretinin, özel yaşamın gizliliği tanımından öte, özel yaşama dair farklı yaklaşımların genel itibariyle - yukarıda açıklanan - dört grup halinde toplandığı üzerinde mutabık kaldığı söylenebilir. Nitekim Ken Gormley'in, Warren ve Brandeis'in özel yaşamın gizliliğini ilk kez konu alarak yayımladıkları makalelerinden, 1890'lı yıllardan başlayarak, sonraki yüz yıl içinde ortaya çıkmış özel yaşama ilişkin anlayışları da dikkate alarak, özellikle Anglo Sakson hukuku açısından özel yaşamın adeta evrimini ortaya koymak üzere yaptığı "Özel Yaşamın 100. Yılı"¹¹⁸ çalışması, genel olarak dört grup yaklaşımın olduğunu ortaya koyar: Tekrar özetlemek gerekirse, bunlar özel yaşamın gizliliğini, i) kişiliği esas olarak tek başına olabilmek ve kişinin kendi seçimlerini ve gelişimini kendisinin belirleyebilmesi olarak gören;¹¹⁹ ii) kişinin kendi oluşturduğu düşünce ve davranışlarını özgürce oluşturması ve uygulaması - kişisel bağımsızlık - olarak kabul eden;¹²⁰ iii) kişinin kendine ait bilgiyi ve böylece başkalarıyla olan ilişkisini de kontrol etme imkanı şeklinde gören¹²¹ ve son olarak da iv) gizliliği, kişinin başkalarından ayrı olabilmelerini ve anonimliği de kapsayacak şekilde, kişinin başkalarının kendisine ne kadar ulaşmasını ve başkalarının ilgilerine ne kadar konu olmayı istediğini belirleyebilmesi¹²² - sınırlı ulaşım - olarak kabul eden yaklaşımlar olarak ifade edilebilir.¹²³ Bunlara belki daha sonraları ifade edilmeye başlanan

¹¹⁷ Case of Niemietz v. Germany, (Application no. 13710/88), Strasbourg, 16 December 1992, para 29.

¹¹⁸ Ken Gormley, "One Hundred Years of Privacy," *Wisconsin Law Review*, C.MCMXCII, 1992, s. 1335-1441.

¹¹⁹ Diffie, Landau, *a.g.e.*, s. 149; Kenyon, Richardson, *a.g.m.*, s. 4; Solove, *Understanding Privacy*, s. 15-18; Etzioni, *a.g.e.*, s. 89, 190; Cate, *Privacy in the Information Age*, s. 21; Bennett, *a.g.e.*, s. 25.

¹²⁰ Solove, Schwartz, *Privacy, Information, and Technology*, s. 42, 43; Solove, *Understanding Privacy*, s. 18-21; Cate, *Privacy in the Information Age*, s. 23, 24; Cohen, *a.e.*; Gavison, *a.g.m.*, s. 449, 450; Diffie, Landau, *a.g.e.*, s. 142.

¹²¹ Bezanson, *The Right to Privacy Revisited*, 1992; Solove, Schwartz, *Privacy, Information, and Technology*, s. 44, 45; Solove, *Understanding Privacy*, s. 24-29; Cate, *Privacy in the Information Age*, s. 21; Bennett, *a.g.e.*, s. 25; Murphy, *a.e.*; Goldman, *a.g.m.*, s. 67.

¹²² Cate, *Privacy in the Information Age*, s. 27, 28; Solove, *Understanding Privacy*, s. 18-21; Bennett, *a.g.e.*, s. 25; Solove, Schwartz, *Privacy, Information, and Technology*, s. 45; Diffie, Landau, *a.g.e.*, s. 142; Godkin, *a.e.*; "The Right to Privacy in Nineteenth Century America," s. 1909; Gavison, *a.g.m.*, s. 428, 429.

¹²³ Gormley, *a.g.m.*, s. 1337-1338.

mahremiyet anlayışı eklenebilir; ama yine de daha önce de ifade edildiği üzere, bu anlayışın da aslında kişisel bilginin kontrol anlayışıyla içiçe geçmiş ve belli noktalarda onu açıklamak üzere ortaya konulmuş olduğu unutulmamalıdır.

Bir yandan, yukarıda bu yaklaşımlar açıklanırken de ifade edildiği gibi, bu anlayışların her biri birçok noktada birbiriyle kesişmektedir. Diğer yandan, bu dört anlayışın dahi tek başına ele alındığında, özel yaşamın gizliliği tanımlamasını eksik veya belirsiz bırakabileceği rahatlıkla görülebilir. Kuşkusuz, daha sonra görüleceği gibi, Anglo Sakson ve Kıta Avrupası hukukçularının kural koyarken izledikleri ilkeler bakımından, her birinden yararlandığı görülür. Fakat buna rağmen, çoğunlukla kabul edildiği üzere bu dört anlayıştan aslında birinin, özellikle çalışmada daha sonra incelenecek olan iletişimin gizliliği bağlamında özel yaşamın gizliliğinin tanımlanmasında, esas rol oynadığı söylenebilir. Bu çerçeveyi Alan Westin'in kişisel bilgi üzerindeki kontrol anlayışından yola çıkarak yaptığı tanımlama oluşturmaktadır. Buna göre, özel yaşamın gizliliği "kişilerin, kendilerine ait bilgiyi ne zaman, ne şekilde ve ne kapsamda başkalarıyla paylaşacaklarını belirleyebilmelerine ilişkin taleplerinin korunmasıdır."¹²⁴

Bu tanımlamanın da çok fazla unsuru içerdiği kimi zaman ifade edilmişse de,¹²⁵ hukuki korumayı sağlayabilecek genişlikte olduğundan hareketle genel itibarıyla makul karşılandığı söylenebilir. Nitekim aslında bir yandan sınırlılık ve tarafsızlık içerdiği de söylenebilir. Başkalarıyla paylaşılması tercih edilecek bilginin doğru veya yanlış, anlamlı veya anlamsız, önemli veya önemsiz olduğuna bir başka anlatımla içeriğine bir belirleme getirmez. Bu noktada önemli olan, özel yaşamın gizliliğinin korunmasına neden ihtiyaç duyduğumuz olabilir. Zira korumak istediğimiz başka amaçlara ulaşmak için mi gereksinim duyuyoruz bir başka deyişle aslında özel yaşam

¹²⁴ Westin, *Privacy and Freedom*, Aktaran Solove, Schwartz, **Privacy, Information, and Technology**, s. 41; Gerety, **a.g.m.**, s. 261. Westin'in özel yaşamın gizliliği yaklaşımının bir yönünün de, sosyal yaşamın gerekleri ve mahremiyet isteği arasındaki dengenin oluşturduğu söylenebilir. Westin'e göre, kişi toplumsal yaşamın bir gereği olarak sosyal paylaşımda bulunma, sosyal yaşama katılma ve ilişkilerde bulunma zorunluluğu ile kendi bağımsızlık ve mahremiyet ihtiyacı arasında denge kurmak zorundadır. Bu dengeyi, bilgiyi tutma ve gerektiğinde paylaşma; topluma katılma ve katılmama; yalnızlık ve başkalarıyla birlikte olma; mahremiyet ve genel sosyal paylaşım arasında sağlaması gerekmektedir, Westin, *Privacy and Freedom*, Aktaran, Etzioni, **a.g.e.**, s. 200.

¹²⁵ Gerety, **a.g.m.**, s. 262-263.

denilen bu konseptle mi yoksa sadece sonuçla mı ilgilimiz? Temel niteliğin “özel” diye kabul edilen bir unsur olduğunu söylemek çok da yerinde midir?

Aslında bu sorular da gösteriyor ki, sorgulanması gereken özel yaşamın olabildiğince sınırlı ve dar bir tanımlamasını bulmaktan öte, hangi işlevlere hizmet ettiği bir başka deyişle hangi değerleri koruduğu olmadığıdır. Bu açıdan, Westin’in kavramsallaştırmasının özel yaşamın korunmasının hizmet edeceği yararların, korunacak değerlerin ne olduğuna da ışık tuttuğu söylenebilir.

Korunan bu değerlerden ilki, kişinin hayatını ve gelişimini kendi istediği yönde devam ettirebilmesi için gerekli olan bağımsızlıktır. Daha önce açıklandığı üzere, kişisel özerklik / bağımsızlık unsurunu özel yaşamı açıklamak üzere, ayrı bir anlayış olarak kabul eden bir yaklaşım da vardır.¹²⁶ Fakat Westin aslında, bu kişisel bağımsızlığın özel yaşamın gizliliğinin korunmasının yerine getirdiği işlevlerden biri olduğunu kabul eder. Nitekim örneğin, kişinin ne zaman sosyal yaşama karışıp toplumun önüne çıkacağına karar vermesinin aslında kişisel bağımsızlığın bir yönü olduğunu ifade eder. Temel soruyu da, bağımsız olarak düşüncelerini ve davranışlarını oluşturmamış bir kişi gerçekten ne hissettiğini ve ne düşündüğünü bilebilir mi şeklinde sorar.¹²⁷ Zira bu bağımsızlık, her şeyden önce kişisel gelişim için vazgeçilmezdir. Kişiye özel bir alan bırakılması, bir bireysellik geliştirebilmesi ve kişisel bütünlüğünü koruyabilmesi bakımından önemlidir. Bu alanı iki çember olarak düşünersek, içteki daireyi kişinin korkuları, yapmak istediklerine ilişkin duyguları gibi aslında zor durumda kalmadıkça paylaşmaya da konu yapmayacağı esas alanın oluşturduğu kabul edilir. Dış daireyi ise çok yakın ilişki içinde olduğu kişilerle paylaşmak isteyebileceği mahrem bilgilerin yer aldığı alan oluşturur.¹²⁸ Asıl

¹²⁶ Solove, Schwartz, **Privacy, Information, and Technology**, s. 42, 43; Solove, **Understanding Privacy**, s. 18-21; Cate, **Privacy in the Information Age**, s. 23, 24; Cohen, **a.g.m.**, s. 46-48; Gavison, **a.g.m.**, s. 449, 450; Diffie, Landau, **a.g.e.**, s. 142.

¹²⁷ Alan F. Westin, “Science, Privacy, and Freedom: Issues and Proposals for the 1970s Part I The Current Impact of Surveillance on Privacy,” **Columbia Law Review**, C.LXVI, No:6, 1966, s. 1023 (Bundan sonra Science, Privacy, and Freedom olarak anılacaktır.) Ayrıca bkz.: Solove, Schwartz, **Privacy, Information, and Technology**, s. 42, 43.

¹²⁸ Westin, **Science, Privacy, and Freedom**, s. 1022, 1023.

tehlike iç daireye de, kişinin paylaşmak zorunda olduğu alan gibi bakılması ve oraya girilmeye çalışılması olacaktır.¹²⁹

Bu bağlamda, özel yaşamın gizliliğinin korunması kişinin bu esaslardan oluşan bağımsızlığını koruma çabası olarak görülür. Bu bağımsızlığın da, demokratik bir toplumda özgür bireyin bağımsız birey olduğundan yola çıkarak; kişinin çok yakınlarıyla dahi paylaşmak istemeyeceklerini kendisinde tutabildiği an başlayacağı kabul edilir.¹³⁰

Özel yaşamın gizliliğiyle ile korunan ikinci değer, duygusal rahatlama ve çözülmedir.¹³¹ Özel yaşam ve sağladığı gizlilik, kişiye özgür bir yaşamın gerektirdiği duygusal rahatlama ile toplumsal sorumluluk ve yükümlülüklerinden sıyrılma alanı sağlamaktadır. Bu yöndeki bir denge, kişinin fiziksel ve zihinsel sağlığı için vazgeçilmezdir ve gereklidir. Çünkü sosyal yaşam bireylerin, ilişkide bulundukları kişiye göre değişen, farklı düzeyde çeşitli roller yüklenmelerini gerektirir. Fakat bu rolleri veya rollerinden kaynaklanan sosyal sorumluluklarını da sürdürebileceği makul bir zaman vardır. Her şeyden önemlisi kişinin, sadece kendisi olabildiği, o zaman içinde bulunduğu psikolojik halini istediği şekilde yaşayabileceği anlar ve alanlar da vardır.¹³²

Bu alan, kimi zaman kişinin evidir; kimi zaman kamunun gözünden uzaklaştığını hissettiği başka bir mekandır; ama her zaman o an yapmak istediğini rahatlıkla açığa vurabildiği, istediği ölçüde duygusal yoğunluğu istediği ölçüde yaşayabildiği yerdir.¹³³ Kısacası, özel yaşamın koruduğu bu alan, sadece kişinin tek başına kaldığı, yanında kimsenin olmadığı kapalı bir kapı arkası değildir; bazen bir arkadaşıyla yaptığı ve kimsenin duymasını istemediği sohbetin geçtiği bir yer olarak bir restraaurantın arka köşesi de olabilir. Korunan bu alan, kişinin rahat iletişim içinde

¹²⁹ Westin, *Science, Privacy, and Freedom*, s. 1023.

¹³⁰ Westin, *Science, Privacy, and Freedom*, s. 1023, 1024.

¹³¹ Solove, Schwartz, *Privacy, Information, and Technology*, s. 43, 44; Cate, *Privacy in the Information Age*, s. 25; Westin, *Science, Privacy, and Freedom*, s. 1024-1026.

¹³² Solove, Schwartz, *Privacy, Information, and Technology*, s. 43.

¹³³ Westin, *Science, Privacy, and Freedom*, s. 1023; Cate, *Privacy in the Information Age*, s. 25; Solove, Schwartz, *Privacy, Information, and Technology*, s. 43.

bulunduğu, bakışlardan uzak olduğunu ve herhangi bir sosyal role bürünmediğini hissettiği alandır.¹³⁴ Bu bağlamda, örneğin gözlenen veya iletişimi denetlenen bir kişinin, bu sosyal rollerden hiçbir an sıyrılamayacağı; çünkü yaptığı hareketleri ve çevreye verdiği imajı kontrol etmekten kaçamayacağı söylenebilir.¹³⁵

Duygusal çözülmenin özel yaşam bağlamında diğer bir yönü ise sosyal normlarla ve hatta yaptırıma bağlanmış şekilleri olan hukuk kurallarıyla olan ilişkisine dayanır. Bu bağlamda, kişinin bazen yasaklanmış - trafik yasakları, tuvalette sigara içme gibi - ve fakat her durumda kişiyi öngörülen yaptırıma maruz bırakmayan davranışları olabilir ve toplum bu uymazlıkları belli oranda ‘izin verilebilir’ olarak kabul edebilir. Nitekim Westin, özel yaşamın bir fonksiyonu olarak duygusal çözülmeye bir oranda izin verilme veya kurallara uygunluk sınırını, haddini aşma hallerinin tümü biliniyor olsa; birçok kişinin şu an kurumsal bir disiplin düzeneği altında veya cezaevinde olacağı veya her şeyden önemlisi bu durumlara maruz bırakılma tehlikesi altında olacağını ifade eder.¹³⁶ Özel yaşamın, bu değeri koruduğu sürece anlam kazanacağı açıktır. Nitekim böyle bir koruma olmasaydı, hukuksal düzenlemeler bir yana, birarada yaşamının gerektirdiği sosyal kurallar bile, bireyin ihtiyacı olan zihinsel ve fiziksel rahatlama bağlamında sergilediği birçok davranış için dahi cezalandırılabilmesini olağan kılardı. Aslında bu yöndeki bir kabul, özel yaşamın gizliliğine sahip olmaya ilişkin en yalın beklenti olan, özel yaşamın, en azından, özgür bir toplumda izin verilebilir ihlaller için var olması gerektiği anlayışının bir yansıması olarak görülebilir.¹³⁷ Zira özel yaşamın gizliliğinin korunmasının, kişinin tek başına iken ve hatta yukarıda ifade edilen mahrem ilişki içinde bulunduğu kişilerle biraradayken, özgür yaşamın esaslı bir unsuru olarak, sosyal etiketlerden sıyrılabilmesini gerektirdiği kabul edilir.¹³⁸

¹³⁴ Cate, **Privacy in the Information Age**, s. 25; Westin, **Science, Privacy, and Freedom**, s. 1024; Solove, Schwartz, **Privacy, Information, and Technology**, s. 43.

¹³⁵ Cate, **Privacy in the Information Age**, s. 25.

¹³⁶ Westin, **Science, Privacy, and Freedom**, s. 1025; Solove, Schwartz, **Privacy, Information, and Technology**, s. 43.

¹³⁷ Westin, **Science, Privacy, and Freedom** s. 1025; Solove, Schwartz, **Privacy, Information, and Technology**, s. 43.

¹³⁸ Westin, sosyal etiketlerden sıyrılabilmenin önemine değinirken; Goffman’ın kişilerin aktörler gibi sürekli sahnede rol yapar gibi, hissettiklerinden farklı duyguları yansıtabileceğinin mümkün olmadığı açıklamasına da gönderme yapar. Buna göre, kişi, aslında yalnızken veya yalnız olmasa da, ailesi veya

Özel yaşamın gizliliğinin korunmasının gerçekleştirdiği diğer işlev, sınırlı ve korunaklı bir iletişimdir.¹³⁹ Her birey, sadece zihinsel olarak rahatladığı korunaklı, özel bir mekana değil; korunaklı bir iletişime de ihtiyaç duymaktadır. Bu korunaklığı, gerek yakın ilişki içinde olduğu insanlarla veya ailesiyle gerek de sosyal yaşamın bir parçası olarak tanıdığı sınırlı bir paylaşım içinde olduğu insanlarla kurduğu iletişim ağına taşımak ister.¹⁴⁰ İşte özel yaşamın koruduğu bir değer olarak, sınırlı ve korunaklı iletişim unsuru bu noktada anlam kazanmaktadır.

Sınırlı ve korunaklı bir iletişim işlevini yerine getirirken özel yaşamın gizliliği, iki hususu içinde barındırır. İlk olarak, kişinin çok yakın ilişki içinde olmadığı kişilerle kurduğu iletişimde ona bir rahatlık ve koruma sağlar. Zira doktoru, avukatı veya profesyonel ilişki içinde olduğu diğer kişilerle sınırlı iletişim kurma özgürlüğüne sahip olur. Bunun yanı sıra, ailesi ve arkadaşları gibi çok yakın ilişki içinde olduğu kişilerle kurduğu iletişimde bir başka ifadeyle baştan aşağı doğal davrandığı, iletişim şeklini de kendisinin belirlediği durumda da bir koruma sağlar. Özel yaşamın gizliliği, kişiye sınırlı ve kendisinin istediği ölçüde korunaklı bir iletişim ve ilişkiler olanağı sağlar.¹⁴¹ Çünkü kişiye, sadece avukatı, doktoru veya iş arkadaşıyla kurduğu ve yasal düzenlemelerin gizliliğini koruduğu iletişimde değil; hiçbir zorunluluk hissetmeden, istediği gibi davrandığı kendisine yakın kişilerle olan ilişkisinde de belli bir güven hissettirir.¹⁴²

Son olarak özel yaşamın gizliliğinin koruduğu diğer değer, kişisel karar alabilme imkanı olarak karşımıza çıkar.¹⁴³ Özel yaşamın gizliliğinin korunması, kişinin yalnızca kendisinin etrafa ne zaman ve ne kapsamda bilgi paylaşmasına imkan

yakın arkadaşları ile beraberken veya kalabalık, kimsenin onu tanımadığı bir parkta veya sokakta iken ondan beklenen rolleri gerçekleştirme hissinden uzaklaşınca aslında kendisini yansıtabilir, Goffman, *The Presentation of Self in Everyday Life*, Aktaran, Westin, **Science, Privacy, and Freedom**, s. 1024. Ayrıca bkz.: Solove, Schwartz, **Privacy, Information, and Technology**, s. 43, 44; Cate, **Privacy in the Information Age**, s. 25.

¹³⁹ Westin, **Science, Privacy, and Freedom**, s. 1027-1029; Cate, **Privacy in the Information Age**, s. 27, 28; Bennett, **a.g.e.**, s. 25.

¹⁴⁰ Solove, Schwartz, **Privacy, Information, and Technology**, s. 44.

¹⁴¹ Cate, **Privacy in the Information Age**, s. 27.

¹⁴² Solove, Schwartz, **Privacy, Information, and Technology**, s. 44.

¹⁴³ Cate, **Privacy in the Information Age**, s. 25, 26; Westin, **Science, Privacy, and Freedom**, 1026, 1027.

sağlayacak bir bağımsızlık işlevi görmez. Aynı zamanda, kişinin kendisine ulaşan bilgileri ve bu bilgi karşısında gerçekleştireceği davranışın alternatiflerini ve olası sonuçlarını da değerlendirebilmesini sağlar.¹⁴⁴ Bu yönüyle, bir kişinin kendine özgü tepkilerini gösterdiği veya mahrem bir iletişim içinde olduğu bir ortamdan, davranışlarını ve duygularını paylaştığı herkese açık sosyal bir ortama geçmek için uygun zamana ilişkin karar vermedeki yararını gerçekleştirir. Böylece kişiye, başkalarının davranışları karşısında nasıl bir tavır takınacağına ilişkin değerlendirme süreci bırakılır. Kısacası, özel yaşamın gizliliğinin gerçekleştireceği esaslı işlevlerinden biri olarak bu imkan, kişisel değerlendirme ve karar alabilme serbestliğini, özel yaşamın koruduğu esaslı değerlerden bir diğeri olarak karşımıza çıkarmaktadır.¹⁴⁵

B. Özel Yaşamın Gizliliğinin Tanımlanması Mümkün mü? Gerekli mi?

Westin'in tanımlaması,¹⁴⁶ özel yaşamın gizliliğinin koruduğu değerlerden hareket ettiği de dikkate alınır, bu çalışmanın kapsamı açısından özellikle iletişimin gizliliğinin anlaşılması açısından yararlı kabul edilebilir. Fakat buna rağmen, görülüyor ki, içerik olarak ve koruduğu değerleri itibarıyla, özel yaşamın gizliliğinden anladığımız her şeyi, tüketici bir sayımla sadece özel yaşamın gizliliği kavramının içine yerleştirebilmek neredeyse imkansız.¹⁴⁷ Bunu, özel yaşamın gizliliğini açıklayan yaklaşımların birbiriyle ne kadar örtüştüğü gerçeğini hatırlayarak da görebiliriz. Bu nedenle, olsa olsa bir ortak payda bulma çabası gösterilebilir; fakat geniş bir payda kavramı daha da belirsiz ve her riski kapsayacak hal getirebilecekken, dar kapsamda bir payda da çok sınırlı bir anlayışa doğru götürebilir.

¹⁴⁴ Alan Bates, "Privacy - A Useful Concept," *Soc. F.*, C.XLII, 1963-1964, s. 432, 433.

¹⁴⁵ Westin, *Science, Privacy, and Freedom*, s. 1027.

¹⁴⁶ "Özel yaşamın gizliliği kişilerin, kendilerine ait bilgiyi ne zaman, ne şekilde ve ne kapsamda başkalarıyla paylaşacaklarını belirleyebilmelerine ilişkin taleplerinin korunmasıdır.", Westin, *Privacy and Freedom*, Aktaran Solove, Schwartz, *Privacy, Information, and Technology*, s. 41.

¹⁴⁷ Diffie, Landau, *a.g.e.*, s. 142; Solove, *Understanding Privacy*, s. 12, 13; Cate, *The Privacy Problem*, s. 2, Solove, Schwartz, *Privacy, Information, and Technology*, s. 40, 41; Etzioni, *a.g.e.*, s. 200-203; Labor C. Velecky, "The Concept of Privacy", *Privacy*, Ed. by. John B. Young, USA, John Wiley&Sons, 1978, s. 17-22.

Her bir yaklaşımın belirli yönlerini göz önünde bulundurarak ve kavramsallaştırma kaygısına kapılmadan, özel yaşamın gizliliğini kişilerin, kendilerine ait bilgiyi ne zaman, ne şekilde ve ne kapsamda başkalarıyla paylaşacaklarını belirleyebilmelerine ilişkin taleplerinin korunması olarak ifade etmek yerinde görülebilir. Fakat unutulmamalıdır ki, önemli olan bu anlatımı dahi sınırlı bir tanımlama olarak kabul etmeden onun esaslı noktalarına, iletişimin gizliliği bakımından da yol gösterici olabilecek şekilde, dikkat çekebilmektir. Bu anlatımda her ne kadar kişinin bilgi üzerindeki kontrol imkanı temel çıkış noktası olsa da, özel yaşamın gizliliğinin üç esaslı nokta işaret ettiği kabul edilmektedir. Kişiye kendisine ait bir münhasır alan bırakma, başkalarının müdahalelerine imkan vermeden kişinin kendi başına karar alabilme bağımsızlığı ve kendi etrafında dönen - ona ulaşan ve onun ulaştırdığı - bilgi üzerindeki kontrolü olarak özetlenebilir.¹⁴⁸

Özel yaşamın gizliliğinin kavramsallaştırılmasının belirsiz, ucu açık ve hatta kimi zaman tartışmalı bir sonuca götürebilmesinin bir diğer nedeni olarak, özel yaşamın gizliliğinin sosyal yönünün olması da gösterilebilir. Özel yaşamın gizliliğine olan ihtiyacın ve özel yaşamın gizliliğinin şekillenmesinin sadece dönemlere değil, toplumlara ve gelişmişlik düzeylerine göre de değiştiği görülür.¹⁴⁹ Aslında özel yaşamın gizliliğinin, toplumsal gereklilik ile yaratılmış olduğundan, tekrar toplumsal farklılık ve gerekliliklere göre de değişen bir şey olması beklenebilir bir husustur.¹⁵⁰ Bu bağlamda, açıkça görülür ki, A.B.D. ve Kıta Avrupası hukuku, özel yaşamın gizliliği kavramına ve hatta korunması yönünde politika oluşturulmasına - uygulandıkları toplumların farklılıkları ve bu farklılıkların özel yaşamın gizliliğinden ne anladıklarına yansımalarından dolayı - farklı yaklaşmaktadırlar.¹⁵¹

¹⁴⁸ Bennett, a.g.e., s. 13.

¹⁴⁹ Etzioni, a.g.e., s. 200, 201.

¹⁵⁰ Cate, *Privacy in the Information Age*, s. 22.

¹⁵¹ Cate, *Privacy in the Information Age*, s. 22.

III. ÖZEL YAŞAMIN GİZLİLİĞİ AÇISINDAN AVRUPA BİRLİĞİ ve A.B.D. HUKUKUNUN YAKLAŞIM FARKLILIĞI

Özel yaşamın gizliliği kavramı ve bu kavramın kapsamı, A.B.D.’de normatif, Avrupa Birliği mevzuatında ise daha çok tanımlayıcı açıdan ele alınmaktadır. Kültürel ve yapısal farklılık bu ayrımı da beraberinde getirmektedir. AB mevzuatında ve özellikle ilgili yönetmeliklerde, üye devletlerde ortaya çıkan bir bilginin kullanımı belirli düzenlemelerle somut olarak yasaklanırken; A.B.D’de bu korumanın daha karmaşık ve merkezi olmayan bir yaklaşıma dayandığı görülmektedir.¹⁵²

AB ve A.B.D. hukuklarının özel yaşamın gizliliği konusundaki yaklaşım farklılığı başlangıçta kendini, bu kavramı ifade etmek için kullandıkları terimlerin farklılığında gösterir. A.B.D. hukukunda özel yaşamın gizliliği kavramıyla (**privacy**) ifade edilmeye çalışılan işlevi, AB mevzuatında “veri koruması (**data protection**)”¹⁵³ kavramı görür.¹⁵⁴ Bu veri koruması mevzuatı kapsamında, sadece bilgisayara kaydedilmiş veya teknolojik veriler değil; aynı zamanda sadece el yazısı belgelerin oluşturduğu dosyalar da bulunmaktadır. Amerikan hukukunda ise özel yaşamın gizliliğinin ucu açık, belirsiz bir kavram olarak karşılandığı düşünülebilir. Hatta kavramın, bir vatandaşın yerleşme hakkına veya kürtajın bir kadının hakkı olup olmayacağına gönderme yapan her terimin yerini alacak şekilde dahi kullanılabildiği görülür.

Bir an için Amerikan hukukundaki özel yaşam kavramından daha belirli ve açık bir kavram olarak düşünülebilecek olsa da, unutulmamalıdır ki, ‘veri koruması’ aslında genel olarak özel yaşamın gizliliği konsepti yerine özel yaşam bağlamında iletişimin

¹⁵² Cate, **Privacy in the Information Age**, s. vii.

¹⁵³ Kişisel veri kavramının tanımı ve kapsamı 3. bölümde ayrıntılı bir şekilde inceleneceğinden, bu bölümde veri tanımı yapılmamıştır. Özel yaşamın gizliliği kapsamında Anglo Sakson hukukunun **privacy** (özel yaşamın gizliliği) kavramıyla ele aldığı husus, genelde Kıta Avrupası özelde de Avrupa Birliği üyesi devletlerin hukuklarında **data protection** (veri koruması) ile ifade edildiğinden, bu bölümde veri kavramı kullanmıştır. Fakat burada ifade edilen veri kavramı ile üçüncü bölümde açıklanan kişisel veriler aynı şeyi ifade ettiğinden; kavramın açıklanması üçüncü bölüme bırakılmıştır.

¹⁵⁴ Bennett, **a.g.e.**, s. 13, Abu Bakar Munir, Siti Hajar Mohd. Yasin, **Privacy and Data Protection, a Comparative Analysis with Special Reference to the Malaysian Proposed Law**, Malaysia, Sweet&Maxwell, 2002, s. 14, 15.

gizliliği kavramını karşılar bir nitelik taşır. Amerikan hukuku bakımından, özellikle de Westin'in yukarıda ifade de edilen ve daha çok özel yaşam bağlamında iletişimin gizliliğini açıklayan tanımı - kişilerin, kendilerine ait bilgiyi ne zaman, ne şekilde ve ne kapsamda başkalarıyla paylaşacaklarını belirleyebilmeleri - Avrupa Birliği hukukunun veri koruması ile ifade edilen anlayışına paralel görülüp, bir değerlendirme yapılabilir.¹⁵⁵ Fakat bir karşılaştırmadan öte, iki düzenin analizinin yapılması daha yerinde olabilir. Zira sadece daha önce açıklanan özel yaşama ilişkin dört yaklaşım değil; özellikle Westin'in anlayışı da Avrupalı kural koyucuları büyük oranda etkilemiştir.

Özel yaşamın gizliliğine ilişkin korumanın, yukarıda sayılan farklı anlayışların da etkisiyle neredeyse A.B.D.'de şekillendiği söylenebilse de, konunun hukuki düzenlemelere dökülmesi açısından, Avrupa'nın A.B.D.'den önce davrandığı ve çok daha ayrıntılı düzenleme yöntemini seçtiği ilk ve genel belirleme olarak ortaya konabilir. Almanya'da ortaya çıkan ilk ulusal veri koruma yasasını, 1973'de İsveç'teki konuya ilişkin bir ulusal yasa takip etti. Bugün ise, Fransa, Çek Cumhuriyeti,¹⁵⁶ Belçika,¹⁵⁷ İspanya,¹⁵⁸ İngiltere,¹⁵⁹ İsveç,¹⁶⁰ Avusturya, Danimarka, Finlandiya gibi Avrupa Birliği'ne üye devletler, kapsamlı özel yaşamın gizliliği veya veri koruması düzenlemelerine sahiptirler.¹⁶¹

¹⁵⁵ Bennett, *a.g.e.*, s. 13, 14.

¹⁵⁶ Consolidated Version of the Personal Data Protection Act on the Protection of Personal Data and on Amendment to Some Acts, Act 101, 4 Nisan 2000, (Çevrimiçi) http://ec.europa.eu/justice/policies/privacy/docs/implementation/czech_republic_act_101_en.pdf, 1 Şubat 2012.

¹⁵⁷ Consolidated text of the Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998 implementing Directive 95/46/EC, Unofficial English translation by K. Buyens, updated by Mieke Loncke, Resmi olmayan İngilizce çeviri için bkz.: (Çevrimiçi) <http://www.law.kuleuven.be/icri/itl/12privacylaw.php>, 1 Şubat 2012.

¹⁵⁸ Organic Law 15/99 of 13 December 1999 on the Protection of Personal Data, (Çevrimiçi) <http://www.privireal.org/content/dp/spain.php>, 1 Şubat 2012.

¹⁵⁹ Data Protection Act, 1998, (Çevrimiçi) <http://www.legislation.gov.uk/ukpga/1998/29/contents>, 1 Şubat 2012.

¹⁶⁰ Personal Data Act (1998:204), 29 Nisan 1998, (Çevrimiçi) <http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf>, 1 Şubat 2012.

¹⁶¹ Cate, *Privacy in the Information Age*, s. 32, Bennett, *a.g.e.*, s. 57.

Genelde Avrupa Birliği veri koruması hukukunun özelde de bu ulusal çerçeve yasaların temelinde sahip olduğu dört özellik ise, genellikle hem özel sektöre hem kamusal makamlara uygulanması; veri toplanması, kaydedilmesi ve işlenmesi gibi geniş bir yelpazedeki davranışları içermesi; çoğunlukla bu davranışlardan birine girmek için ulusal makamlardan izin alma veya onları haberdar etme gibi bir edimde bulunma sorumluluğu yüklemesi ve verinin konusunu çok da dikkate almaksızın birtakım sınırlamaların uygulanması olarak karşımıza çıkmaktadır. Bu benzerliklerin yanı sıra, ulusal düzeyde farklılıklar da bulunmaktadır. Örneğin, İsveç ve Fransa'nın konuya ilişkin ulusal komisyonları, geniş kapsamlı yetkilere sahiptirler. Kaldı ki, Fransa'nın birçok alt komisyonu ve çalışma komisyonu bulunan Veri Koruma Kurulu, Avrupa'nın en geniş yetkiye sahip kuruluşlarından biri olarak kabul edilmektedir. Gerçi bu şekildeki fazla kurumsallaşmanın, geniş yetkili ve fazla bürokratik yapılanmaların yarattığı aksaklıklardan dolayı, her zaman özel yaşamın gizliliğini korumada da aynı genişlikte sonuç vermediği de görülebilir.¹⁶²

Fransa ve İsveç'in bu ayrıntılı ve geniş yetki veren 'düzenleyici' yapılanmasının karşısında Federal Almanya'nın ise, 'danışmacı' bir sistem benimsediği söylenebilir.¹⁶³ Nitekim Alman veri koruma müdürü, İçişleri Bakanlığı'na bağlı, onun otoritesi altında çalışan biri olarak karşımıza çıkar. Bu temsilcinin görevi, hükümeti uyarmak, ona tavsiyede bulunmak ve yardım etmek olarak belirlenmiştir. Temsilci, federal hükümet yetkililerine şikayetleri sunar ve fakat yasal olarak bağlayıcı işlem yapma yetkisi ona değil federal makamlara aittir. Böyle bir sistem Fransa'nın düzenleyici sistemi karşısında daha korumasızdır denemez belki ama özel yaşamın gizliliğine ilişkin ulusal korumanın sistemin sadece bir parçası olduğu ve sosyal ve politik baskının korumaya ilişkin adım atmada daha belirleyici olduğu söylenebilir. Ulusal sistemlerde olabilecek bu farklılıklar nedeniyledir ki, uluslararası ve bölgesel koruma mevzuatına daha fazla eğilim olmuştur.¹⁶⁴

¹⁶² Cate, **Privacy in the Information Age**, s. 33.

¹⁶³ Federal Veri Koruma Kanunu, Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), In the version published on 20 December 20, 1990 (BGBl. I 1990 S.2954), as amended by the law of 14 September, 1994 (BGBl. I S. 2325), (Çevrimiçi) <http://www.iuscomp.org/gla/statutes/BDSG.htm>, 2 Şubat 2012.

¹⁶⁴ Cate, **Privacy in the Information Age**, s. 33, 34.

Ulusal düzeydeki mevzuat düzenlemelerine paralel, çokuluslu yapılanmalarda da benzer düzenlemelerin görüldüğü söylenebilir. Örneğin, OECD (**Organization for Economic Cooperation on the Protection of Privacy**/Ekonomik Kalkınma ve İşbirliği Teşkilatı) verilerin korunması ve korumaya ilişkin ilkelerle uyumlu hükümlere sahip devletler arasında veri taşınmasına ilişkin bir Yönerge yayımlamıştır.¹⁶⁵ Unutulmamalıdır ki, Yönerge'nin hukuken bir bağlayıcılığı olmamakla beraber, ulusal düzenlemelerde farklılıklara da izin veren bir yapısı bulunmaktadır.¹⁶⁶ OECD Yönergesi'nin yayımlanmasından bir yıl sonra Avrupa Konseyi, Kişisel Verilerin Otomatik İşlenmesiyle İlgili Olarak Bireylerin Korunmasına dair 1985'te bir Sözleşme yayımladığı görülür.¹⁶⁷ OECD'nin yayımladığı Yönerge'ye benzemekle birlikte, Konsey'in bu Sözleşmesi'nin çoğunlukla kişisel bilgilerin korunmasına, özel yaşamın gizliliğini koruma anlayışıyla yaklaştığı görülür. Sözleşme, bu bilgilerin adil bir şekilde elde edilmesi ve işlenmesini; sadece yasal nedenlerle kullanılması ve depolanmasını; elde edildikleri amaca ilişkin, o amaçla uyumlu ve ilgili olmasını düzenlemektedir. Kişilere bu bağlamda, kendileriyle ilgili elde edilen bilgileri içeren dosyaların varlığını sorgulama, kopyalarını isteme ve bilgileri sildirme veya doğrulama imkanı tanınmaktadır.¹⁶⁸

Tüm bu düzenlemelere rağmen, özel yaşamın gizliliğinin korunmasının tek tip bir şekilde tam olarak sağlanmasının her zaman mümkün olmayacağı da göz önünde bulundurulmalıdır. Bunun nedenleri arasında, ulusal düzeydeki düzenlemelerden de kaynaklanan etkiler vardır. Öncelikle, bazı ulusal kişisel bilgilerin korunmasına ilişkin düzenlemelerin Avrupa Konseyi Sözleşmesi'nin kabul edilmesinden önce ortaya çıktığı görülür. Bununla birlikte, Sözleşme kendiliğinden uygulanabilirlik

¹⁶⁵ "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", (Çevrimiçi) http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html, 23 Ekim 2011.

¹⁶⁶ Part Four-National Implementation of the Guidelines, (Çevrimiçi) http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html, 23 Ekim 2011.

¹⁶⁷ Council of Europe - ETS no. 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981, (Çevrimiçi) <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>, 23 Ekim 2011.

¹⁶⁸ Chapter II, Basic Principles for Data Protection, ETS no. 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

gücüne sahip olmadığından, üyesi olan her devletin Sözleşme’de farklılaşan konularda kendi hukuklarını uygulama olanağını düzenler.¹⁶⁹ Son olarak da, Sözleşme’nin özel yaşamın gizliliği bağlamında kişisel bilgilerin korunmasına yoğunlaşmayı amaçladığı söylene de, hangi seviyede bir korumanın verilerin yeterli korunmasını karşılayacağı gibi unsurların açıklanmadığı ve böylece ulusal düzenlemelerin birbiriyle uyumlu olmayan tanımlamalarına fazlasıyla olanak verdiği görülebilir.¹⁷⁰

Hem OECD Yönergesi’nin hem de Sözleşme’nin izin verdiği şekilde, farklı ve birbiriyle uyumluluk göstermeyen ulusal uygulamaların etkisiyle, 1990’da Avrupa Komisyonu Kişisel Verilerin Serbest Dolaşımı ve Elde Edilmesiyle İlgili Olarak Bireylerin Korunmasına Dair Taslak Yönerge (**Directive**) kabul etti. Bu Taslak, Avrupa Birliği devletlerinin Roma Anlaşmasıyla şekillenen Avrupa Birliği’nin ortak piyasa ve ekonomik birlik yapılanmasının, 1992’de Maastricht Anlaşmasıyla siyasi birliğe doğru gidişine dair çabalarının verdiği ürünlerden biri olarak görülebilir. Bu bağlamda, ekonomik birlikten siyasal birliğe de geçiş anlayışı, özel yaşamın gizliliği bağlamında iletişimin gizliliğine ve bunun korunmasına yoğunlaşılmasını da adeta beraberinde getirmiştir. Nitekim 1992’de Avrupa Parlamentosu veri korumasına ilişkin özel ve kamu ayrımını ortadan kaldıracak şekilde, Komisyon’un önerisini değiştirdi ve Taslak Yönerge’yi onayladı. Komisyon’un değişik halini 1992’de sunduğu “(95/46) Kişisel Verilerin İşlenmesi Sürecinde Kişilerin Korunmasına ve Verilerin Serbest Dolaşımına İlişkin Avrupa Konseyi Yönergesi” 1995 yılında kabul edilerek, Avrupa Birliği’nin özel yaşamın gizliliği bağlamında veri koruması hukukuna dair temel bir nokta kazandırmıştır.¹⁷¹

¹⁶⁹ 4. ve 11. madde bu yöndeki anlayışın yansıdığı örnekler olarak görülebilir. 4. madde: Her üye taraf, veri korumasına dair bu bölümde yer alan ilkelere işlerlik kazandırmak için gerekli tedbirleri alacaktır. 11. madde: Bu bölümdeki (veri korumasına ilişkin temel ilkeleri düzenleyen bölüm-Bölüm II) maddelerin hiçbirisi, taraf devletlerin bilgilerin ait olduğu kişilere daha geniş bir koruma sağlamasını etkileyecek veya sınırlayacak şekilde görülemez, Council of Europe - ETS no. 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981, (Çevrimiçi) <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>, 23 Ekim 2011.

¹⁷⁰ Cate, **Privacy in the Information Age**, s. 35.

¹⁷¹ Bu Yönerge’nin ilgili hükümleri ile kişisel verilerin ve bu yönde özel yaşam bağlamında iletişimin gizliliğinin korunmasına dair getirdiği temel ilkeler daha ayrıntılı olarak üçüncü bölümde incelenecektir. Bu ve ilgili diğer temel hukuki düzenlemeler ve yönetmeliklere, iletişimin önleme

Genelde Avrupa Birlięi, özelde de Avrupa Birlięi üyesi devletlerin özel yaşamın gizlilięine dair yaklaşımına ilişkin genel bir bakış açısı yansıtmak bakımından, konunun hukuken başlangıç noktası olarak kabul edilen bu Yönerge'nin genel ruhuna bakmak yerinde olabilir. Yönerge, üye devletlerin uyumlu bir ekonomik birlięe doğru geçiş yaklaşımlarını ve özel yaşama ilişkin Avrupa anlayışının hukuksal temellerini yansıtan bir belge olarak karşımıza çıkmaktadır. Nitekim özel yaşamın gizlilięini bir hak olarak nitelendirmeye ilişkin duyulan baęlılık, Yönerge'nin hükümlerinde de görülebilir. Zira Avrupa Birlięi'nin hukuki yapısı ve düzenlemeler bakımından birçok açıdan yenilikçi olan bir bakış açısı getirmiştir. Bu doğrultuda Yönerge üye devletlerin gerçek kişilerin temel hak ve özgürlüklerini ve kişisel verilerin işlenmesi bağlamında özel yaşamın gizlilięi hakkının korunması gerektięini hükme bağlamıştır.¹⁷² Aslında Komisyon, Yönerge'nin taslaęını hazırlarken dahi, spesifik olarak veri korumasından öte, Birlik dahilinde kişilerin hak ve özgürlüklerinin korunması ihtiyacının bu taslaęa hayat verdięini açıklamıştı.¹⁷³ O nedenle, Avrupa Birlięi düzenlemeleri bağlamında veri korumasından bahsederken, bireylerin temel hak ve özgürlüklerine, özellikle de özel yaşamlarının gizlilięine saygı ihtiyacından bahsedildięi kabul edilir. Özel yaşamın gizlilięini bu şekilde bir hak olarak niteleyerek ve korunmasından bahsederek, aslında Yönerge'nin özel yaşamın gizlilięine dair hukuksal korumanın hem özel sektör hem de kamu bakımından deęerini artırdıęı söylenebilir. Fakat bununla birlikte, Yönerge'de dönemin mevcut otoriter rejimini önlemenin de, yine kişisel verilerle ilgili faaliyetleri denetleyebilecek kamusal makamlar yaratarak sağlanabileceęi öngörülmektedir. Aslında bu durumun dahi üye devletlerin o dönem ki sosyal koşullarını ve yaklaşımını yansıttıęı belirtilmektedir.¹⁷⁴ Nitekim Kıta Avrupası hukukuna hakim ve üye devletlerin düzenlemelerine de yansımış olan ayrıntılı düzenleme anlayışı açıkça görülür. O kadar ki, hükümetlerin günlük yaşamı

amaçlı denetlenmesi yoluyla elde edilen verilerin nitelięi ve korunması başlıklı üçüncü bölümde, kişisel veriler ayrıntılı olarak incelenirken yer verilmiştir.

¹⁷² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, m. 1 ve 2, Official Journal L 281, 23.11.1995 P.0031-0050, (Çevrimiçi) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>, 23 Ekim 2011.

¹⁷³ Spiros Simitis, **Unpublished Address, Information Privacy and the Public Interest**, Annenberg Washington Program, Aktaran Cate, **Privacy in the Information Age**, s. 42.

¹⁷⁴ Cate, **Privacy in the Information Age**, s. 44.

etkileyecek davranışları veya kimi zaman müdahaleleri, hizmetler şeklinde; örneğin Anglo Sakson hukukunun egemen olduğu İngiltere’de dahi devletin eğitimi, yerleşmeyi ve sağlık ihtiyaçlarına etkin davranışları ve düzenlemeleriyle kendini gösterir.¹⁷⁵

Anayasa’nın vatandaşların devlete karşı kullanabilecekleri temel haklarını koruduğu ve fakat devlete sınırlı sayıda aktif bir şekilde müdahale yükümlülüğü yüklediği A.B.D. yaklaşımının aksine; Avrupa anlayışı, devletleri vatandaşların hak ve özgürlükleri açısından garanti sağlayıcı olarak görür.¹⁷⁶ Kısacası, Avrupa özel yaşamın gizliliğinin korunmasını yasal düzenlemelere bağlama bakımından bir ilk olan, ilk ulusal özel yaşam yasasını barındıran ve şimdi de özel yaşam bağlamında iletişimin gizliliğine en kapsamlı koruma sağlayan bir yaklaşımla karşımıza çıkmaktadır. Bunun temelinde özel yaşamın gizliliğinin temel bir hak olarak kabul edilmesine dair genel kabulün de büyük payı vardır. Kıta Avrupası’nın geneline hakim olan bu kabul, kapsamlı ve ayrıntılı düzenleme imkanını da beraberinde getirmiştir. Kaldı ki, aslında A.B.D. anlayışının aksini oluşturacak şekilde bundan daha da düzenleyici ve ayrıntılı bir anlayışın neredeyse beklenemeyeceği söylenebilir.¹⁷⁷

Kıta Avrupası’nın özel yaşamın gizliliğinin korunması hukuku, özellikle Avrupa Birliği Anlaşmaları ve siyasi ve hukuki birliğe doğru geçiş anlayışıyla da yansıyan şekilde, kamusal yetkilerin koordinasyonuna ve merkezîyetçiliğe dayanan bir yaklaşım sergilemektedir. A.B.D. hukukunda ise, konuya yönelik yasal düzenlemelerin farklı kaynaklarda toplandığı görülebilir. Aslında Amerikan anlayışının özellikle hukuki farklılıklarda kendini gösteren temelleri incelenmeden önce esas olarak; en başta belirlediğimiz, özel yaşamın gizliliği anlayışının toplumdan topluma farklılık göstereceği, çünkü toplumsal farklılıklara ve koşullara bağlı şekillendiği tespitini bir kez daha hatırlamak gerekmektedir. Nitekim nüfusun fazlalığı ve kalabalık olarak yayılmış olması, örneğin Hindistan gibi diğer bazı

¹⁷⁵ Cate, *Privacy in the Information Age*, s. 44.

¹⁷⁶ Bennett, *a.g.e.*, s. 55-59.

¹⁷⁷ Cate, *Privacy in the Information Age*, s. 48.

devletlerle benzerlik gösterse de, özel yaşamın gizliliği kavramından ne anlaşıldığı ve nasıl düzenlendiği bu devletler arasında bile yine de farklılık gösterebilecektir.¹⁷⁸

Farklılığın, toplumsal yapıyla olduğu kadar, A.B.D.'de yerleşmiş olan siyasal ve hukuki sistemle de bağlantılı olduğu söylenebilir. Zira federal, yerel ve hatta belediye dahilindeki yöresel (**local**) kural koyucuların yetkileri arasında A.B.D. Anayasası'ndan¹⁷⁹ kaynaklanan bir hiyerarşik sıralama bulunmaktadır. Bununla birlikte, sadece federal değil yerel hükümetlere de, üçlü bir sistemle her ne kadar ayrılmış olsa da birbiriyle çakışan yasama, yürütme ve yargı işlevleri kullanmaları olanağı vermektedir. Ayrıca, yargısal kararlar (**case law**) aracılığıyla mevcut yasal düzenlemelerin ve uygulamaların yorumlanmasına imkan tanıyan bir yargısal sisteme sahip olması da bu farklılığın nedenleri arasında sayılabilir.¹⁸⁰

A.B.D. özel yaşamın gizliliği anlayışının irdelenebilmesi için A.B.D. Anayasası'nın esaslı bir nokta oluşturduğu söylenebileceği gibi aslında Anayasa'nın kendisinin değil, anayasal hakların bu noktada bir önem arz ettiği daha yerinde bir ifade olabilir. Zira Anayasa'nın federal ve yerel hükümetlerin geniş yetkilerini sınırlayan bir işlevi olduğu ve bu nedenle aslında bu makamların işlemlerinin ve yargının bu işlemlere karşı Anayasa çerçevesinde yaptığı yorum ve uygulamanın incelenmesinin tartışmaya ışık tutacağı söylenebilir.¹⁸¹

Özel yaşamın gizliliği hakkının A.B.D. Anayasası'nda garanti altına alındığı bir yönden doğru bir ifade olmakla birlikte, diğer yanıyla da - özellikle de sadece sözel olarak - gerçeği tam olarak yansıtmamaktadır. A.B.D. Anayasası'nın hiçbir yerinde, özel yaşamın gizliliği (**privacy**) geçmemekte ve değişikliklerle de (**amendments**) düzenlenmiş bir hak olarak karşımıza çıkmamaktadır. Fakat bununla birlikte, şu da

¹⁷⁸ Diffie, Landau, **a.g.e.**, s. 143.

¹⁷⁹ The Constitution of the United States of America, English original text of the Constitution of 1789, together with Amendments I to XXVII (Ratified 5-7-1992), Doc. No 110-50, House of Representatives, United States Government Printing Office, Washington, 2007.

¹⁸⁰ Cate, **Privacy in the Information Age**, s. 49, 50.

¹⁸¹ Cate, **Privacy in the Information Age**, s. 51.

unutulmamalıdır ki, özel yaşamın gizliliği Amerikan Anayasası'nın ilgili maddelerinde dolaylı olarak garanti altına alınmıştır.¹⁸²

A.B.D. Anayasası'nın Birinci Değişikliği (**First Amendment**) ifade, din ve örgütlenme özgürlüğünü korumaktadır. Üçüncü Değişiklik (**Third Amendment**), askeri güçlerin vatandaşların evlerine girerek sığınmalarına karşı, vatandaşları korurken; Dördüncü Değişiklik (**Fourth Amendment**) ise, ölçüsüz arama ve el koymaları yasaklamaktadır. Beşinci Değişiklik (**Fifth Amendment**), kişinin kendi aleyhine tanıklık yapmak üzere zorlanamayacağını düzenler. Dokuzuncu Değişiklik (**Ninth Amendment**), bazı hakların Anayasa'da sıralanmış olmasının, diğer hakların reddedilmiş anlamına gelmeyeceğini açıkça ortaya koyar. On Dördüncü Değişiklik (**Fourteenth Amendment**) ise, kimsenin hukuki usuller uygulanmadan yaşamından, özgürlüğünden ve malından yoksun bırakılamayacağını ifade ederek; kişinin özel yaşamının gizliliğine devletin müdahale etmesine karşı ayrı bir savunma daha sağlamaktadır.¹⁸³

Bu anayasal hükümlerin hiçbiri açıkça özel yaşamın gizliliğine yer vermemiş olsa da, Amerikan Yüksek Mahkemesi'nin bu düzenlemeleri, devletin faaliyetlerine karşı, özel yaşamın gizliliğini korumaya temel teşkil edecek şekilde yorumladığı görülür.¹⁸⁴ Yüksek Mahkeme, ilk defa özel yaşamın gizliliği kavramını, Boyd v. United States kararında, Fourth Amendment hükmüyle koruma altına alınan, kişinin evinin ve özel eşyalarının gerekli neden olmadıkça aranamayacağı ve el konamayacağından ve bunlar yapılırsa kişisel güvenliği, özgürlüğü ve mülkiyetinin ihlal edilmiş sayılacağı hükmü ile korunan değerden bahsederken kullanmaktadır.¹⁸⁵ Nitekim 4 yıl sonra 1890'da, Warren ve Brandeis, teknolojik gelişmelerin özel yaşamın gizliliğine

¹⁸² Ersan Şen, "Anglo Sakson Hukukunda Özel Hayatın Gizliliği ve Korunması Hakkı," **İstanbul Üniversitesi Mukayeseli Hukuk Araştırmaları Dergisi**, No:18, İstanbul, 1990, s. 85, 86.

¹⁸³ The Constitution of the United States of America, English original text of the Constitution of 1789, together with Amendments I to XXVII (Ratified 5-7-1992), Doc. No 110-50, House of Representatives, United States Government Printing Office, Washington, 2007.

¹⁸⁴ Diffie, Landau, **a.g.e.**, s. 148-152.

¹⁸⁵ Boyd v. United States, 116 U.S. 616, para 630: "The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employes of the sanctity of a man's home and the privacies of life."

hukukta da bir karşılık verilmesi gerektiği anlayışından yola çıkarak, yukarıda açıklanan Özel Yaşamın Gizliliği Hakkı başlıklı ünlü makalelerini yazarlar. Esas itibarıyla, ansızın çekilen fotoğrafların ve gazete haberi şeklindeki yayınların kişinin saklı, özel yaşam bölgelerinin işgali olduğunu belirtmektedirler. Bu bağlamda, hukukun o ana kadar, sadece fiziksel müdahalelere karşı ve mülkiyete koruma sağladığını; fakat kişinin duygu ve düşüncelerinin, iç dünyasının da dikkate alınması gerektiğini ve kişinin tek başına olabilme hakkı bağlamında özel yaşamın gizliliğinin korunması gerektiğini ifade ederler.¹⁸⁶

1928'e gelindiğinde ise Yargıç Brandeis'in gerekçesi, çoğunluğun görüşüne karşı oy halinde ortaya çıkmasına rağmen, özel yaşamın gizliliğinin korunması tartışmasına hala ışık tutacak bir bakış açısı yansıtır. Bu gerekçe *Olmstead v. United States* kararında ortaya çıkar. Karar, içki ihracatı ve dağıtım işiyle ilgilenen bir işadamı olan Roy Olmstead'ın ve ortaklarının sahip olduğu şirkette ve evlerinde sahip oldukları şirket telefon hatlarının federal yetkililerce dinlenmesiyle ilgilidir. Şirkete ve eve yakın yerlere yerleştirilen cihazlarla konuşmaların gizlice dört ay dinlenmesinden sonra, yasaklamaya rağmen yapılan içki siparişi ve dağıtımını ve şirket yetkililerinin polise verdikleri rüşvet ortaya çıkar. Bunun yanı sıra, hakim kararı olmadan izinsiz yapılan dinlemelerle elde edilen deliller Olmstead'in mahkumiyetinde önemli rol oynar. Davacılar, elde edilen delillerin kullanılmasının, şirket ortaklarını kendileri aleyhine tanık haline getirdiği için Anayasa'yı (Beşinci Değişikliği / **Fifth Amendment**)¹⁸⁷ ihlal ettiği ve bunların kullanılamayacağını ifade eder. Yüksek Mahkeme'nin 9 yargıcından 5'i ise, devlet yetkililerince telefon hatlarının dinlenmesiyle fiziksel olarak bir mekana girilmediği ve maddesel bir şeyin bulunduğu yerden alınıp götürülmediği, bir arama veya el koymanın oluşmadığı kanaatine varmışlardır.¹⁸⁸

¹⁸⁶ Warren, Brandeis, a.e.

¹⁸⁷ A.B.D. Anayasası'nın Beşinci Değişikliği, hiç kimsenin bir ceza davasında kendi aleyhine tanıklık yapmaya zorlanamayacağını garanti altına almaktadır: "No person (...) nor shall be compelled in any criminal case to be a witness against himself", Amendment 5 of the U.S. Constitution.

¹⁸⁸ *Olmstead v. United States*, 277 U.S. 438 (1928).

Çoğunluğun görüşüne karşı oy kullanan ve karşı gerekçesini yazan Brandeis ise, Anayasa ile koruma altına alınanın, bu kadar dar kapsamda bir güvence olmadığını ortaya koymaktadır. Kaldı ki, en önemlisi anayasa koyucuların, vatandaşların yaşamının sadece maddesel şeylerden oluşmadığını, onların zihinlerinin, duygu ve düşüncelerinin ve davranışlarını tek başına oluşturabilmelerine ilişkin özgürlüklerinin korunmasını da göz önünde bulundurdıklarını ifade eder. Bu bağlamda, devletin kişiye tek başına olma imkanı bırakmayan ve haklı kabul edilemeyecek her müdahalesini, dokunulabilir bir şeyin alınması veya bir yere fiziken girilmesi sonucu doğurmasa dahi Anayasa'nın ihlali olarak değerlendirmektedir.¹⁸⁹

Bu karardan yaklaşık 40 yıl sonra 1967'de, Yargıç Brandeis'in azınlıkta kalan bu görüşü Katz v. United States kararında,¹⁹⁰ Yüksek Mahkeme'nin çoğunluk görüşü olarak karşımıza çıkar. Katz aynı zamanda, Yüksek Mahkeme'nin 40 yıl önce getirdiği ve bugün hala uyguladığı özel yaşamın gizliliğinin ihlal edilip edilmediği testini de ortaya koyması bakımından, önemli başlangıç noktalarından birini oluşturmaktadır.¹⁹¹ Olayda, Federal Soruşturma Bürosu / **Federal Bureau of Investigation** (FBI)'nin şehirlerarasında yürütülen yasadışı kumar faaliyetlerini inceleyen yetkilileri, bir telefon kulübesinin dışına yerleştirdikleri bir elektronik dinleme cihazıyla Charles Katz'ın yaptığı telefon konuşmasının bir kısmını alırlar. Mahkeme ise, herhangi bir arama izni çıkarılmaya da gerek duyulmadan, bu şekilde delil etmenin, özel mülke girilmemiş olsa da, Anayasa'yı ihlal ettiği kanısına varır. Bu önemli kararında Yüksek Mahkeme, bu şekildeki bir dinlemeyle kişilerin evlerinin, belgelerinin ve üstlerinin gereksiz arama ve el koymaya konu olamayacağı ve ayrıca yetki veren izin kararının gerekli ve yeterli bir nedene dayanması gerektiğini öngören Anayasa'nın Dördüncü Değişiklik (**Fourth Amendment**) hükmüne aykırılık olduğu kanaatindedir.¹⁹²

¹⁸⁹ Olmstead v. United States, 277 U.S. 438 (1928), Dissent by Brandeis.

¹⁹⁰ Katz v. United States, 389 U.S. 347 (1967).

¹⁹¹ Street, Grant, **a.g.e.**, s. 117.

¹⁹² Katz v. United States, 389 U.S. 347 (1967).

Şu da unutulmamalıdır ki, Mahkeme, bir kişinin gerek işyerinde gerek evinde kamuya sunduğu, toplumla paylaştığı şeylerin **Fourth Amendment** hükmünün kapsamında olmadığı ayrımını ortaya koymuştur. Fakat bu ayrımla birlikte, **Fourth Amendment**'in mekanlara veya eşyalara değil, kişilere bir koruma sağlama amacıyla düzenlendiğinden hareketle, böyle bir dinleme karşısında da Anayasa'nın sağladığı korumanın devam edeceği değerlendirmesini yapmaktadır.¹⁹³ Mahkeme'ye göre, topluma açık bir yerde de olsa, kişinin 'özel' olarak kabul ettikleri, Anayasa tarafından korunmuştur.¹⁹⁴

Aslında **Fourth Amendment** hükmü bağlamında neyin özel olarak kabul edildiğine ilişkin Mahkeme'nin halen kullanacağı test de, bu kararda Yargıç Harlan'ın kararı destekleyen gerekçesiyle ortaya konulmuştur: Makul bir özel yaşamın gizliliği beklentisi (**reasonable expectation**) testi. Buna göre, **Fourth Amendment**'in koruduğu özel yaşama ilişkin o korunaklı alanı, bir kişinin kendi sübjektif beklentisi ve içinde bulunduğu toplumun ne kapsamda bu beklentiyi makul olarak karşılayabileceği ile ilgilidir.¹⁹⁵ Mahkeme'nin bir kişinin evi, işyeri, kilitlenmiş bavul ve paketlerinde beklenebilir makul bir gizlilik beklentisi olduğunu ve fakat örneğin yazı örneklerinde, banka kayıtlarında ve gizlenmiş de olsa mikrofon kayıtlarında ise böyle bir beklentisinin olamayacağını kabul ettiği görülür.¹⁹⁶ Bununla birlikte, Yargıç Harlan'ın bu yaklaşımının, teknolojinin değiştirdiği ve şekillendirdiği günlük yaşamda neredeyse her bilginin kaydedilip saklanabilmesinden dolayı eleştirildiği ve **Fourth Amendment** hükmünü günün koşullarına uygunluktan uzaklaştırdığının ileri sürüldüğü de görülür.¹⁹⁷

Tüm bu değerlendirmelere rağmen, Katz, Amerikan özel yaşamın gizliliği hukuku bakımından, Anayasadan kaynaklanan ilkelerle oluşturulan doktrinsel bir başlangıç noktası yaratmıştır. O da şöyle ifade edilebilir: Amerikan Yüksek Mahkemesi, böcek (**bug**) diye nitelendirilen gizli dinleme aracıyla dinlemeyi ve gizli telefon dinlemeyi

¹⁹³ Katz v. United States, 389 U.S. 347 (1967). Ayrıca bkz.: Street, Grant, **a.g.e.**, s. 117, 118.

¹⁹⁴ **A.e.**

¹⁹⁵ Justice Harlan, concurring, Katz v. United States, 389 U.S. 347 (1967).

¹⁹⁶ Cate, **Privacy in the Information Age**, s. 58.

¹⁹⁷ Cate, **Privacy in the Information Age**, s. 58, 59.

kabul edilebilir bir izleme ve arama yöntemi olarak kabul etmektedir ve fakat sınırlamalara tabi olduğunu ve muhtemel / olası neden (**probable cause**)¹⁹⁸ bulunması şartı dolayısıyla yargıç kararı gerektiğini ve karar çıkarılmadan bu yollarla yapılacak dinlemenin ise Anayasa'ya aykırı olduğunu ortaya koymaktadır.¹⁹⁹

Bu karara rağmen, federal yetkililerin izinsiz dinleme ve izlemelerinin devam etmesiyle birlikte, Yüksek Mahkeme 1972'de, ulusal güvenlik gerekçesiyle dahi olsa, izin almadan yapılacak dinlemeleri sona erdirecek bir karar benimsemiştir.²⁰⁰ Bu olay, **Central Intelligence Agency (CIA)**'in²⁰¹ ofislerinden birini bombalamadan dolayı suçlanan kişilerin telefonlarının, dinlenme kararı henüz çıkmadan dinlendiği ve konuşmalarının kaydedilmesi ile ilgilidir. Sanıklardan birinin telefon kayıtlarının bir kopyasını istemesi ve devlet yetkililerinin ulusal güvenlik gerekçesiyle, bunların **Fourth Amendment** koruması dışında kaldığını ileri sürerek reddetmesi üzerine Yüksek Mahkeme'ye gelmiştir. Yüksek Mahkeme bu kararında, ulusal güvenlik nedeniyle yapılan dinlemelerin Anayasa'nın koruması dışında kaldığı görüşünü benimsememiş ve ulusal güvenlik gerekçesi de söz konusu olsa, muhtemel neden bulunuyorsa, yargıç izninin alınması gerektiğini hükme bağlamıştır.²⁰²

Amerikan Yüksek Mahkemesi, 1970'li yıllarda, özel yaşamın gizliliği konusuna dair yaklaşımındaki bu gelişme ve değişikliklere rağmen, özel yaşamın gizliliği hakkı ile hassas davrandığı sosyal konular arasındaki dengeyi gözettiği ve bu tür konular söz konusu olduğunda kişinin 'özel yaşamın gizliliğine dair makul beklentilerini' daraltıcı olarak yorumladığı eleştirilerini engelleyememiştir. Hassas davrandığı bu

¹⁹⁸ A.B.D. hukukundaki reasonable suspicion makul şüphe; probable cause ise muhtemel / olası neden olarak ifade edilebilir. Türk hukukuyla kurulabilecek paralellik bakımından probable cause kavramının, basit şüpheden daha yoğun nitelikte olan makul nedeni ifade ettiği söylenebilir. Bu bağlamda, A.B.D. hukukunda arama, tutuklama, dinleme tedbirleri, diğer bir deyişle hakim kararının gerektiği tedbirler bakımından reasonable suspicion (makul şüphe) değil; probable cause şeklinde başlangıç şüphesinden yoğun olayın özelliklerinin dikkate alındığı ve somut bulgularla da desteklenmiş nitelikte muhtemel / olası nedenin arandığı söylenebilir, Harvard Hukuk Fakültesi ders notları, Introduction to American Law dersi, 4 Kasım 2010.

¹⁹⁹ Diffie, Landau, **a.g.e.**, s. 189.

²⁰⁰ United States v. United States District Court for the Eastern District of Michigan et al., 407, U.S. 297, 1972.

²⁰¹ Central Intelligence Agency, USA, (Çevrimiçi) <https://www.cia.gov/>, 29 Ocak 2012.

²⁰² United States v. United States District Court for the Eastern District of Michigan et al., 407, U.S. 297, 1972.

konuların ise alkol ve uyuşturucu ile ilgili olduğu ve genellikle yasadışı alkol ve uyuşturucu satışının önlenmesi karşısında toplumun menfaatinin korunması yönünde bir eğilim benimsediği söylenebilir. Öncelikle **Fourth Amendment** hükmünün, A.B.D. Anayasası'nda düzenlenmiş tüm anayasal haklar gibi, sadece devlet faaliyetlerine karşı bir koruma sağladığı belirtilmelidir. Yüksek Mahkeme bu bağlamda, örneğin banka kayıtları veya yazışmaları gibi üçüncü kişinin kontrol ettiği durumları kapsamadığını öngörmüştür.²⁰³

Nitekim Miller kararında²⁰⁴ Mahkeme, bir kişiye ait banka hesabı bilgilerinin ve kayıtlarının banka tarafından, federal yetkililere verilmesiyle ve buna ilişkin iznin dahi yasal olmayan arama ve izleme izni olduğuyla ilgilenir. Banka çekleri ve depozito fişleri gibi finansal kağıtlarda içerik itibarıyla özel yaşamın gizliliği beklentisi olamayacağını ileri sürer. Mahkeme'ye göre, bu belgelerin içeriği, kişinin kendisi tarafından zaten banka yetkilileri ve hatta onların alt çalışanlarıyla ticari yaşamın gerekliliği içinde paylaşılmıştır.²⁰⁵

1978'de ise, Yabancı İstihbarat Denetimi Kanunu / **Foreign Intelligence Surveillance Act** (FISA),²⁰⁶ A.B.D. vatandaşlarının ülke içinde, telefon veya radyo yoluyla yapılan iletişimin içeriğinin elektronik, mekanik veya başkaca gizli izleme yoluyla elde edilmesini kapsar.²⁰⁷ A.B.D.'de bulunan bir vatandaşla iletişim halinde olan A.B.D. vatandaşları hariç, ülke dışındaki A.B.D. vatandaşlarının iletişimine uygulanmaz. Ülkede bulunan A.B.D. vatandaşları sadece uluslararası terörizme yardım ve yataklık yapmaktan dolayı şüpheli bulunurlarsa denetime tabi olabilirler.²⁰⁸ A.B.D. vatandaşının²⁰⁹ iletişimin bir tarafı olması durumunda, FISA

²⁰³ United States v. Miller, 425 U.S. 435 (1976), Couch v. United States, 403 U.S. 322 (1973). Ayrıca bkz.: Schachter, **a.g.e.**, s. 15-20.

²⁰⁴ United States v. Miller, 425 U.S. 435 (1976); Schachter, **a.g.e.**, s. 15-20.

²⁰⁵ **A.e.**

²⁰⁶ 50 USCS § 1801.

²⁰⁷ 50 USCS § 1801 (f1).

²⁰⁸ 50 USCS § 1801 (b).

²⁰⁹ FISA kapsamında vatandaş, A.B.D. vatandaşı, hukuken sürekli oturma izni olan yabancı veya bir Amerikan şirketi olarak ifade edilmiştir, 50 USCS § 1801 (i).

kapsamında dinleme yapılabilmesi için hakim kararı gerekmektedir.²¹⁰ Karar FISA altında yapılan istihbari dinleme faaliyetleri hakkında Meclis'teki ilgili kurulları yılda iki defa bilgilendiren savcı tarafından da onaylanır ve ilgili federal yetkili tarafından uygulanır. FISA'nın uygulanmaya başlanmasından uzun bir süre sonra, yılda ortalama 500 dinleme izni çıkartılırken; 1995'e gelindiğinde hükümetin 8 bin civarında dinleme izni çıkartılması isteğinde bulunduğu ve bunlardan hiçbirinin geri çevrilmediği bilinmektedir.²¹¹ Bu durumu olumlu karşılayanlar, başvuruların yerinde isteklerle ve çok iyi hazırlandığı için geri çevrilmediğini; eleştirenler ise izin kararının, devletin isteğinin onaylandığı, tamamlanması gereken usuli bir süreç olduğunu ileri sürmektedirler.²¹²

İletişimin denetlenmesi ile ilgili başlıca ulusal düzenlemelerden sonraki ise, Elektronik İletişimin Gizliliği Kanunu / **The Electronic Communications Privacy Act** (ECPA)²¹³ 1986'da kabul edilmiştir. ECPA'da yer alan **The Pen Register Act**,²¹⁴ iletişimin gerçekleştirdiği taşınabilir cihazları değiştirerek denetimi engelleyebilme tehlikesine karşılık, muhtemel neden kanıtlanırsa, sadece spesifik olarak belirlenmiş bir yerden dinleme yapma zorunluluğunu ortadan kaldıracak şekilde izin istenmesini olanaklı kılmaktadır. Bu yasa, özellikle cep telefonu ile yapılan iletişimin denetlenmesi için izin gerekliliğini getirmiştir. Ayrıca bir telefonda aranan tüm numaraların kaydedilmesinin (**pen register**) ve bir telekomünikasyon sistemi içinde tüm sinyallerin kaydedilmesi ve izlenilmesinin (**trap and trace**) de yargıç kararı gerektireceğini düzenlemiştir. Son iki denetleme yöntemini kullanmak üzere yargıç kararını almak için ilgili federal yetkili başvurabileceği gibi, kararın çıkarılması için muhtemel neden varlığı aranmamıştır.²¹⁵

²¹⁰ Hakim kararının gerekmediği iki durum bulunmaktadır: Savaş ilanından sonra, Devlet Başkanı hakim kararına gerek olmadan Başsavcı aracılığıyla yabancı istihbarat amacıyla dinleme yapılmasına izin verebilir. Ayrıca, iletişim sadece yabancı güçler arasında ise veya yabancı güçlerin münhasır kontrolü altındaki yerdeki bireylerin konuşmaları yerine, teknik istihbarata ilişkin bir iletişim ise yine hakim kararına gerek olmamaktadır. 50 USCS § 1803, 1804.

²¹¹ Diffie, Landau, **a.g.e.**, s. 203.

²¹² Diffie, Landau, **a.y.**

²¹³ 18 USCS § 2510.

²¹⁴ The Pen Register Act, 18 USCS § 3121-3127.

²¹⁵ The Pen Register Act, 18 USCS § 3127.

1968’de yılda ortalama 400 bin civarında olan dinlenen konuşmaların sayısı düzenli olarak artarak, 2 milyona kadar ulaştı. Bununla birlikte, 1994’te sadece elektronik iletişim yoluyla denetleme için 1137 yargıç kararıyla verilen izin, 2.35 milyon konuşmanın dinlenmesiyle sonuçlanmıştır.²¹⁶

2000’lere gelindiğinde ise, iki gelişme dikkat çeker. İlki, taşınabilir cihazlarla yapılan iletişimin denetlenmesinin artmasıyken; bir diğeri de bu gelişmeye paralel olarak, devletin denetlediği iletişim sayısının da artış göstermesiydi. 2004’te müdahale edilen (**intercepted**) iletişim sayısı, 4.9 milyon civarında olurken; bunların 1 milyona yakını suç isnadıyla sonuçlanmıştır.²¹⁷

Sadece iletişimle sınırlı olmayan ve özel yaşam alanına müdahaleyi de ilgilendiren teknolojik ilerlemenin ve değişimin aslında Amerikan Yüksek Mahkemesi’nin kararlarına da aynı dönemde yansdığı görülse de; Amerikan özel yaşamın gizliliği anlayışının daha önce ifade edilen esaslarını koruduğu belirtilebilir. 2001yılındaki *Kyllo*²¹⁸ kararında Mahkeme’nin, ısı görüntüleme (**thermal-imaging**) yöntemiyle bir evin içinde yapılan çeşitli faaliyetleri - olayda marijuana yetiştiriciliğini - saptayabilmeyi **Fourth Amendment**’ın ihlali olarak kabul ettiği görülür. Bu kararında, Mahkeme’nin *Katz* kararında ortaya atılan ucu açık bir standart olarak eleştiren ‘makul bir özel yaşamın gizliliği beklentisinin’ aslında çok uzun zaman sonra da bu karara dayanak oluşturan bir nokta olduğu ifade edilebilir. Nitekim Mahkeme burada, vatandaşların rahatça elde edemeyeceği, toplumun kullanımına çok da açık olmayan ısı görüntüleme faaliyeti yaparak, evin içinde belli faaliyetlerin yoğunlaştığını saptayabilen bu cihazın kullanılmasının, eve fiziksel girmeyi gerektirmese de, **Fourth Amendment** koşulları altında değerlendirilebileceğini belirtmiştir. Bu nedenle, kişinin özel yaşamın gizliliği beklentisinin olduğu bir alana ilişkin ayrıntıları ortaya koyduğu da dikkate alınarak, hakim kararı gerektirdiği ifade edilmiştir.²¹⁹ A.B.D. hukukunda, 11 Eylül saldırısından sonra ortaya çıkan yaklaşım farklılığının bir yönüyle değişiklik getirdiği ileri sürülebileceği gibi; sorunun

²¹⁶ Diffie, Landau, **a.g.e.**, s. 213.

²¹⁷ Diffie, Landau, **a.g.e.**, s. 214, 215.

²¹⁸ *Kyllo v. United States*, 533 U.S. 27, 2001.

²¹⁹ *Kyllo v. United States*, 533 U.S. 27, 2001.

değişiklik meselesi olmadığı ve aksine devlete, yasal sorumlulukları önemsemeyerek vatandaşları kontrol etmek için yeni bir alan sağlandığı da ifade edilebilir.²²⁰

²²⁰ David Lyon, **Surveillance after September 11**, UK, Polity, 2008, s. 14, 15; Jacqueline Klosek, **The War on Privacy**, London, Praeger, 2007, s. 14.

İKİNCİ BÖLÜM

TÜRK HUKUKUNDA TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN GİZLİLİĞİ VE DENETİMİ

I. KAVRAMLAR

Elektronik iletişimdeki gelişmeler ve internet yoluyla özellikle kişilere ait birçok bilginin ulaşılabilirliğinin kolaylığı, elektronik iletişim kullanıcılarına birçok imkan yaratırken; kişisel verilerin somut ve belirli usullerle korunması gerekliliğini de beraberinde getirmektedir.²²¹ Zira günümüzde yüz yüze iletişim ve elden ulaştırılan posta yoluyla iletilen mesajlar dışında hiçbir iletişim yolu, elektronik iletişim teknolojilerinin ulaştığı yoğunluğu ve etkiyi sağlayamamaktadır. İlk bakışta sadece internette ibaret görünen ve hızla gelişmeye devam etmekte olan dijital bilgi yoğunluğu telekomünikasyon yoluyla yapılan iletişimi ve birçok ulusal ve uluslararası bilgi ağlarını kapsamaktadır. İnternet, bu gelişmelerden sadece bir tanesini ve belki de insanlar için en somut olanını oluşturmaktadır.²²² Önlenemez bir hızla devam eden tüm bu gelişmeler, özel yaşamın gizliliğine dair kavramsal tartışmalardan başlayarak, devletlerin terörle mücadele ve aynı özel yaşamın gizliliğiyle ilgili yasal ve düzenleyici işlem yapma politikalarına ve hatta toplumsal koşullara ilişkin birçok sorunu da beraberinde getirmektedir.²²³

²²¹ L.J.H.F. Garzaniti, **Telecommunications, Broadcasting and the Internet: EU Competition Law and Regulation**, 2. bs., London, Sweet&Maxwell, 2003, s. 109.

²²² Cate, **Privacy in the Information Age**, s. 6, 7.

²²³ Patrick J. McMahon, **Counterterrorism Technology and Privacy**, Cantigny Conference Series, Conference Report, USA, McCormick Tribune Foundation, 2005, s. 22-24; Paul H. Robin, Thomas M. Lenard, **Privacy and the Commercial Use of Personal Information**, USA, Kluwer Academic, 2002, s. 1-5; Julie J. McMurry, "Privacy in the Information Age: The Need for Clarity in the ECPA," **Washington University Law Quarterly**, C.LXXVIII, 2000, s. 597; Bennett, **a.g.e.**, s. 12-44.

A. İletişim

İletişim (**communication**) kelime anlamıyla, “duygu, düşünce veya bilgilerin akla gelebilecek her türlü yolla başkalarına aktarılması, bildirişim, haberleşme, komünikasyon” anlamına gelirken; teknik anlamıyla “telefon, telgraf, televizyon, radyo vb. araçlardan yararlanarak yürütülen bilgi alışverişi, bildirişim, haberleşme, muhabere, komünikasyon”²²⁴ olarak Türkçe’ye çevrilmiştir. Görülmektedir ki, haberleşme ve iletişim kelimelerinin aynı anlama gelecek şekilde beraber kullanılabilmeleri söz konusu olsa da, bu çalışma kapsamında “**communication**” kelimesinin karşılığı olarak, “haber alma, haber aktarma olgusunun karşılıklı görünümü”²²⁵ olarak tanımlanan haberleşmeyi de içine alacak şekilde, iletişim kelimesi kullanılmaktadır.

İletişim ses, görüntü, dokunma, koku ve tat alma yoluyla algılanan işaretler şeklindeki semboller aracılığıyla, kişiler veya gruplar arasındaki bilgi, duygu ve düşüncelerin alışverişi olarak ifade edilebilir.²²⁶ Bu bilgi, duygu ve düşünce alışverişinin şekli ise, iletişimin sınıflandırılmasını ve daha sonra görüleceği üzere denetlenmesini de belirleyecektir. Bu bağlamda iletişim, yüz yüze ve yüz yüze olmayan şeklinde iki grup halinde düşünülebilir. Bir araç kullanmadan veya kullanarak ve fakat aynı anda olmasa da hemen yanıt verebilme veya karşılıklı olarak bir bilgi iletebilme olanağı yaratan iletişim yüz yüze iletişim olarak kabul edilebilir. Bu bağlamda, elektronik posta (e-mail) yoluyla yapılan iletişimin de, karşılık olarak mesajların birbirine iletilme olanağı yarattığı bir iletişim olması nedeniyle yüz yüze iletişim olarak değerlendirebildiği görülmektedir.²²⁷ Buna karşılık, bu bilgi, duygu, düşünce alışverişi sürecinde bilgi alan kişinin daha sonradan da olsa, karşılıklı olarak devamında yanıt verme imkanının bulunmadığı iletişim ise yüz yüze olmayan iletişim olarak ifade edilebilir.²²⁸ Buna, posta, basın, radyo, televizyon, sinema, video

²²⁴ Büyük Türkçe Sözlük, Türk Dil Kurumu, (Çevrimiçi) <http://tdkterim.gov.tr/bts/>, 28Ekim 2011.

²²⁵ Büyük Türkçe Sözlük, Türk Dil Kurumu, (Çevrimiçi) <http://tdkterim.gov.tr/bts/>, 28Ekim 2011.

²²⁶ Kayıhan İçel, Yener Ünver, **Kitle Haberleşme Hukuku**, 8. bs., İstanbul, Beta, 2009, s. 3-5.

²²⁷ İçel/Ünver, s. 5, 6. Farklı görüş için bkz.: Seydi Kaymaz, **Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi**, Ankara, Seçkin, 2009, s. 50, dipnot 92.

²²⁸ İçel/Ünver, a.g.e., s. 5, 6, Kaymaz, a.g.e., s. 49, 50.

bantları gibi kitle iletişim araçları ile yapılan iletişim örnek olarak gösterilebilir.²²⁹ Bu şekildeki iletişim telekomünikasyon yoluyla yapılan iletişime yoğunlaştıldığı bu çalışmanın kapsamında değerlendirilmemiştir.

Gerek 5397 sayılı Kanun'da,²³⁰ Ceza Muhakemesi Kanunu'nda (CMK)²³¹ ve Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik'te (İletişimin Denetlenmesi Yönetmeliği)²³² gerekse konuya ilişkin Telekomünikasyon Yoluyla Yapılan İletişimin Tepiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığı'nın Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik'te (TİB Yönetmeliği)²³³ iletişim kavramına dair bir tanım bulunmamaktadır. Buna karşılık mülga 4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanununun Uygulanmasına İlişkin Yönetmelik,²³⁴ 4. maddesinde, “telefon, faks ve bilgisayar gibi kablolu, kablosuz veya diğer elektromanyetik sistemlerle veya tek yönlü sistemlerle alınan veya iletilen sinyaller, yazılar, resimler, görüntü veya sesler ve diğer nitelikteki verilerin nakledilmesini” iletişim olarak tanımlamıştı.²³⁵

²²⁹ İçel/Ünver, a.g.e., s. 6.

²³⁰ 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Resmi Gazete No. 25884, 23 Temmuz 2005.

²³¹ 5271 sayılı Ceza Muhakemesi Kanunu, Resmi Gazete No. 25673, 17 Aralık 2004. Çalışmada bundan sonra CMK olarak anılacaktır.

²³² Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik, Resmi Gazete No. 26434, 14 Şubat 2007. Çalışmada bundan sonra İletişimin Denetlenmesi Yönetmeliği olarak anılacaktır. Yönetmelikle ilgili değişiklikler için ayrıca 2006 yılında Yönetmelikte yapılan değişiklik bakımından 24/02/2006 tarihli, 26090 numaralı Resmi Gazete; 2007 yılında yapılan değişiklik bakımından 4/7/2007 tarihli, 26572 numaralı Resmi Gazete; 2009 yılında yapılan değişiklik bakımından 7/8/2009 tarihli, 27312 numaralı Resmi Gazete.

²³³ Telekomünikasyon Yoluyla Yapılan İletişimin Tepiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığı'nın Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik, Resmi Gazete No. 25989, 10 Kasım 2005. Çalışmada bundan sonra TİB Yönetmeliği olarak anılacaktır.

²³⁴ 4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanununun Uygulanmasına İlişkin Yönetmelik, Resmi Gazete No. 24299, 26 Ocak 2001. Bu Yönetmelik, 26513 sayılı ve 5 Mayıs 2007 tarihli 4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanununun Uygulanmasına İlişkin Yönetmeliğin Yürürlükten Kaldırılmasına Dair Yönetmelik ile yürürlükten kaldırılmıştır.

²³⁵ 4422 Sayılı Kanun, 2. maddesinde ise, dinlenebilecek veya tespit edilebilecek olan iletişimi açıklarken, “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

B. Telekomünikasyon Yoluyla Yapılan İletişim

TİB Yönetmeliği, adeta yukarıda açıklanan iletişim tanımlamasının daha da kapsamlı bir halini sunarcasına telekomünikasyon kavramını açıklar. Buna göre, Yönetmelik'te yer alan telekomünikasyon kavramının, “işaret, sembol, ses ve görüntü ile elektrik sinyallerine dönüştürülebilen her türlü verinin; kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektro-kimyasal, elektro-mekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması” olarak anlaşılması gerektiğini ifade etmiştir.²³⁶ Bu noktada telekomünikasyon kavramının aslında iletişimin tel, radyo, optik vb. elektromanyetik sistemlerle yapıldığı ve bu bağlamda iletişimi (**communication**) de kapsadığı söylenebilir.²³⁷ Bu bağlamda örneğin, radyo ve televizyon gibi kitle iletişim araçları da kavram itibariyle telekomünikasyon kapsamında kalmaktadır. Nitekim Türkiye Radyo ve Televizyon Kanunu'na göre, televizyon yayını, elektromanyetik dalgalar yoluyla halkın doğrudan alması maksadıyla yapılan, hareketli veya sabit resimlerin sesli veya sessiz kalıcı olmayan yayını;²³⁸ radyo yayını ise, elektromanyetik dalgalar yoluyla halkın doğrudan alması maksadıyla yapılan ses yayınları olarak açıklanabilir. Fakat bunlar 5397 sayılı Kanun'da düzenlenen telekomünikasyon yoluyla yapılan iletişimin denetimi kapsamında değildir.²³⁹ Nitekim radyo ve televizyon yoluyla verilen bilgiler ve yayında yapılan açıklamalar çok sayıda kişi tarafından rahatlıkla öğrenilebilecek, kamuya açık bir iletişim olarak değerlendirilebilir. Kaldı ki, kişilerin özel yaşamın gizliliğine dair makul beklentilerinin de bu iletişim araçları bakımından söz konusu olmayacağı düşünülebilir.

diğer nitelikteki bilgileri” bu kapsamda kabul ederek; dolaylı olarak bir iletişim tanımlaması vermişti denilebilir, Kanun No. 4422, Kabul Tarihi: 30 Temmuz 1999, Resmi Gazete No. 23773, 1 Ağustos 1999.

²³⁶ TİB Yönetmeliği'nin 3/r maddesi.

²³⁷ Telekomünikasyon, “haber, yazı, resim, sembol veya her çeşit bilginin tel, radyo, optik vb. elektromanyetik sistemlerle iletilmesi, bunların yayımı veya alınması, uziletişim” olarak tanımlanabilir, Büyük Türkçe Sözlük, Türk Dil Kurumu, (Çevrimiçi) <http://tdkterim.gov.tr/bts/>, 29 Ekim 2011.

²³⁸ Madde 3 (b) ve 3 (c), 2945 sayılı 11 Kasım 1983 tarihli Türkiye Radyo ve Televizyon Kanunu, (Çevrimiçi) <http://www.mevzuat.adalet.gov.tr/html/660.html>, 29 Ekim 2011.

²³⁹ Adem Sözüer, “Türkiye’de ve Karşılaştırmalı Hukukta Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi,” **İHFM**, C.LV, No:3, 1997, s. 70; Kaymaz, **a.g.e.**, s. 134.

5397 sayılı Kanun kapsamında denetimi yapılacak iletişimin, telekomünikasyon yoluyla yapılan iletişim olarak nitelendirilmesi de eleştirilebilir. Zira zaten iletişimi - tel, radyo, optik vb. elektromanyetik sistemlerle sağlanan iletişim - ifade eden telekomünikasyon, kelime anlamıyla değil; işaret, sembol, ses ve görüntüleri tel, radyo, optik vb. elektromanyetik sistemlerle iletme, almaya veya yaymaya yarayan²⁴⁰ araçları ifade etmek üzere kullanılmıştır. Bu nedenle aslında kastedilenin, tel ile yapılan ve elektronik iletişim (**wire and electronic communication**) olduğu söylenebilir.²⁴¹ Nitekim bazı yasalarımızda elektronik iletişim kullanılmakta ve fakat yönetmeliklerde açıklanan telekomünikasyon kavramıyla neredeyse aynı şekilde tanımlandığı görülmektedir. Örneğin, 5809 sayılı Elektronik Haberleşme Kanunu,²⁴² elektronik haberleşme ifadesini kullanmakla birlikte; telekomünikasyon kavramının yukarıda açıklanan tanımından farklı yapmamıştır. Elektronik haberleşme, elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması olarak düzenlenmiştir.²⁴³

Çalışmada da, CMK'nın, 5397 sayılı Kanunun ve ilgili yönetmeliklerin kullandığı şekilde telekomünikasyon kavramı kullanılacaktır. Bu kavram kullanılırken de, radyo ve televizyon gibi kitle haberleşme araçlarıyla yapılan iletişim gibi posta yoluyla ve telgraf ile yapılan iletişim de bu kapsamda değerlendirilmeyecektir. Ayrıca, kişinin konutunda uygulanamayacak şekilde, kamuya açık yerlerdeki faaliyetlerinin ve işyerinin teknik araçlarla izlenmesi, ses veya görüntü kaydının alınması işleminin de bu kapsamda kabul edilemeyeceği söylenebilir. Yüz yüze veya sözlü olarak da ortaya çıkabilecek bu iletişimin, öngörülen şekilde denetlenmesi, CMK'da gizli soruşturmacı ve teknik araçlarla izleme başlığı altında, 139 vd. maddelerinde ayrıca

²⁴⁰ Sözüer, a.y.; Kaymaz, a.y.

²⁴¹ Doktrinde uzakla haberleşme şeklinde de ifade edildiği görülmektedir, Veli Özer Özbek, M. Nihat Kanbur, Koray Doğan, Pınar Bacaksız, İlker Tepe, **Ceza Muhakemesi Hukuku**, 2. bs., Ankara, Seçkin, 2011, s. 396. (Bundan sonra Özbek ve diğerleri olarak anılacaktır.) A.B.D. hukukunda ECPA'daki telle yapılan iletişim ve elektronik iletişim ayrımı da bu bağlamda değerlendirilebilir, 18 USCS § 2510 (1) ve 18 USCS § 2510 (12).

²⁴² 5809 sayılı Elektronik Haberleşme Kanunu, Resmi Gazete No. 27050, 10 Kasım 2008.

²⁴³ 5809 sayılı Elektronik Haberleşme Kanunu'nun 3 (h) maddesi.

düzenlenmiştir.²⁴⁴ Buna karşın, örneğin telefon, faks, e-mail ve kablolu veya kablosuz birbirine bağlı bilgisayarlar ile yürütülen iletişim, telekomünikasyon yoluyla yapılan iletişim kapsamında kabul edilebilecektir.²⁴⁵

C. İletişimin Denetlenmesi

5397 sayılı Kanun,²⁴⁶ denetim kavramına ilişkin bir tanıma yer verilmemekle birlikte; Polis Vazife ve Selahiyet Kanunu, Jandarma Teşkilat, Görev ve Yetkileri Kanunu ve Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nda belirtilen görevlerin yerine getirebilmesi için, iletişimin tespit edilebileceğini, dinlenebileceğini, kayda alınabileceğini ve sinyal bilgilerinin değerlendirilebileceğini²⁴⁷ düzenlemiştir. Nitekim bu işlemlerin 'denetim' kapsamında değerlendirilmesi gerektiği söylenebilir. Bu işlemler telekomünikasyon

²⁴⁴ Ceza Muhakemesi Kanunu'nun 140. maddesi "(1) Aşağıdaki suçların işlendiği hususunda kuvvetli şüphe sebepleri bulunması ve başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir: a) Türk Ceza Kanununda yer alan; 1. Göçmen kaçakçılığı ve insan ticareti (madde 79, 80), 2. Kasten öldürme (madde 81, 82, 83), 3. Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188), 4. Parada sahtecilik (madde 197), 5. Suç işlemek amacıyla örgüt kurma (iki, yedi ve sekizinci fıkralar hariç, madde 220), 6. İhaleye fesat karıştırma (madde 235), 7. Rüşvet (madde 252), 8. Suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282), 9. Silahlı örgüt (madde 314) veya bu örgütlere silah sağlama (madde 315), 10. Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337), Suçları. b) Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (madde 12) suçları. c) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar. d) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74 üncü maddelerinde tanımlanan suçlar. (2) Teknik araçlarla izlemeye hâkim, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından karar verilir. Cumhuriyet savcısı tarafından verilen kararlar yirmidört saat içinde hâkim onayına sunulur. (3) Teknik araçlarla izleme kararı en çok dört haftalık süre için verilebilir. Bu süre gerektiğinde bir defaya mahsus olmak üzere uzatılabilir. (4) Elde edilen deliller, yukarıda sayılan suçlarla ilgili soruşturma ve kovuşturma dışında kullanılamaz; ceza kovuşturması bakımından gerekli olmadığı takdirde Cumhuriyet savcısının gözetiminde derhâl yok edilir." şeklinde bir düzenleme getirmiş ve bu madde hükümlerinin, kişinin konutunda uygulanamayacağını kabul etmiştir, 5271 sayılı Ceza Muhakemesi Kanunu, Resmi Gazete No. 25673, 17 Aralık 2004.

²⁴⁵ Nurullah Kunter, Feridun Yenisey, Ayşe Nuhoğlu, **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku**, 17. bs., İstanbul, Beta, Nisan 2010, s. 44, Mustafa Taşkın, **Adli ve İstihbari Amaçlı İletişimin Denetlenmesi**, Ankara, Seçkin, 2008, s. 75.

²⁴⁶ 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Resmi Gazete No. 25884, 23 Temmuz 2005.

²⁴⁷ Sinyal bilgilerinin değerlendirilmesini de kapsayacak şekilde, 4.7.1934 tarihli ve 2559 sayılı Polis Vazife ve Selahiyet Kanununun ek 7 nci maddesi, 10.3.1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi, 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 6 ncı maddesi'ne getirilen değişiklikler için bkz.: 5397 sayılı Kanun, Resmi Gazete No. 25884, 23 Temmuz 2005.

yoluyla yapılan iletişimin önleme amaçlı denetlenmesinin şartları ve uygulanması bölümünde ayrıntılı olarak inceleneceğinden burada sadece bu denetim şekilleriyle genel itibariyle ne kastedildiğinin belirtilmesiyle yetinilecektir.

Öncelikle, hukukumuzda denetim kavramının, çoğunlukla A.B.D hukukundaki **intercept** kelimesinin karşılığı olarak kullanıldığı ve fakat **intercept** kelimesiyle iletişimin içeriğinin de elde edilmesi kastedildiği için, tam olarak da Türk hukukunda iletişimin denetlenmesi kapsamında denetim kavramını karşılamadığı ileri sürülebilir.²⁴⁸ Zira iletişimin denetlenmesi derken, hukukumuzda iletişimin dinlenmesi ve kaydının yanı sıra iletişimin içeriğinin elde edilmediği tespit ve sinyal bilgilerinin değerlendirilmesi de ifade edilmektedir. Bu nedenle, Amerikan hukukundaki **interception** kavramının hukukumuzda kullanılan denetim kavramıyla birebir aynı anlama gelmediğini düşünmekteyiz. Fakat bu iki hukuktaki interception ve denetim işlemlerinin hiç de paralel olmadığı fikrine de²⁴⁹ katılmamaktayız.

Intercept kavramıyla, elektronik, mekanik veya başkaca araçlarla sözlü, elektronik veya tel (işitsel transferin yapıldığı telefon veya kablo teli gibi) ile yapılan iletişimin işitsel veya buna benzer elde edilen içeriğine müdahale edilerek elde edilmesi kastedilmektedir. Fakat denildiği gibi, **interception** sadece içeriğin elde edilmesini ifade eden bir denetim şekli değildir. Bununla birlikte, hukukumuzdaki denetim kavramı da her durumda, sadece iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime yönelik, içerikle hiçbir ilişkisi olmayan tespit odaklı bir işlemi ifade etmemektedir. Nitekim iletişimin tespiti ve sinyal bilgilerinin değerlendirilmesi olmasa da; iletişimin kaydedilmesi ve telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmaların dinlenmesi,²⁵⁰ iletişimin içeriğinin de elde edildiği işlemleri ifade etmektedir ve bunlar da hukukumuzda denetim kavramı kapsamında kabul edilmektedir. A.B.D. hukukunda da **intercept** kavramını karşıladığı ifade edilen en

²⁴⁸ Kaymaz, a.g.e., s. 30-35.

²⁴⁹ Kaymaz, a.g.e., s. 30-35.

²⁵⁰ İletişimin dinlenmesi ve kayda alınması, İletişimin Denetlenmesi Yönetmeliği'nin 4 (e) maddesinde, telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmaların dinlenmesi ve kayda alınması ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemleri olarak açıklanmaktadır.

yaygın örnek, işitsel transferin yapıldığı telefon ile iletişim devam ederken, telefon konuşmasının dinlenmesi ve içeriğin elde edilmesidir.²⁵¹

Türk hukukunun denetim kapsamında değerlendirdiği işlemlerin **intercept** kavramından tamamıyla farklı olduğu söylenemeyebilir. Fakat bununla birlikte Türk hukukundaki iletişimin denetlenmesi üst başlığının esasında A.B.D. hukukundaki **surveillance** kavramını yansıttığı da belirtilmelidir. Zira A.B.D. hukukunda, içeriğin elde edilip edilmediği ayrımı yapılmaksızın, örneğin bir kişiye ait görüntüsüne (**video surveillance**)²⁵² veya süregelen iletişimine müdahale edilmesini de içerir şekilde yapılan denetim surveillance kavramıyla ifade edilmektedir. Kısacası, **interception** (müdahale) yerine, **surveillance** (denetim) kavramının üst başlık olarak iletişimin denetlenmesini de kapsadığı ve bu nedenle hukukumuzda iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi şeklinde sayılan işlemlerin oluşturduğu telekomünikasyon yoluyla yapılan iletişimin denetlenmesi kavramının içeriğini karşıladığı söylenebilir. Zira kanımızca, Türk hukukunun konuya ilişkin kanun ve yönetmeliklerinde içeriğin elde edilip edilmediğine bakılmaksızın, dört işlem de aynı hükümlerde düzenlenerek, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi başlığı altında ele alınmıştır.

Denetim şekilleri son bölümde ayrıntılı olarak açıklanacak olmakla birlikte, Türk hukukunda telekomünikasyon yoluyla yapılan iletişimin hangi işlemlerle denetlenmiş sayılacağını genel olarak ifade etmek, denetim kavramının konumuz açısından ne ifade ettiğini belirlemek açısından yararlı olabilir. İletişimin tespiti, TİB Yönetmeliği'nde, içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemler olarak ifade edilmektedir.²⁵³ Bu düzenlemelerde,

²⁵¹ Solove, Schwartz, **Privacy, Information, and Technology**, s. 142, 143.

²⁵² Bir kişiye ait sessiz bir video görüntüsünün, izleme amacıyla kurulmuş kamerayla ele geçirilmesi, bir kayıtlı görüntüye müdahale (interception) veya anında ulaşım olmasa da surveillance (denetim) olarak değerlendirilmiş ve video surveillance (görüntü - video denetimi) olarak düzenlenmiştir, Solove, Schwartz, **Privacy, Information, and Technology**, s. 147.

²⁵³ TİB Yönetmeliği'nin 3/i maddesi gibi, İletişimin Denetlenmesi Yönetmeliği'nin 4/f maddesi de iletişimin tespitini aynı şekilde tanımlamaktadır.

telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmaların dinlenmesi ve kayda alınması ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemler ise, iletişimin dinlenmesi ve kayda alınması olarak açıklanmaktadır. Dinleme açısından, konuşma ile aynı anda dinlemenin; kayda alma bakımından ise, konuşma ile aynı anda kayıt yapılması bu iki denetim şeklinin temel özelliklerini oluşturur.²⁵⁴ Sinyal bilgilerinin²⁵⁵ iletişim sistemleri üzerinde bıraktığı izlerin tespit edilerek, bunlardan anlamlandırılan sonuçlar çıkarmak üzere gerçekleştirilen değerlendirme işlemleri ise sinyal bilgilerinin değerlendirilmesi olarak ifade edilmiştir.²⁵⁶

Bu işlemler gibi, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi olarak kabul edilen ve fakat CMK'da ayrı olarak düzenlenmiş olan²⁵⁷ mobil telefonun yerinin tespiti bakımından ise, CMK'nın 135. maddesinin ilk halinde şüpheli veya sanığın yakalanabilmesi için, kullanmakta olduğu mobil telefonun yerinin tespiti söz konusu iken; 135. maddede yapılan değişiklikle;²⁵⁸ kullanmakta olduğu ifadesi çıkarılmıştır. Böylece, bu tespit sadece şüpheli veya sanığın kullanmakta olduğu mobil telefon ile sınırlı kalmamakta ve şüpheli veya sanık dışında, üçüncü kişilere ait mobil telefonların da yerinin tespit edilmesini mümkün kılmaktadır.

İletişimin denetlenmesi tedbirleri, Türk hukukunda önleme (suç öncesindeki) ve adli (suç işlenmesinden sonraki) olmak üzere iki şekilde ortaya çıkmaktadır. Bu çalışma bakımından, suç işlendikten sonra delil elde etme amacıyla iletişimin (adli) denetimi şeklindeki koruma tedbiri konumuz dışında kalmakta ve asıl inceleme alanımızı istihbari faaliyet kapsamında ve suç işlenmesinin önlenmesi amacıyla telekomünikasyon yoluyla yapılan iletişimin denetlenmesi oluşturmaktadır. Adli

²⁵⁴ Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 44, 45, Kaymaz, **a.g.e.**, s. 34, 35.

²⁵⁵ Sinyal bilgisi, TİB Yönetmeliği'nin 3/p maddesinde, bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veri olarak tanımlanmıştır.

²⁵⁶ İletişimin Denetlenmesi Yönetmeliği'nin 4 (1) maddesi.

²⁵⁷ İletişimin tespiti, dinlenmesi ve kayda alınması CMK'nın 135/1 maddesinde düzenlenirken; mobil telefonun yerinin tespiti CMK m. 135/4'de düzenlenmiştir.

²⁵⁸ 5353 sayılı Ceza Muhakemesi Kanununda Değişiklik Yapılmasına Dair Kanun'un 17. maddesi, Resmi Gazete No. 25832, 1 Haziran 2005.

amaçlı, koruma tedbiri niteliğindeki iletişimin denetlenmesi CMK hükümleri,²⁵⁹ önleme amaçlı denetim ise 5397 sayılı Kanun çerçevesinde uygulanmaktadır.

CMK 135 vd. maddelerinde bir koruma tedbiri olarak iletişimin (adli) denetlenmesi ayrıntılı olarak düzenlenmiştir. Buna göre, bir suç dolayısıyla yapılan soruşturmalarda, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkanının bulunmaması durumunda bu tedbire başvurulacaktır. Önleme amaçlı iletişimin denetlenmesi bakımından ise, 5397 sayılı Kanun başta olmak üzere, 2559 sayılı Polis Vazife ve Selahiyet Kanunu (PVSK), 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu (Jandarma Kanunu) ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu (MİT Kanunu) konuya ilişkin temel yasal düzenlemeleri oluşturmaktadır.

Türk hukukunda 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu (ÇASÖMK)'nun yürürlüğe girmesinden önce iletişimin önleme amaçlı denetlenmesi, CMK'nın arama ve postada el koymaya dair hükümleri kıyas yoluyla uygulanarak gerçekleştirilmekteydi.²⁶⁰ Unutulmamalıdır ki, 4422 sayılı Kanun, hem adli hem de önleme amaçlı denetime dayanak oluşturmaktaydı; fakat aslında uygulanma şartları bakımından iki denetim türü arasında bir ayrıma yer vermemekteydi. Bununla birlikte, 4422 sayılı Kanun'a dayanılarak yapılan adli ve önleyici denetimin dahi, Kanun'un iletişimin dinlenmesi veya tespitine ilişkin hükmünün geniş yorumlanmasıyla yapıldığı söylenebilir. Zira Kanun sadece çıkar amaçlı suç örgütleriyle mücadele için çıkartılmıştı ve önleme amaçlı denetime dayanak oluşturacak şekilde uygulanan ikinci maddesi ise sadece Kanun'da öngörülen suçları işleme veya bu suçlara yardım veya aracılık ya da yataklık etme kuşkusu altında

²⁵⁹ Suçların önlenmesine ilişkin düzenlemelere dair genel esaslar ve bu bağlamda iletişimin önleme amaçlı denetlenmesi - önleme araması ve önleme el koymasında da olduğu gibi - CMK'nın 2005'te değiştirilmesiyle farklı bir rejime tabi tutulmamıştır, Bahri Öztürk, Durmuş Tezcan, Mustafa Ruhan Erdem, Özge Sırma, Yasemin F. Saygılar, Esra Alan, **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku**, Ed. by. Bahri Öztürk, 3. bs., Ankara, Seçkin, 2010, s. 466. (Bundan sonra Öztürk ve diğerleri olarak anılacaktır.)

²⁶⁰ Fatih Selami Mahmutoglu, "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi," **Polise Görev, Yetki ve Sorumluluk Veren Mevzuat Uygulamaları Eğitim Projesi (MUYEP) Tebliğleri - 2**, EGM Yayınları Katalog No: 444, Eğitim Dairesi Başkanlığı Yayın No: 43, 2008, Ankara, s. 408 vd; Sözüer, **a.g.m.**, s. 77.

bulunan kimselerin iletişimlerinin dinlenebileceğini ve tespit edilebileceğini düzenlemektedir.

Kısacası, 4422 sayılı Kanun'un 1999 yılında, iletişimin denetlenmesini - ikinci maddesiyle - ilk defa hükme bağladığı görülmektedir. Sadece bu Kanunda öngörülen suçlara ilişkin iletişimin denetlenmesini öngörmesi nedeniyle, önleme amaçlı denetime yönelik açık bir düzenleme olarak dahi kabul edilemeyebilecek olan; önleme amaçlı denetime dayanak oluşturduğu kabul edilerek uygulanan bu Kanun da 2005 yılında yürürlükten kaldırılmıştır.²⁶¹ Bu nedenle, özel yaşamın gizliliğini ve haberleşme özgürlüğünü yakından ilgilendiren iletişimin önleme amaçlı denetlenmesinin, 2001 yılında 1982 Anayasası'nda temel hak ve özgürlüklerin sınırlandırılmasına yönelik yapılan değişikliklerle de uyumlu olarak²⁶² 5397 sayılı Kanun'un²⁶³ yürürlüğe girmesiyle, 2005 yılında yasal dayanak bulduğu söylenebilir. Nitekim Polis Vazife ve Selahiyet Kanunu, Jandarma Teşkilat, Görev ve Yetkileri Kanunu ve Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'na getirilen değişikliklerle, iletişimin önleme amaçlı denetiminin hangi şartlar altında yapılabileceği - aşağıda ayrıntılı olarak inceleneceği üzere - açıklığa kavuşturulmuştur. Buna göre, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı bakımından, CMK'nın, casusluk suçları hariç, 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların²⁶⁴ işlenmesinin önlenmesi

²⁶¹ 5320 sayılı Ceza Muhakemesi Kanununun Yürürlük ve Uygulama Şekli Hakkında Kanun'un 18/1 (d) maddesi, Resmi Gazete No. 25772, 31 Mart 2005.

²⁶² 1982 Anayasası'nın 13. maddesinin ilk düzenlemesi temel hak ve hürriyetlerin (...) Anayasanın özüne ve ruhuna uygun olarak kanunla sınırlandırabileceğini ifade ederken; 2001 yılında yapılan değişiklik, temel hak ve hürriyetlerin (...) yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlandırabileceği hükme bağlanmıştır. 2001 yılında yapılan anayasa değişiklikleriyle ilgili ayrıntılı bilgi için bkz.: Saadet Yüksel, **Constitutional Changes of Turkey in 2001 under the Framework of the EU Adaptation Process**, Annales, C.XXXIX, No:56, 2007, 153-165. Ayrıca suç işlenmesinin önlenmesi amacıyla, özel hayatın gizliliğinin sınırlandırabileceği hükme bağlanmıştır, 4709 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinin Değiştirilmesi Hakkında Kanun, m. 2 ve m. 20/2, Resmi Gazete No. 24556 Mükerrer, 17 Ekim 2001. 2001 değişikliklerini de esas alarak, temel hak ve özgürlüklerin ve bu bağlamda özel yaşamın gizliliğinin sınırlandırılması ile ilgili bkz.: Bülent Tanör, Necmi Yüzbaşıoğlu, **1982 Anayasasına Göre Türk Anayasa Hukuku**, 11. bs., İstanbul, Beta, 2012, s. 141, 147-156, 169, 170.

²⁶³ 5397 sayılı Kanun, Resmi Gazete No. 25884, 23 Temmuz 2005.

²⁶⁴ CMK m. 250 a, b ve c bentlerinde belirtilen suçlar, a) Örgüt faaliyeti çerçevesinde işlenen uyuşturucu veya uyarıcı madde imal ve ticareti suçu, b) Haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar, c) İkinci Kitap

amacıyla iletişim tespit edilebilecek, dinlenebilecek, sinyal bilgileri değerlendirilebilecek ve kayda alınabilecektir.²⁶⁵

Milli İstihbarat Teşkilatı bakımından ise, MİT Kanunu'nun "4. maddesinde belirtilen görevlerin yerine getirilmesi amacıyla Anayasanın 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 önlenmesine ilişkin olarak" bu denetimin yapılabileceği düzenlenmiştir.²⁶⁶ Bununla birlikte, gerek Polis ve Jandarma'nın gerek de MİT'in bu denetim kapsamında başvurabileceği yollardan biri olarak, teknik araçla izleme yapılabilecek olması da hükme bağlanmıştır.

CMK hükümleri çerçevesinde düzenlenen koruma tedbiri niteliğindeki iletişimin denetlenmesinden farklı olarak, önleme amaçlı denetimde, mobil telefonun yerinin tespit edilmesinin düzenlenmediği görülmektedir. Nitekim bu ayrımın temelinin, iletişimin önleme amaçlı mı yoksa koruma tedbiri amaçlı mı dinlendiğiyle ilgili bir noktada olduğu söylenebilir. Henüz hüküm verilmeden bazı temel hak ve özgürlüklerin sınırlandırılması sonucunu doğuran, geçici olarak başvuru koruma tedbiri, şüphelerin belli bir yoğunlukta olduğu hallerde söz konusu olabilir.²⁶⁷ Bununla birlikte, önleme amaçlı denetime suçun işlenmesinin önlenmesi amacıyla başvurulacakken; koruma tedbirine ise, suç delili elde etmek veya şüpheli ya da sanığın yakalanabilmesi için başvuru mobil telefonun yerinin tespitinde olduğu gibi muhakemenin yapılabilmesini sağlamak ve/veya yargılama sonunda verilen hükmün yerine getirilmesini sağlamak amacıyla başvurulur.²⁶⁸

Dördüncü Kısımın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçlar (305, 318, 319, 323, 324, 325 ve 332. maddeler hariç) olarak sayılabilir.

²⁶⁵ 5397 sayılı Kanun'un - Polis Vazife ve Salahiyet Kanunu ve Jandarma Teşkilat, Görev ve Yetkileri Kanunu'na ek maddeler getiren - 1. ve 2. maddesi.

²⁶⁶ 5397 sayılı Kanun'un - 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 6. maddesinin birinci fıkrasına değişiklik getiren - 3. maddesi.

²⁶⁷ Öztürk ve diğerleri, a.g.e., s. 380-382.

²⁶⁸ Öztürk ve diğerleri, a.g.e., s. 469, Taşkın, a.g.e., s. 81, 82, Kaymaz, a.g.e., s. 128-132.

Önleme amaçlı ve koruma tedbiri amacıyla iletişimin denetlenmesi, uygulama koşulları ve sonuçları açısından farklılıklar göstermekle beraber; denetim kararını hakimın vermesinin²⁶⁹ öngörülmesi gibi esasa ilişkin benzerlikler de taşımaktadır. Kaldı ki, iletişimin önleme amaçlı denetlendiği sırada yetkili görevlilerin, iletişimini denetledikleri kişinin başka bir suçu işlediğine dair yeterli bilgi elde etmiş olması halinde, sadece önleme amaçlı denetime yetkili olması dolayısıyla, denetlemeye hangi şartlar altında devam edeceği gibi içiçe geçmiş soruları beraberinde getirebilir. Bu duruma ilişkin mevcut yasal düzenlemelerde bir açıklık olmamakla birlikte; gerekli diğer şartların da varlığı halinde²⁷⁰ artık koruma tedbiri kapsamında CMK bağlamında adli amaçlı denetim için, hakim kararına başvurulması gerektiği düşünülebilir. Buna rağmen unutulmamalıdır ki, Türk hukukunda, iletişimin koruma tedbiri amacıyla denetlenmesi ve - çalışmanın esas konusunu oluşturan - önleme amaçlı denetlenmesi farklı iki tedbir türünü ifade etmektedir.

II. TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN DENETLENMESİNİN ÖZEL YAŞAMIN GİZLİLİĞİ VE İLETİŞİMİN GİZLİLİĞİ BAĞLAMINDA DEĞERLENDİRİLMESİ

A. Özel Yaşamın Gizliliği Bakımından

Türk hukukunda özel yaşamın gizliliğini ifade etmek için mahremiyet kelimesi kullanılsa da, ilk bölümde ifade edildiği üzere, özel yaşamın gizliliğine ilişkin neredeyse her yaklaşımın ortak olarak belirlediği özel yaşamın koruduğu değerler göstermektedir ki, özel yaşamın gizliliği kavramı sadece mahrem olanla sınırlı kalmamaktadır. Nitekim özel yaşamın gizliliği, çoğunlukla gizlilik veya kişisel gizlilik olarak ifade edilen mahremiyet²⁷¹ kavramının ötesinde veya onu da içine alacak şekilde, kişiye ait mahrem alan bırakılması kadar, başkalarının müdahalelerine

²⁶⁹ CMK m. 135/1 ve 5397 sayılı Kanun m. 1, 2 ve 3.

²⁷⁰ Çalışmanın son bölümünde ayrıntılı olarak inceleneceği üzere, CMK'nın 135. maddesi bağlamındaki kuvvetli suç şüphesi sebeplerinin bulunması gibi şartlar bu bağlamda düşünülebilir.

²⁷¹ Büyük Türkçe Sözlük, Türk Dil Kurumu, (Çevrimiçi) <http://tdkterim.gov.tr/bts/>, 12 Kasım 2011.

imkan vermeden kendi başına karar alabilme bağımsızlığını ve ona ulaşan ve onun ulaştırdığı bilgi üzerindeki kontrolünü de içinde barındırır.²⁷² Bu nedenle çalışmada, Türk hukukunda özel yaşamın gizliliği hakkının değerlendirilmesine dair bundan sonraki açıklamalarımızda da kavramın ifade edilmesi bakımından da mahremiyet kelimesi yerine özel yaşamın gizliliği kavramı kullanılacaktır.

1. 1961 Anayasasında Özel Yaşamın Gizliliği

Kişi hak ve özgürlüklerini düzenlemeyen 1921 Anayasası'ndan sonra yürürlükte olan doğal hukukçu, liberal ve bireyci bir özgürlük anlayışı benimseyen 1924 Anayasası'nda, "Türklerin kamu hakları" başlığı altında hak ve özgürlükler düzenlenmişti.²⁷³ Fakat bağlantılı hükümler Anayasa'da bulunsa da,²⁷⁴ özel yaşamın gizliliği hakkı açıkça yer almamaktaydı. 1961 Anayasası'nda, özel hayatın korunması başlığı altında, özel yaşamın gizliliği düzenlenmiş ve adli kovuşturmanın gerektirdiği istisnalar saklı kalmak kaydıyla özel yaşamın gizliliğine dokunulamayacağı hükme bağlanmıştır.²⁷⁵ 1971 değişikliğinden sonra 1961 Anayasası'nın temel hak ve özgürlüklerin sınırlanmasına ilişkin 11. maddesinin²⁷⁶ genel sınırlama maddesi haline geldiği ve özel yaşamın gizliliği hakkının da diğer hak ve özgürlükler için geçerli rejime tabi olduğu dikkate alınırsa, özel yaşamın gizliliği hakkının 1961 Anayasası düzeninde gerek 11.maddedeki gerek bu hakkı düzenleyen 15. maddede sayılan nedenlerle²⁷⁷ sınırlanabileceği sonucu ortaya

²⁷² Bennett, a.g.e., s. 13.

²⁷³ Necmi Yüzbaşıoğlu, **Anayasa Hukukunun Temel Metinleri**, İstanbul, Beta, 2006, s. 6-31.

²⁷⁴ 1924 Anayasası'nın 70. maddesi kişi dokunulmazlığını Türklerin tabii haklarından biri olarak belirtmiş ve 71. maddede de cana, mala, ırza ve konuta hiçbir türlü dokunulamayacağını hükme bağlamıştır. Bununla birlikte kanunda yazılı usul ve haller dışında kimsenin konutuna girilemeyeceği ve üstünün aranmayacağı (madde 76) ve telgraf ve telefonla haberleşmenin gizliliğinin bozulamayacağı (madde 81) belirtilmiştir.

²⁷⁵ 1961 Anayasası, Resmi Gazete No. 10859, 20 Temmuz 1961, Yüzbaşıoğlu, **Anayasa Hukukunun Temel Metinleri**, s. 32-105. 1961 Anayasası'nın 15. maddesi için bkz.: Yüzbaşıoğlu, **Anayasa Hukukunun Temel Metinleri**, s. 36.

²⁷⁶ 1961 Anayasası'nın 11. maddesi, 1971 değişikliğiyle, temel hak ve özgürlüklerin milletiyle bütünlüğünün, Cumhuriyetin, millî güvenliğin, kamu düzeninin, kamu yararının, genel ahlâkın ve genel sağlığın korunması amacı ile veya Anayasanın diğer maddelerinde gösterilen özel sebeplerle, Anayasanın sözüne ve ruhuna uygun olarak, ancak kanunla sınırlanabileceğini hükme bağlamaktaydı, Yüzbaşıoğlu, **Anayasa Hukukunun Temel Metinleri**, s. 35.

²⁷⁷ Özel yaşamın gizliliği hakkının milli güvenlik veya kamu düzeni nedneleriyle, usulüne göre verilmiş hakim kararıyla sınırlanabileceği düzenlenmiştir (1961 Anayasası m. 15/2). Gecikmede

çıkılmaktadır.²⁷⁸ Nitekim Anayasa Mahkemesi'nin 1971 değişikliğinden önce çoğunlukla kararlarında 11. maddenin tüm temel hak ve özgürlükler için genel bir sınırlama nedeni içerdiğini hükme bağladığı görülebilse de,²⁷⁹ Anayasa'nın öngördüğü bir temel hak ve özgürlüğün yine Anayasa'nın ilgili maddesinde sınırlandırılması durumunda Anayasa'nın 11. maddesinin uygulanma yerinin olamayacağını ve tüm özgürlükler için genel bir sınırlama hükmü sayılamayacağını kabul ettiği kararlarının da²⁸⁰ olduğu söylenebilir. 1971 değişikliğinden sonra da kararlarında çoğunlukla kabul ettiği üzere, 11. maddenin adeta tüm özgürlükler için geçerli genel bir sınırlama hükmü olduğu yolundaki anlayışını devam ettirdiği görülebilir.²⁸¹ Anayasa Mahkemesi, özel yaşamın gizliliği hakkı bakımından, ilgili maddede zaten sınırlama nedenlerinin gösterilmiş ve gecikmesinde sakınca bulunması halinde yetkili mercii arama veya el koymayı yapabileceğinin düzenlenmiş olduğunu ve fakat böyle bir düzenleme getirilmese de - haberleşme özgürlüğünde olduğu gibi - 11. maddeye dayanılarak sınırlama yoluna gidilebileceğini hükme bağlamıştır.²⁸²

2. 1982 Anayasasında Özel Yaşamın Gizliliği

1982 Anayasası'nın 20. maddesi, herkesin özel hayatına saygı gösterilmesini isteme hakkına sahip olduğunu ve özel hayatın gizliliğine dokunulamayacağını güvence altına almıştır. Bir kişinin üstünün, özel kağıtları ve eşyasının da aranamayacağı ve

sakınca bulunan hallerde ise kanunla yetkili kılınan mercii de bir kişinin üstünü, özel kağıtlarını ve eşyasını arayabilecek ve el koyabilecek. Maddenin 1971 değişikliğinden önceki ilk halinde "milli güvenlik" sınırlama nedenleri arasında sayılmamış ve el koyma yasağı düzenlenmemiştir.

²⁷⁸ Tanör, Yüzbaşıoğlu, **a.g.e.**, s. 169, 170; Necmi Yüzbaşıoğlu, **Türk Anayasa Yargısında Anayasallık Bloku**, İstanbul, İ.Ü. Basımevi ve Film Merkezi, 1993, s. 210-213.

²⁷⁹ E. 1963/16, K. 1963/83, K.t. 8 Nisan 1963. Bu kararında Anayasa Mahkemesi'nin, düşünce ve kanaat özgürlüğünün hiçbir sınırlama nedeni içermemiş olmasını, bu özgürlüğü, Anayasa'nın dayandığı temel ilkelere uygun olmak ve Anayasa'nın 11 inci maddesinde gösterilen esaslar dahilinde kalmak şartıyla; her yönde sınırlayabilmek hususunda kanun koyucuya takdir hakkı tanınmış olduğu şekilde yorumlamanın uygun olacağı şeklinde bir kanaate vardığı görülmektedir. Diğer bir kararında da, Anayasa Mahkemesi'nin, (...) hak arama hürriyetinin de öteki hak ve hürriyetler gibi Anayasa'nın 11. maddesinde yazılı koşullar içinde sınırlanabileceği sonucuna vardığı görülebilir, E. 1968/61, K. 1969/23, K.t. 29 Nisan 1969.

²⁸⁰ E. 1969/31, K. 1971/3, K.t. 12 Ocak 1971.

²⁸¹ E. 1972/1, K. 1972/20, K.t. 27 Nisan 1972, E. 1977/1, K. 1977/20, K.t. 5 Nisan 1977.

²⁸² E. 1971/31, K. 1972/5, K.t. 15 ve 16 Şubat 1972, Resmi Gazete No. 14336, 14 Ekim 1972.

bunlara el konamayacağı da özel yaşamın gizliliğini garanti altına alan bu maddede hükme bağlanmıştır. 1982 Anayasası'nın 20. maddesinin ilk fıkrası, 2001 değişikliğinden önce adli soruşturma ve kovuşturmanın gerektirdiği istisnaların saklı olduğunu hükme bağlamaktaydı. Değişiklikle birlikte hükmün ilga edildiği görülmekte ve özel yaşamın gizliliği hakkının sınırlanması açısından sadece maddenin 2. fıkrasında belirtilen nedenlerin²⁸³ özel sınırlama sebepleri olarak dikkate alınması gerekmektedir. Bununla birlikte, özel yaşamın gizliliği hakkının sınırlanması bakımından, 20. maddenin ikinci fıkrasında 2001 değişikliğinden önce, kanunun açıkça gösterdiği hallerde usulüne göre verilmiş bir hakim kararı öngörülmüş iken; 2001 değişikliğinden sonra hakim kararı kanunun göstermesi koşuluna bağlı kalmayacak şekilde esaslı unsur haline getirilmiştir. Bu bağlamda, fıkranın ilk halinde bir kişinin üstünün, özel kağıtları ve eşyasının aranması ve bunlara el konulması bakımından, gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınan merciin bu kararı hakimın onayına sunması öngörülmemişken; değişiklik sonrası bu yetkili merciin yazılı emri ve bu kararın da yirmi dört saat içinde hakimın onayına sunulması zorunluluğu getirilmiştir.²⁸⁴

Türk hukukunda, 1982 Anayasası'nda gizliliği korunan özel yaşamın, bir kişinin üstü, özel kağıtları ve eşyasının aranamayacağı ve bunlara el konulamayacağını; konutunun dokunulmazlığını ve haberleşmesinin gizliliği alanlarını kapsar şekilde düşünülmesi gerektiği ileri sürülmüştür. Her ne kadar, bir kişinin üstü, özel kağıtları ve eşyasının aranamayacağı ve bunlara el konulamayacağı, özel yaşamın gizliliğine dokunulamayacağına ilişkin hükümle birlikte aynı maddede düzenlenmiş (20. madde) ve konut dokunulmazlığı (21. madde) ile haberleşme özgürlüğü (22. madde) ayrı maddelerde düzenlenmiş olsalar da; bu üç alanın özel yaşam kavramı

²⁸³ 1982 Anayasası bağlamında özel hayatın gizliliği hakkının “milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak” sınırlandırılabilceği kabul edilmiştir. Buna göre, bu özel sınırlandırma sebepleri gözetilerek; usulüne göre verilmiş hakim kararı olmadıkça, yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça kimsenin üstü, özel kağıtları ve eşyası aranamayacak ve bunlara el konulamayacaktır. Bu durumda yetkili merciin kararı yirmi dört saat içinde görevli hakimın onayına sunulacak ve hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklayacak; aksi halde, el koyma kendiliğinden kalkacaktır, 1982 Anayasası m. 20/2.

²⁸⁴ 4709 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinin Değiştirilmesi Hakkında Kanun'un 5. maddesi.

kapsamında korunması gereken alanlar ve fakat aynı zamanda ayrı birer hak olarak değerlendirilmesi gerektiği ifade edilmektedir.²⁸⁵ Nitekim bu üç maddenin ortak üst başlığı da “özel hayatın ve gizliliğin korunması” olarak karşımıza çıkmaktadır. Böylece Türk hukukunda özel yaşamın gizliliği, çalışmanın ilk bölümünde ifade edilen özel yaşamın koruduğu değerleri esas alan yaklaşımları ve hatta bu hakkın sınırlanması bakımından da Amerikan hukukunun konuya ilişkin belirleyici kararlarından olan Katz kararındaki makul bir özel yaşamın gizliliği beklentisi (**reasonable expectation**) testinin etkilerini yansıtacak şekilde açıklanabilir. Bu bağlamda Türk hukukunda da, genel geçer bir tanımlama yapmanın güç olduğu hususunda baskın bir anlayış bulunsa da,²⁸⁶ çalışmanın ilk bölümünde açıklanan, özel yaşamın gizliliğinin koruduğu değerlerin dikkate alındığı görülür.²⁸⁷

Kanımızca 1982 Anayasasında yer alan üç alanın (kişinin üstü, özel kağıtları ve eşyası, konutu, haberleşmesine dair) bağımsız bir hak olarak değerlendirilmeleri yanı sıra; aslında ilk bölümde anlatılan, özellikle Anglo Sakson hukukundaki gelişmelerle açıklık kazanmış ve benimsenmiş olan özel yaşamın koruduğu değerleri ifade ettiği düşünülebilir. Buna göre, yukarıda belirlediğimiz Anglo Sakson hukukundaki (i) kişinin tek başına olabilmesi, (ii) düşünce ve davranışlarını özgürce oluşturması ve uygulaması, (iii) kişinin kendine ait bilgiyi ve böylece başkalarıyla olan ilişkisini de kontrol edebilmesi ve (iv) başkalarının kendisine ne kadar ulaşmasını ve başkalarının ilgilerine ne kadar konu olmayı istediğini belirleyebilmesi şeklindeki korunan değerlerin, 1982 Anayasası’nda da paralel bir şekilde ortaya çıktığı görülebilir. 1982 Anayasası’nda korunan kişinin üstü, özel kağıtları ve eşyasının, konutu ve haberleşmesinin bu korunan değerlerle aynı içeriği karşılayacak şekilde karşımıza çıktığı söylenebilir.

Sadece bu üç alanın özel yaşamın gizliliğiyle ilgili olduğunu söylemek de çok da yerinde bir belirleme olmayabilir. Zira 1982 Anayasası’nda özel yaşamın gizliliğiyle bağlantılı, bunlar dışında birden fazla hüküm bulunabilir. Bunların başında da,

²⁸⁵ Sultan Uzeltürk, **1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı**, İstanbul, Beta, 2004, s. 60-63.

²⁸⁶ Uzeltürk, **a.g.e.**, s. 2-4, 63; Kaymaz, **a.g.e.**, s. 73.

²⁸⁷ Uzeltürk, **a.g.e.**, s. 4-11.

kişinin yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkı (m. 17); kişi hürriyeti ve güvenliği (m. 19); düşüncüyü açıklama ve yayma özgürlüğü ve bu özgürlüğün devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının veya kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabileceğini (m. 26) öngören hükümler sayılabilir.

Özel yaşamın gizliliği hakkının özellikle 1982 Anayasası açısından değerlendirilebilmesi bakımından diğer önemli husus, öncelikle Anayasa'nın 13. maddesinin ve bu bağlamda özgürlükler rejiminin 2001 yılında uğradığı değişikliktir. Buna göre, 1982 Anayasası'nın temel hak ve özgürlüklerin sınırlanmasını düzenleyen 13. maddesinin ilk şekli, temel hak ve özgürlükler bakımından hem genel hem de özel bir sınırlama hükmü niteliğindeydi. Kaldı ki son fıkrasında, bu hususa ilişkin bir belirsizlik bırakmayacak şekilde, 13. maddede bulunan genel sınırlama sebeplerinin temel hak ve özgürlüklerin hepsi için geçerli olduğu hükme bağlanmıştı.²⁸⁸ Fakat 2001 değişikliğinden sonra, bu sisteme son verilerek, temel hak ve özgürlüklerin sadece Anayasanın ilgili maddelerinde belirtilen nedenlere bağlı olarak sınırlanabileceği düzenlenmiştir.²⁸⁹ Bu bağlamda, özel yaşamın gizliliğini düzenleyen 20. maddede belirtilen sınırlama sebepleri önem arz eder.

Esasında Anayasa'da düzenlenmiş diğer temel hak ve özgürlükler gibi özel yaşamın gizliliği hakkı için de, genel sınırlama hükmü öngören bir sistemin ortadan

²⁸⁸ 1982 Anayasası'nın 13. maddesi 2001 değişikliğinden önce, temel hak ve hürriyetlerin "Devletin ülkesi ve milletiyle bölünmez bütünlüğünün, milli egemenliğinin, Cumhuriyetin, milli güvenliğinin, kamu düzeninin, genel asayişin, kamu yararının, genel ahlakın ve genel sağlığın korunması amacı ile ve ayrıca Anayasanın ilgili maddelerinde öngörülen özel sebeplerle, Anayasanın sözüne ve ruhuna uygun olarak kanunlarla sınırlanabileceğini" öngörmekteydi. Ayrıca, bir genel sınırlama hükmü olduğuna kuşku bırakmayacak şekilde, "temel hak ve hürriyetlerle ilgili genel ve özel sınırlamaların demokratik toplum düzeninin gereklerine aykırı olamayacağı ve öngörüldükleri amaç dışında kullanılamayacağı (m. 13/2) ve bu maddede yer alan genel sınırlama sebeplerinin temel hak ve hürriyetlerin tümü için geçerli olduğu da (m. 13/3)" düzenlenmişti.

²⁸⁹ 1982 Anayasası'nın 13. maddesinde, 2001 değişikliğinden sonra, temel hak ve hürriyetlerin "özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği ve bu sınırlamaların, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı" hükme bağlanmıştır.

kaldırılması önemli olduğu gibi; özel olarak, özel yaşamın gizliliğini düzenleyen 20. maddenin 2001 değişikliği sonrasındaki hali de önemlidir. Nitekim daha önce 20. maddede yer alan ve 13. madde de sayılan genel sınırlama nedenlerine ek olarak öngörülen özel bir sınırlama nedeni olan adli soruşturma ve kovuşturmanın gerektirdiği istisnalar halinde, özel hayatın gizliliğine dokunulabileceğine ilişkin hüküm de çıkarılmıştır. Böylece, özel yaşamın gizliliğinin, milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak sınırlanabileceği hükme bağlanmıştır.

Özel yaşamın gizliliği hakkına müdahale bakımından, Türk Anayasa Mahkemesi'nin yaklaşımından önce, Amerikan Yüksek Mahkemesi'nin ve AİHM'nin kimi zaman aynı kimi zaman farklı gerekçelerle ve fakat ortak olarak kullandığı ölçütten bahsetmek Türk Anayasa Mahkemesi'nin yaklaşımı bakımından yerinde bir karşılaştırma olanağı yaratabilir. Gerek Amerikan Yüksek Mahkemesi²⁹⁰ gerek AİHM tarafından, özel yaşamın gizliliğine müdahale açısından makul bir özel yaşamın gizliliği beklentisine değinilmektedir. Nitekim Amerikan Yüksek Mahkemesi, telefonla konuşmak üzere kapıyı kapatıp bir telefon kulübesine giren kişinin ağzından çıkan her sözcüğün herkes tarafından bilinmesini istememeye hakkı olduğunu kabul eder. Bu bağlamda, kişinin, konuşmasını yaptığı telefon kulübesine herhangi bir fiziksel müdahale olmasa da, konuşmalarının gizli kalacağı beklentisinin olduğu sonucuna varır,²⁹¹

AİHM de bu beklentiye özel yaşamın gizliliği hakkına saygı açısından bir ölçüt olarak nitelendirir. Örneğin, polis istasyonunda gözaltındaki bir kişinin video kamerayla görüntülerinin alınmasının, AİHS'nin özel yaşamın gizliliği hakkına ilişkin 8. maddesini²⁹² ihlal ettiği sonucuna vardığı görülür.²⁹³ Bu yaklaşımında

²⁹⁰ Katz v. United States, 389 U.S. 347 (1967).

²⁹¹ Katz v. United States, 389 U.S. 347 (1967).

²⁹² Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi birinci fıkrasıyla "herkesin özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahip olduğunu" güvence altına alırken; ikinci fıkrasında "bu hakkın kullanılmasına bir kamu makamının müdahalesinin, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve

AIHM, gözetimindeki böyle bir kişinin makul özel yaşam beklentisine sahip olduğu iddiasını kabul etmemiştir. Mahkeme, polis istasyonundaki güvenlik kameralarının varlığından bir kişinin haberdar olmasının, bu kameraların onun gözetimindeyken uzun görüntülerinin tanığın onu teşhis etmesi ve böylece duruşma öncesi delil toplamak üzere alınması beklentisini de beraberinde getirmeyeceği sonucuna varmıştır. Bu şekilde kişiye ait bilginin toplanmasının da, özel yaşamın gizliliğine olan saygıya müdahale olduğu dile getirilmiştir.²⁹⁴

Mahkeme bir hırsızlık olayının olacağı haberini alan polisin, sokağına yerleştirdiği kameralarla düzenli izlemeye aldığı kişinin daha sonra evine de dinleme cihazı yerleştirilmesiyle ilgili olarak yaptığı değerlendirmede, kamusal bir alanda bilerek ve isteyerek de olsa bir faaliyet içinde olmasının özel yaşamın gizliliği beklentisini ortadan kaldırmadığı kanısına varmıştır. Mahkeme her şeyden önce böyle bir makul beklentinin sonuca yönelik kesin olmasa da, çok önemli bir unsur olduğunu kabul etmiştir. Aslında bu beklentinin de bir ölçüt olarak dikkate alınabilecek olmasının; özel yaşamın gizliliğinin, bir kişinin evi veya başkaca özel olarak nitelendirdiği yer dışında gerçekleştirilen işlemlerden etkilenip etkilenmeyeceği ve onun bu ortamda böyle bir müdahale beklentisi içinde olup olmadığı düşüncesine dayandığı söylenebilir.²⁹⁵

Görülüyor ki, AIHM ve Amerikan Yüksek Mahkemesi'nin her ikisi de makul özel yaşam beklentisine başvursa da, ikisinin yaklaşım farklılığı arasında bir nokta dikkat çeker. Kanımızca, makul özel yaşam beklentisine AIHM, daha çok müdahalenin

özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabileceğini" hükmüne bağlamıştır, 11 ve 14 No'lu Protokoller ile Değişik İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme ve 1, 4, 6, 7, 12 ve 13 No'lu Protokoller, Türkçe Çeviri, Avrupa İnsan Hakları Mahkemesi Yazı İşleri Müdürlüğü, Haziran 2010, s. 6.

²⁹³ Case of Perry v. The United Kingdom (Application No. 63737/00), Strasburg, Final Judgment 17 October 2003, (Çevrimiçi) <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=perry%20%7C%20UNITED%20%7C%20KINGDOM&sessionid=81828549&skin=hudoc-en>, 15 Kasım 2001.

²⁹⁴ Case of Perry v. The United Kingdom, para 37-41.

²⁹⁵ Case of P.G. and J.H. v. The United Kingdom (Application No. 44787/98), Strasburg, Final Judgment 25 December 2001, para 57, (Çevrimiçi) <http://cmiskp.echr.coe.int/tkp197/view.asp?item=5&portal=hbkm&action=html&highlight=p.g.%20%7C%20j.h.&sessionid=81832097&skin=hudoc-en>, 15 Kasım 2011; Case of Perry v. The United Kingdom, para 37. Ayrıca bkz.: Daniel J. Solove, Paul M. Schwartz, **Information Privacy Law**, 3. bs., USA, Aspen, 2009, s. 1021-1025.

sınırı ve özel yaşamın gizliliğine saygının korunması açısından yaklaşırken;²⁹⁶ Amerikan Yüksek Mahkemesi ise özel yaşamın gizliliği kavramının, anayasal koruma altındaki kapsamının belirlenmesi açısından değinmektedir.²⁹⁷

Konumuz özel yaşamın her alanı değil de, iletişimin denetlenmesi yönünden özel yaşamın gizliliği olduğu için şu da açıkça belirtilmelidir ki, iletişimin denetlenmesi bağlamında her iki anlayışta da esas itibariyle üzerinde durulan makuliyet beklentisi özel yaşamın diğer alanlarından - örneğin banka kayıtları, özel yaşamına dahil görebileceği trafikte olduğu gibi çeşitli kural ihlalleri - farklı olarak, toplumun makuliyet beklentisinden öte; kişinin haklı olarak (**justifiably**) dayanabileceği özel yaşam beklentisidir. Bu açıdan bakıldığında iki yargı düzeni de aslında bu beklentiye sahip çıkan bir yaklaşım sergiler. Bu nedenle tüm toplumun makul karşılaması kaygısından öte,²⁹⁸ her somut olayın kendi koşulları altında ilgili kişinin saygı duyulmasını beklediği özel yaşamın gizliliği, korunan esaslı unsur olarak karşımıza çıkar.

Türk hukuku bakımından ise, Anayasa Mahkemesi'nin de özel hayatın gizliliğine saygıyı koruyucu bir anlayışa sahip olduğu söylenebilir. Örneğin bir kişinin rızası olmadan hakkında bilgi toplanmasının söz konusu kişinin özel hayatını ilgilendireceğini ve özel yaşamın gizliliğini etkileyecek müdahalelerin sınırlanması gerektiğini açıkça dile getirir.²⁹⁹ 1982 Anayasası'nın ikinci kısmının ikinci bölümünde yer alan bir temel hak ve özgürlük olarak özel yaşamın gizliliği hakkı

²⁹⁶ Case of Halford v. The United Kingdom (Application No. 20605/92), Strasburg, Final Judgment 25 June 1997, para 41-60, (Çevrimiçi) <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=halford&sessionid=81891767&skin=hudoc-en>, 16 Kasım 2011; Case of Perry v. The United Kingdom, para 37-39; Case of P.G. and J.H. v. The United Kingdom 57.

²⁹⁷ Katz v. United States, 389 U.S. 347 (1967); United States v. Miller, 425 U.S. 435 (1976).

²⁹⁸ Amerikan hukuku için bkz.: Cate, **Privacy in the Information Age**, s. 59; United States v. Miller, 425 U.S. 435 (1976); United States v. White, 401 U.S. 745; Schachter, **a.g.e.**, s. 27. AİHM'nin de ilgili kararlarında, denetlenen iletişimin özel yaşamın gizliliği anlamında saygı beklentisi yaratıp yaratmaması için, mekanın kişinin evi ya da ofisi olması nedeniyle otomatik olarak özel yaşam beklentisini ortadan kaldıracığı yaklaşımıyla değil; bunların dışında da olsa o olaya özgü koşullar altında kişinin makul beklentisini dikkate alarak bir değerlendirme yaptığı görülebilir, Case of Halford v. The United Kingdom, para 45; Case of P.G. and J.H. v. The United Kingdom, para 54.

²⁹⁹ E. 2006/167, K. 2008/86, K.t. 20 Mart 2008, Resmi Gazete No. 26917, 25 Haziran 2008.

sadece yasayla düzenlenebilecektir.³⁰⁰ Bu bağlamda bu hakkın KHK, tüzük veya yönetmelik gibi yürütmenin düzenleyici işlemleriyle sınırlanabilmesi mümkün değildir.³⁰¹ Özel yaşamın gizliliği hakkını sınırlayacak yasanın kendisinin belirsiz olmama ve açık tartışmalarla hazırlanma özelliklerini taşıması gerektiği gibi, hakime aşırı takdir yetkisi bırakacak nitelikte olmaması da yasa kaydı özelliği bakımından önem arz edecektir.³⁰²

Özel yaşamın gizliliği hakkı, daha önce de ifade edildiği üzere, milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebepleriyle sınırlanabilecektir.³⁰³ Böylece 2001 değişikliğinden önce sadece kanunun açıkça gösterdiği haller denilirken; değişiklik sonrası bu nedenler açıkça sayılmıştır. Bu nedenlerden biri veya birkaçına bağlı olarak yapılacak sınırlamada uyulması gereken ilkeler ve - kanunla sınırlama gibi - Türk hukukunda özel yaşamın gizliliği hakkı bakımından sınırlamanın sınırları, Anayasa Mahkemesi'nin bu hakka ilişkin yaklaşımını anlayabilmek bakımından önem arz edebilir.

Öncelikle diğer hak ve özgürlüklerin sınırlanmasında olduğu gibi özel yaşamın gizliliği hakkı bakımından da sınırlamanın son noktası bağlamında ölçülülük ilkesi göz önünde bulundurulmalıdır. Bu ilke, 1982 Anayasası'nda anayasal norm haline getirilmeden önce dahi Anayasa Mahkemesi kararlarında yer bulan bir ölçüt olarak karşımıza çıkmaktadır.³⁰⁴ Ölçülülük ilkesi genel olarak demokratik toplum düzeninin gerekleri ve öze dokunmama ilkesinin yanında bir sınırlamanın sınırı güvencesi olarak nitelendirilebilse de, unutulmamalıdır ki, söz konusu özgürlüğün

³⁰⁰ 1982 Anayasası'nın 91. maddesinin birinci fıkrası, sıkıyönetim ve olağanüstü haller saklı kalmak üzere, Anayasanın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel haklar, kişi hakları ve ödevleri ile dördüncü bölümünde yer alan siyasi haklar ve ödevlerin kanun hükmünde kararnamelerle düzenlenemeyeceğini hükme bağlamıştır.

³⁰¹ Tanör, Yüzbaşıoğlu, **a.g.e.**, s. 147-149.

³⁰² İbrahim Ö. Kaboğlu, **Özgürlükler Hukuku**, 6. bs., İstanbul, İmge, 2002, s. 89, 90.

³⁰³ 1982 Anayasası m. 20/2.

³⁰⁴ E. 1988/50, K. 1989/27, K.t. 23 Haziran 1989, Resmi Gazete No. 20302, 4 Ekim 1989; E. 1996/68, K. 1999/1, K.t. 6 Ocak 1999, Resmi Gazete No. 24292, 19 Ocak 2001.

sınırlanmasının anayasal denetimi bakımından, sınırlamanın ölçülü olup olmadığı bu diğer iki ilkedен önce değerlendirilecektir.³⁰⁵

Özgürlüğün kural, sınırlamanın istisna olduğu anlayışından hareketle,³⁰⁶ ölçülülük, esas itibarıyla üç alt unsuru içinde barındırır: yasal önlemin sınırlama amacına ulaşmaya “elverişli” olması; sınırlayıcı önlemin sınırlama amacına ulaşma bakımından “zorunlu/gerekli” olması³⁰⁷ ve amaç ve aracın “ölçüsüz bir oranı” kapsamaması (orantılılık). Böylece özel yaşamın gizliliğinin korunması bağlamında yapılacak bir anayasa yargısı denetiminde, örneğin, “sayısı yüz binlere varan personele yer, zaman, bağlı olduğu kuruluşun yetki ve sorumluluk alanı gibi herhangi bir kayıt getirilmeksizin, yasanın diğer bir maddesine yollama suretiyle arama yetkisi verilmiş” olması ölçülü olarak nitelendirilemeyecektir.³⁰⁸

Anayasa Mahkemesi, 1982 Anayasası’nın 2001 değişikliğinden önceki halinde bir sınırlama ölçütü olmayan öze dokunma yasağını, demokratik toplum düzeninin gereklerine aykırı olmama ilkesinin sınırını belirlemede kullanmaktaydı ve bu bağlamda “anayasal değerde ilke”³⁰⁹ olarak varolduğu da kabul edilmekteydi. Nitekim genelde, sınırlamanın özgürlüğün kullanılmasını tümüyle ortadan kaldıracak düzeyde ve ağırlıkta olamayacağı şeklinde de ifade edildi.³¹⁰ 2001 değişikliklerinden sonra ise, Anayasada da yer alan öze dokunmama ilkesini, Anayasa Mahkemesi’nin

³⁰⁵ Tanör, Yüzbaşıoğlu, *a.g.e.*, s. 154, 155.

³⁰⁶ Kaboğlu, *a.g.e.*, s. 101; Tanör, Yüzbaşıoğlu, *a.g.e.*, s. 154.

³⁰⁷ Ölçülülük ilkesinin bir alt unsuru olarak gereklilik ilkesinin değerlendirilmesi bakımından Fazıl Sağlam, E. 2001/143, K. 2004/11, K.t. 10 Şubat 2004, Resmi Gazete No. 25460, 12 Mayıs 2004 kararının karşı oy yazısında, “(...) gereklilik ilkesinin de amaca ulaşma bakımından aynı derecede etkili araçlar arasından hak ve özgürlüğü en az sınırlayanın seçilmesini zorunlu kıldığını” ileri sürmektedir. Sağlam’a göre, “yasa koyucunun kişi özgürlüğünü sınırlayıcı bir önlem olarak öngöreceği suç ve cezalarda oranlılık ilkesini göz önünde tutması ve buna göre hak sahibine fiiline oranla “ölçüsüz” bir yükümlülük getirecek düzenlemelerden kaçınması gerekir. (...) işlenen eylem ile ceza arasında büyük bir oransızlık mevcuttur. (...) bu eyleme böylesine ağır bir yaptırım öngörülmesine dayanak teşkil edemez. Kaldı ki bu amaçlara ulaşmanın tek yolu hapis cezası yaptırımı da değildir. Daha sıkı bir denetimle ve buna bağlı olarak uygulanacak idari ve/veya cezai nitelikte para cezalarıyla anılan amaçlara daha etkili bir biçimde ulaşmak mümkündür. Bunun yerine anılan amaçları hapis cezasının yüksekliği ile sağlamaya yönelmek, (...) ölçülülük ilkesinin ikinci alt ilkesi olan gereklilik ilkesini de ihlal eder.”

³⁰⁸ E. 2005/43, K. 2008/143, K.t. 18 Eylül 2008, Resmi Gazete No. 27089, 23 Aralık 2008, Osman Alifeyyaz Paksüt’ün karşı oy yazısı.

³⁰⁹ Yüzbaşıoğlu, *Türk Anayasa Yargısında Anayasallık Bloku*, s. 316.

³¹⁰ E. 1987/16, K. 1988/8, K.t. 19 Nisan 1988; E. 1989/6, K. 1989/42, K.t. 7 Kasım 1989.

yine demokratik toplum düzeninin gerekleri ve ölçülük ilkesiyle birlikte kullandığı ve hakkın kullanılamaz hale gelmesi olarak nitelediği görülmektedir.³¹¹ Bununla birlikte, 1982 Anayasası dönemi açısından Anayasa Mahkemesi’nin, hangi durumlarda sınırlamanın yapılacağına açık olmaması gibi belirsiz durumlarda veya örneğin sınırlama yetkisinin kullanılacağı gecikmesinde sakınca bulunan hallerin açıkça belirlenmediği durumlarda, özel yaşamın gizliliği hakkının özünün zedelenebileceğini kabul ettiği görülür.³¹² Anayasa Mahkemesi’nin 1961 Anayasası döneminden başlayarak öz kavramını kullandığı da dikkate alınırsa, özel yaşamın gizliliği hakkının özünün bu şekilde değerlendirilmesinin aslında 1961 Anayasası dönemindeki kararlarında da yer bulduğu ileri sürülebilir.³¹³

Özel yaşamın gizliliği hakkının özüne dokunulmaması ilkesine ek olarak bu hakka yönelik yasal sınırlamanın usulüne göre verilmiş hakim kararıyla yapılacak olması ise özel yaşamın gizliliğinin korunması açısından güvence oluşturmaktadır. Buna göre, Anayasa’nın 20. maddesi bağlamında, bir kişinin üstünün, özel kağıtları ve eşyasının aranması ve bunlara el konulması hakim kararıyla gerçekleşecektir. Gecikmesinde sakınca bulunan hallerde ise, kanunla yetkili kılınan merciin yazılı emri gerekmektedir. Adli ve Önleme Arama Yönetmeliği, “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 halini” önleme aramaları bakımından gecikmesinde sakınca bulunan hal olarak açıklamıştır.³¹⁴

³¹¹ E. 2002/166, K. 2004/3, K.t. 21 Ocak 2004, Resmi Gazete No. 25510, 2 Temmuz 2004.

³¹² E. 2005/43, K. 2008/143, K.t. 18 Eylül 2008, Resmi Gazete No. 27089, 23 Aralık 2008; E. 1996/68, K. 1999/1, K.t. 6 Ocak 1999, Resmi Gazete No. 24292, 19 Ocak 2001, Karşı oy gerekçesi, Ahmet Necdet Sezer.

³¹³ Oya Araslı, Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi, Aktaran Uzeltürk, a.g.e., s. 79, 80.

³¹⁴ Adli ve Önleme Aramaları Yönetmeliği’nin 4. maddesi, Resmi Gazete No. 25832, 1 Haziran 2005.

Özel yaşamın gizliliğine müdahale yollarından birini gerçekleştirecek olan yetkili mercii savcı, kolluk veya mülki amir olacaktır. Polis Vazife ve Selahiyetleri Kanunu'nda bu mercii önleme amacıyla kişilerin üstüne, özel kağıtlarına, eşyasına ilişkin yapılacak arama açısından, gecikmesinde sakınca bulunan hallerde mülki amirin;³¹⁵ Adli ve Önleme Aramaları Yönetmeliği ise Cumhuriyet savcısının, Cumhuriyet savcısına ulaşamadığı durumlarda kolluk amirinin yazılı emri veren mercii olacağını düzenlemektedir.³¹⁶ Bu yetkinin denetlenmesi görevli hakim tarafından gerçekleştirilecektir. Nitekim, yetkili kılınan mercii karar 24 saat içinde hakim onayına sunulacaktır. İdari vesayet yetkisi tartışmalarına yol açan bu uygulamaya dair görüşler, aşağıda aynı usulün benimsendiği iletişimin gizliliği hakkında incelenecektir. Sadece bu hususun değil; özel yaşamın gizliliği hakkı ve bu hakka müdahale ile ilgili diğer birçok temel esasın genel itibarıyla, iletişimin gizliliğinde de kendini gösterdiği söylenebilir.

B. İletişimin Gizliliği Bakımından

1982 Anayasası'nın 22. maddesine göre, herkes iletişim özgürlüğüne sahiptir ve iletişimin gizliliği esastır. İletişimin denetlenmesi, sadece özel yaşamın değil aynı zamanda iletişimin de gizliliğine müdahale olarak nitelendirilmelidir. Bu bağlamda iletişim özgürlüğü ve gizliliği hem özel yaşamın gizliliğiyle, adeta onun alanlarından biri olarak ilişkili hem de Kanuni Esası'nın 1909 değişikliklerinden itibaren Anayasayla koruma altına alınmış bağımsız bir temel hak ve özgürlük olarak değerlendirilmelidir. 1982 Anayasası'nda kullanılan haberleşme kavramını, iletişim kelimesini karşılayacak şekilde³¹⁷ ve bu nedenle de telefon, faks ve bilgisayar gibi kablolu, kablosuz veya diğer elektromanyetik sistemlerle alınan veya iletilen yazılı, sözlü, resimli veya diğer nitelikteki verilerin nakledilmesi³¹⁸ şeklinde geniş bir çerçevede değerlendirmek yerinde olabilir.

³¹⁵ 5681 sayılı Polis Vazife ve Salahiyet Kanununda Değişiklik Yapılmasına Dair Kanun m. 3, 2 Haziran 2007, Resmi Gazete No. 26552, 14 Haziran 2007.

³¹⁶ Adli ve Önleme Aramaları Yönetmeliği m. 7/2.

³¹⁷ Türk Dil Kurumu, Büyük Türkçe Sözlük, (Çevrimiçi) <http://tdkterim.gov.tr/bts/>, 21 Kasım 2011.

³¹⁸ 4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu'nun 2. maddesi.

Gerek çalışma konumuz gerek de özel yaşamın bir parçası olan iletişimin değerlendirilmesi bakımından 1982 Anayasası'nda düzenlenen iletişim özgürlüğü ve gizliliğinin kapsamında, kişisel (**private**) iletişimin değerlendirilmesi gerektiği ileri sürülebilir.³¹⁹ Aslında konumuz basın, radyo ve televizyon gibi kitle iletişim (**mass communication**) araçlarıyla yapılan iletişim olmasa da, Avrupa Konseyi Parlamenterler Meclisi'nin 428 (1970) sayılı kararıyla kabul edilen Kitleli İletişim Araçları ve İnsan Hakları Bildirisi'ndeki değerlendirme de bu belirlemeye ışık tutabilir. Kararda AİHS'nin 8. maddesince korunduğu şekliyle özel yaşamın gizliliği hakkına baktığımızda, bu hakkın, “bir kişinin hayatını minimum müdahaleyle yaşama hakkı” şeklinde tanımlandığını görmekteyiz.³²⁰ Buna göre özel yaşamın gizliliği genel itibariyle kişinin kendi yaşamını en az müdahale ile sürdürmesiyle bir anlam ifade eder. Bu nedenle de bu hak özel yaşamın ve aile yaşamının korunması kadar, kişisel iletişimin kötüye kullanılmasına karşı korumayı da ifade eder.³²¹

Avrupa Parlamentosu ve Konseyi'nin 2002/58 sayılı Yönerge'si de, 2/d maddesinde, söz konusu iletişimin kamuya açık elektronik haberleşme hizmeti aracılığıyla sınırlı (**finite**) sayıda taraflar arasında değiştirilen veya iletilen her türlü bilgi anlamına geldiğini kabul etmektedir.³²² Bu kavram, bilginin ulaştığı kişiye veya tanımlanabilir bir aboneye dair olduğu durumlar hariç, bir elektronik haberleşme ağı üzerinden kamuya sunulan yayıncılık hizmetinin bir bölümü olarak iletilen bilgiyi kapsamaz.³²³

Özel yaşamın gizliliği hakkına ilişkin açıklamalarda olduğu gibi, iletişimin gizliliği hakkı bakımından da önce Türk hukukunun temel ilkeler bakımından paralellik gösterdiği AİHM anlayışının yansıtılması yerinde olabilir. Nitekim AİHM, iş veya özel amaçlı telefon konuşmalarının açıkça belirtilmiş olmasa da, AİHS'nin 8.

³¹⁹ Sözüer, **a.g.m.**, s. 70.

³²⁰ Council of European Parliamentary Assembly, Resolution 428 (1970) containing a declaration on mass communication media and human rights, C/2 maddesi, (Çevrimiçi) <http://www.assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta70/ERES428.htm#3>, 23 Kasım 2011.

³²¹ Council of European Parliamentary Assembly, Resolution 428 (1970), bölüm C.

³²² Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal of the European Communities, 31 July 2002, L 201/43.

³²³ Directive on privacy and electronic communications.

maddesi çerçevesinde “özel yaşam” ve “iletişim” kavramlarının içerisinde değerlendirilmesi gerektiğini ileri sürmektedir.³²⁴ Bunun yanı sıra, özel yaşamın gizliliği hakkı bakımından yukarıda belirttiğimiz güvenceler gibi yasallık kaydı ve demokratik toplum düzeninin gerekleriyle bağdaşıp bağdaşmadığı doğrultusunda ölçülülük ilkesinin değerlendirmesini yaptığı görülmektedir. Bu bağlamda, örneğin, ses kayıt örneklerinin elde edilmesinin de, telefon konuşmalarının içeriğine ulaşılması genel amacıyla hareket edilmiş olduğunda, hakkın koruma kapsamı dışında kalmayacağına hükmetmiştir.³²⁵

AİHM’nin uygulaması bakımından birinci aşamada, korumaya çalışılan hakkın 8. maddede koruma altına alınan özel yaşam, aile yaşamı, konut veya iletişimin gizliliği haklarından biri veya birkaçını ilgilendirip ilgilendirmediği incelenmektedir.³²⁶ Yapılan müdahalenin maddeye ilişkin koruma kapsamında olduğu belirlendikten sonra ise AİHM, alınan önlemin özel yaşamın ve/veya iletişimin gizliliğine müdahale olup olmadığını değerlendirmektedir. Burada unutulmaması gereken şudur ki, sadece alınan önlemlerin değil; belirli koşullar altında bu önlemlere yönelik kanunların da iletişimin gizliliğine müdahale niteliğinde olabileceğine karar verebilecektir.³²⁷ Kaldı ki, alınan önlemlerden bağımsız olarak, iletişimin gizli olarak denetlenmesine imkan veren yasal düzenlemelerin ve uygulamaların varlığının dahi iletişimin gizliliğine müdahale sayılabileceğini hükme bağladığı görülebilmektedir.³²⁸

Bu değerlendirmeler sonucunda, eğer söz konusu hakka bir müdahalenin olduğuna karar verilirse, değerlendirmenin ikinci aşamasına geçilir. İkinci aşamanın ilk unsuru

³²⁴ Case of Klass and others v. Germany (Application No. 5029/71), Strasbourg, 6 Eylül 1978, para 41; Case of Halford v. The United Kingdom (Application No. 20605/92) Strasbourg, 25 Haziran 1997, para 42-60.

³²⁵ Case of Halford v. The United Kingdom (Application No. 20605/92) Strasbourg, 25 Haziran 1997, para 42-60.

³²⁶ Bu değerlendirmeden sonra, AİHM - özellikle aile hayatına saygı gösterme yükümlülüğü ile ilgili olarak - pozitif yükümlülüğün söz konusu olup olmayacağına ilişkin de bir değerlendirme yapabilmektedir. Bu bağlamda, Devletin bir bireyin aile ve özel hayatına keyfi olarak negatif müdahale etmemesi şeklindeki yükümlülüğünün yanı sıra, bireylere AİHS’nin 8. maddesi’nin öngördüğü hakları sağlamak için özel hayata saygı gösterilmesini sağlayacak önlemler almasının (pozitif yükümlülük/positive obligation) öngörülebileceğini de kabul etmiştir, Case of Kroon and Others v. The Netherlands (Application No. 18535/91), Strasbourg, 27 Ekim 1994, para 35 ve 36.

³²⁷ Case of Klass and others v. Germany, para 34.

³²⁸ Case of Malone v. The United Kingdom (Application No. 8691/79), Strasbourg, 2 Ağustos 1984, para 64.

olarak müdahale, öncelikle, yasallık kaydını karşılayacak şekilde yasal dayanağa sahip olmalıdır. Bu bağlamda, AİHM, gizli olarak iletişimin denetlenmesinin, kamusal makamların dinleme yetkisinin kapsamını yeterli açıklıkta düzenleyen yasal düzenlemelerle gerçekleştirilmesi gerektiğini kabul etmektedir.³²⁹ Aksi takdirde bu nitelikleri barındırmayan idari uygulamalar ile kişilerin veya kamunun doğrudan ulaşamayacağı veya yasal olarak bağlayıcılığı olmayan ve idarenin yetki alanını muğlak bir şekilde düzenleyen kuralların bu koşulu karşılamayacağı ve keyfi denetlemeler karşısında kişiye gerekli koruma sağlamayacağı ileri sürülebilir.³³⁰

Unutulmamalıdır ki, sorun kendini sadece yasal değil de idari bir düzenleme olduğu durumlarda göstermeyecektir. Kimi durumlarda, yasanın varlığına rağmen, yasallık şartının yerine getirilmediğine karar verilmiştir. Örneğin, bir hukuk bürosunun telefon hatlarının dinlenmesi olayını değerlendirirken, dinlenenin şüpheli değil ilgili ceza kanununa göre üçüncü şahıs sıfatıyla dinlenmesini, yasanın kalitesini göz önünde bulundurarak değerlendirmiştir.³³¹ Teknolojik gelişmeler de dikkate alınarak, bir avukatın özel yaşamına ve iletişimine bu şekilde müdahaleye dayanak sağlayacak yasanın açık ve belirli olması gerektiği kabul edilmiştir. Bu noktada, sorunun bir yasanın olmaması veya bu yasanın ulaşılır olmaması değil; uygulanacak önlemin doğası ve anlamı açısından öngörülebilir olmaması olduğu ileri sürülmüştür.³³²

Öngörülebilirlik bakımından şu nokta açığa kavuşturulmalıdır ki, yasallık kaydının sağladığı öngörülebilirlik, bir kişinin yetkili kamusal makamların iletişimini ne zaman denetleyeceğini tahmin ederek, davranışlarını ona göre ayarlaması olarak anlaşılmamalıdır.³³³ Aksine, kişinin belli koşullar içinde davranışının yaratabileceği

³²⁹ Case of Malone v. The United Kingdom, para 68.

³³⁰ Case of Khan v. The United Kingdom, (Application No. 35394/97), Strasbourg, 12 May 2000, para 27; Case of Malone v. The United Kingdom, para 68; Case of Rotaru v. Romania, (Application No. 28341/95), Strasbourg, 4 May 2000, para 47-63.

³³¹ Case of Kopp v. Switzerland, (Application No. 13/1997/797/1000), Strasbourg, 25 March 1998, para 16.

³³² Case of Kopp v. Switzerland, para 62-75.

³³³ Case of Malone v. The United Kingdom, para 67.

sonuçları makul bir şekilde öngörebilmesi kastedilmektedir.³³⁴ İletişimin gizliliği bakımından bu husus, denetime dayanak sağladığı ileri sürülen hukuki düzenlemeye şöyle bir nitelik taşıma gerekliliği yüklemektedir: Söz konusu yasa, hangi koşullar altında yetkili makamların, iletişimin ve bu bağlamda özel yaşamın gizliliğinin ihlalini yaratabilecek bu gizli ve muhtemelen tehlikeli denetime başvuracağını kişinin makul bir şekilde öngörebilmesini sağlayacak açıklıkta olmalıdır.³³⁵

Müdahalenin yasaya uygunluğunun ardından, bu aşamadaki ikinci husus incelenir. Bu bağlamda müdahalenin meşru amaca dayanıp dayanmadığı değerlendirilir. Bu açıdan devletler genel itibariyle, davalarda da genelde kabul edildiği üzere ulusal güvenlik, toplumsal düzenin bozulmasının ve suç işlenmesinin önlenmesi gibi amaçları ileri sürmektedirler.³³⁶ İkinci aşamadaki incelenen son husus ise müdahalenin demokratik bir toplumda gerekli olup olmadığıdır. Bu noktada da, ölçülülük ilkesinin uygulanmasıyla kamu yararı ve kişinin hakkı arasında bir denge oluşturulması söz konusu olacaktır. Öngörülen yasal amaç açısından ölçülü olmasını da içeren demokratik toplumda gereklilik ilkesi ile müdahalenin acil bir sosyal ihtiyaç olarak ortaya çıkması gerekliliğinin vurgulandığı da ileri sürülür. Bu bağlamda, devletin yasal bir amacı koruma isteğinin, bireyin temel hak ve özgürlüğünü ölçüsüz olarak sınırlamaya izin vermeyeceği kabul edilir.³³⁷ Kaldı ki, örneğin acil toplumsal ihtiyaç söz konusu olduğunda bile, müdahaleyi haklı çıkaracak ciddilikte bir durum olmalıdır. Zira ancak böyle bir haklı nedenin, kişinin özel yaşamına zarar verecek kötü etkiler karşısında daha ağır basacağı kabul edilmektedir.³³⁸

Türk hukuku bakımından da özel yaşamın gizliliği hakkındaki hakim kararı ve yasa kaydı gibi güvencelerle sınırlamaya ilişkin esasları genel itibariyle iletişimin

³³⁴ Ursula Kilkelly, **Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı, Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesinin Uygulanmasına İlişkin Kılavuz**, İnsan Hakları El Kitapları No:1, Strasbourg, Avrupa Konseyi İnsan Hakları Genel Müdürlüğü, 2001, s. 44, 45.

³³⁵ Case of Malone v. The United Kingdom, para 67.

³³⁶ Kilkelly, **a.g.e.**, s. 52, 53.

³³⁷ John Wadham, **Human Rights and Privacy – The Balance**, speech given at Cambridge (March 2000), Aktaran Solove, Schwartz, **Information Privacy Law**, s. 1006, 1007.

³³⁸ Case of Dudgeon v. The United Kingdom, (Application No. 7525/76), Strasbourg, 22 October 1981, para 60, 61.

gizliliğinin ihlali niteliğindeki iletişimin denetlenmesinde de benzer şekillerde görebilmekteyiz. Nitekim iletişimin gizliliğine müdahale açısından, 1982 Anayasası'nın temel hak ve özgürlüklerin sınırlandırılmasına dair 13. ve haberleşme özgürlüğüne ilişkin 22. maddesini karşılamak için, yasayla düzenleme gereklidir ve fakat yeterli değildir. Bu özgürlüğün milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması nedenlerinden biri veya birkaçına bağlı olarak ve demokratik toplum düzeninin gerekleri ve ölçülülük ilkesi gibi sınırlamanın sınırı ölçütlerine aykırı olmadan sınırlandırılması gerekmektedir. Nitekim Anayasa Mahkemesi'nin de genel itibarıyla bu konuya ilişkin yaklaşımını inceleyebilmek bakımından, doğrudan sadece iletişime dair olmasa da örneğin polisin istihbarat için izleme olanağını da kapsayacak yetkilerini hangi hallerde kullanacağını düzenleyen bir yasa hükmüne ilişkin yaptığı değerlendirme göz önünde bulundurulabilir.³³⁹

Mahkeme, yasada genel ahlak ve edep kurallarına aykırı haller ve toplum düzeni bakımından tasvip edilmeme gibi kavramların kullanılmasını, içeriği açıkça anlaşılmayan kavramlara yer verilmesi olarak değerlendirmiş ve böylece polisin içeriği objektif esaslara dayanmayan, belirsiz kavramlara dayanarak müdahale yetkisini kullanabilmesine olanak tanıdığını ifade etmiştir. Kaldı ki, özgürlüğün bu şekilde sınırlandırılması ilgili temel hak ve özgürlüğün özüne dokunup, onu tümüyle kullanılamaz hale getiriyorsa, sınırlamanın demokratik toplum düzeninin gereklerine de aykırı olacağı ileri sürülmüştür.³⁴⁰

Kanımızca hakikaten de, genelde Anayasa Mahkemesi'nin 2001 değişikliklerine kadar 1982 Anayasası'nda yer almamasına rağmen öz kriterini kullanmaya devam ettiğini ve hatta demokratik toplum düzeninin gerekleriyle öze dokunmama ilkesini neredeyse aynı anlama gelecek şekilde kullandığını; özelde de iletişimin gizliliği hakkını dikkate almak gerekirse, şöyle bir değerlendirme yapmak mümkün olabilir: İletişimin gizliliğine müdahale niteliğinde sayılabilecek bir önlemin dayandığı yasal düzenlemenin keyfilik yaratabilecek, belirsiz ve yeterli açıklıkta olmayan bir

³³⁹ E. 1985/8, K. 1986/27, K.t. 26 Kasım 1986, Resmi Gazete No. 19544, 14 Ağustos 1987.

³⁴⁰ E. 1985/8, K. 1986/27, K.t. 26 Kasım 1986, Resmi Gazete No. 19544, 14 Ağustos 1987.

düzenleme olması sadece yasa kaydını değil; iletişimin gizliliğine ilişkin öz kriterini ve demokratik toplum düzeninin gerekleriyle uyumlu olma ölçütünü de zedeleyebilir.

Bu belirlemeyi yaparken; öze dokunmama güvencesiyle, sınırlamanın demokratik toplum düzeninin gereklerine aykırı olmaması güvencesinin birbirinden bağımsız olduğunu ve birbirinin yerine geçemeyeceklerini göz ardı etmemekteyiz. Fakat bununla birlikte, Anayasa Mahkemesi'nin de ifade ettiği gibi demokratik bir hukuk devletinde, güdülen amaç ne olursa olsun, özgürlük sınırlamalarının demokratik hukuk devletine özgü olmayan yöntemlerle yapılmaması ve belli bir özgürlüğün kullanılmasını ortadan kaldıracak düzeye vardırılmaması gerektiği³⁴¹ gerçeğinin de göz önünde bulundurulması gerektiğini düşünmekteyiz. Yeterli açıklıkta olmayan bir yasal düzenlemenin, uygulanması itibariyle nitelikleri farklı olan³⁴² bu iki güvence arasındaki ilişkiyi ve iletişimin gizliliğini zedeleyeceği açıktır.

C. 5397 Sayılı Kanun'un Özel Yaşamın Gizliliği ve İletişimin Gizliliği Hakkının Sınırlandırılması Açısından Değerlendirilmesi

İletişimin önleme amaçlı denetlenmesine hukukumuzda yasal dayanak sağlayan 5397 sayılı Kanun'un sayılan hususlar açısından bir değerlendirmesi yapılabilir. 5397 sayılı Kanun her şeyden önce, yasama organının usulüne göre kabul edilen ve Resmi Gazete'de yayımlanarak usulüne göre yürürlüğe girmiş³⁴³ ve alenilik kazanmış bir yasa olarak ulaşılabilir. 5397 sayılı Kanun'un, iletişimin önlenme amaçlı denetlenmesini mümkün kılacak suçları açıkça ifade ettiği görülebilir. Fakat AIHS'nin yasanın kalitesi olarak nitelendirdiği diğer unsurlarından açıklık ve

³⁴¹ E. 1985/8, K. 1986/27, K.t. 26 Kasım 1986, Resmi Gazete No. 19544, 14 Ağustos 1987.

³⁴² Öze dokunmama güvencesi, her hak ve özgürlük açısından mutlak bir koruma sağlarken; demokratik toplum düzeninin gerekleri ölçütü her hak ve özgürlük için somutlaştırılması gereken nispi bir kriter olarak değerlendirilmiştir, Tanör, Yüzbaşıoğlu, a.g.e., s. 153; Yüzbaşıoğlu, **Türk Anayasa Yargısında Anayasallık Bloku**, s. 310, 311.

³⁴³ 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun 25884 no'lu ve 23 Temmuz 2005 tarihli Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

öngörülebilirlik açısından ise,³⁴⁴ 5397 sayılı Kanun - çalışmanın son bölümünde ayrıntılarıyla görüleceği üzere - tedbirin uygulanmasına dair hükümleri bakımından yeteri kadar açıklıkta ve öngörülebilir olmadığı yönünden eleştirilebilir. Örneğin AİHM'nin Fransız hukukunun kamu hukuku sistemini (**common law system**) de benimsemediği göz önüne alınınca; yargısal kararların oluşturduğu uygulamanın değil de yasal düzenlemenin konuyu ele alması ve bu düzenlemenin de ulaşılabilirlik ve öngörülebilirlik şartları taşıması gerektiği gerekçesiyle Fransa'yı mahkum ettiği görülmektedir.³⁴⁵

Bu yönde yasanın, sadece herhangi bir ciddilik derecesinde iletişimin denetlenmesine imkan verecek şekilde değil de; şüphe derecesinin ne olacağını belirtecek, buna ilişkin kategorileri açıkça gösterecek nitelikte olması beklenmektedir.³⁴⁶ Bu bağlamda, mevcut düzenlemeyle iletişimin denetlenmesini gerçekleştirecek polis, jandarma ve istihbarat yetkililerinin kanaati büyük bir önem kazandığı için, bu yöndeki görüşlerinin objektif verilere dayanması gerekliliği aranmalıdır.

5397 sayılı Kanun, iletişimin önleme amaçlı denetlenmesinin amacı açısından, 5271 sayılı Ceza Muhakemesi Kanunu'nun 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesine işaret etmiştir. Bu bağlamda, Türk Ceza Kanunu (TCK)'nda³⁴⁷ düzenlenen 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 ve istisnaları olmakla birlikte³⁴⁸ devlet güvenliği aleyhine işlenebilecek suçların önlenmesi amacıyla iletişimin denetlenmesi

³⁴⁴ Case of Amann v. Switzerland, (Application No. 27798/95), Strasbourg, 16 February 2000, para 50; Case of Kopp v. Switzerland, para 55.

³⁴⁵ Case of Kruslin v. France, (Application No. 11801/85), Strasbourg, 24 April 1990, para 20, 28-30. Bu dava, bir cinayete ilişkin yürütülen soruşturma kapsamında dinlenen bir kişiye ait telefonu kullanan başka bir kişinin (başvurucunun) konuşmasının dinlenmesi ve aşka bir cinayete ilgili konuşmanın elde edilmesi ve bunun delil olarak kullanılmak istenmesiyle ilgilidir. Case of Huvig v. France, (Application No. 11105/84), Strasbourg, 24 April 1990, para 18, 26-29.

³⁴⁶ Ibid.

³⁴⁷ 5237 sayılı 26/09/2004 tarihli Türk Ceza Kanunu, Resmi Gazete No. 25611, Resmi Gazete tarihi: 12/10/2004.

³⁴⁸ Türk Ceza Kanunu'nun ikinci kitap dördüncü kısmının dört, beş, altı ve yedinci bölümünde tanımlanan suçlar (305, 318, 319, 323, 324, 325 ve 332. maddeler ve casusluk suçları hariç).

gerçekleştirilebilecektir. Ayrıca 2937 sayılı MİT Kanunu'nun 6. maddesine yapılan eklemeyle, 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 önlenmesine ilişkin olarak da telekomünikasyon yoluyla yapılan iletişim tespit edilebileceği, dinlenebileceği, sinyal bilgilerinin değerlendirilebileceği ve kayda alınabileceği hükme bağlanmıştır. 5397 sayılı Kanun'un, önlenmesi amaçlanan bu suçlar dikkate alındığında, AİHS bağlamında iletişimin gizliliğine müdahale oluşturan bir önlemin meşru bir amaca dayanıp dayanmadığına ilişkin yukarıda yapılan değerlendirme açısından, suç işlenmesinin önlenmesine yönelik meşru bir amacı benimsediği söylenebilir.

5397 sayılı Kanun, ayrıca, adli amaçlı iletişimin denetlenmesini düzenleyen CMK'nın 135. maddesinin aksine, bu tedbire son çare olarak başvurulabileceği yönünde bir yaklaşım benimsememiştir. Bu ilkeyle ifade edilmek istenen, iletişimin bu şekilde denetlenmesi dışında başka bir yolla delil elde etme olanağının çok az olduğu suçları ortaya çıkarmak veya suçun önlenmesi için zaruri ise bu yola başvurulacağıdır.³⁴⁹ İletişimin adli amaçlı denetlenmesi açısından CMK'nın 135. maddesinin birinci fıkrasında bu şart, “başka suretle delil elde edilmesi imkanının bulunmaması durumunda” şeklinde yer bulmaktadır. Aslında yürürlüğe girdiği 1999 yılından 2005'e kadar telekomünikasyon yoluyla yapılan iletişimin denetlenmesine dayanak olarak kabul edilen 4422 sayılı Kanun'da da bu ilkenin, “başka bir tedbir ile failin belirlenmesi, ele geçirilmesi veya suç delillerinin elde edilmesi mümkün ise, iletişimin dinlenmesine veya tespitine karar verilemeyeceği” hükmüyle yer aldığı görülebilir. Fakat bu ilke bu şekliyle iletişimin önleme amaçlı denetimine dayanak oluşturan 5397 sayılı Kanun'da düzenlenmemiştir. Bu nedenle bu eksiklik, başka önlemlerle suçun işlenmesinin önlenilebileceği hallerde de iletişimin ve özel yaşamın gizliliğinin ihlalini yaratabilecek şekilde iletişimin denetlenmesine başvurulabileceği sakıncasını beraberinde getirmektedir.

³⁴⁹ Kunter, Yenisey, Nuhoglu, a.g.e., s. 49, 50.

Bu hususun farkındalığıyla, iletişimin önleme amaçlı denetlenmesine, örgüt faaliyeti çerçevesinde işlenen suçlar veya terörist faaliyetlerin önlenmesine yönelik suçlar gibi bazı ağır suçlar bakımından başvurulduğu unutulmamalıdır. Bu yönüyle de, adli amaçlı denetimde olduğu gibi, hem elde edilmek istenen sonuca hizmet edecek hem de iletişimin denetlenmesi yerine başvurulabilecek önlemleri belirlemenin çok da kolay olmayacağı da unutulmamalıdır. Nitekim telekomünikasyon yoluyla yapılan iletişimin adli amaçlı denetlenmesi açısından, arama, yakalama, el koyma, ifade alma ve benzeri delil elde edilebilecek başkaca klasik önlemlerin göz önünde bulundurulabileceği ileri sürülebilir.³⁵⁰ Fakat aynı şekilde, telekomünikasyon yoluyla yapılan iletişimin yukarıda sayılan suçların önlenmesi amacıyla denetimi açısından da benzer belirleme kolaylıkla yapılamayabilir. Örneğin, uyuşturucu madde ticareti suçu ile ilgili olarak, suçun tespit edilerek, ticareti yapanın yakalanması için izleme veya gizli görevli kullanma yolları seçilerek amaca ulaşılabileceği; fakat konuyla ilgili bir örgütün bu faaliyetleri çerçevesinde böyle bir suçun ve tüm ilişkilerinin tespit edilmesi için telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesinin gerekli görülebileceği düşünülebilir.³⁵¹

Kaldı ki, adli amaçlı denetim açısından dahi, Ceza Muhakemesi'nin 135. maddesi başka suretle delil elde edilmesi imkanının bulunmaması halinde bu yola başvurulacağını ifade etmiş olsa da, bu halden ne anlaşılması gerektiğini böyle bir yasal düzenlemede açıklamamış ve bu açıklama değiştirilmesi yasal düzenlemeye göre daha kolay olabilecek bir yürütme işlemi olan İletişimin Denetlenmesi Yönetmeliği'nin 4. maddesine bırakılmıştır. Buna göre, başka suretle delil elde edilmesi imkanının bulunmaması hali “soruşturma veya kovuşturma sırasında diğer tedbirlere başvurulmuş olsa bile sonuç alınamayacağı hususunda bir beklentinin varlığı veya başka yöntemlerden biri veya birkaçının uygulanmasına rağmen delil elde edilememesi ve delillere ancak bu Yönetmelikte düzenlenen tedbirlerle ulaşılabilecek olmasını” ifade etmektedir.³⁵² Yasal düzenlemenin kendisinde yer almayan beklenti gibi kavramların, Yönetmelik'te öngörülüyor olması; gerek bu

³⁵⁰ Kunter, Yenisey, Nuhoglu, a.g.e., s. 50.

³⁵¹ Kaymaz, a.g.e., s. 225, 613. dipnot.

³⁵² İletişimin Denetlenmesi Yönetmeliği m. 4/c.

önleme tanıdığı ucu açık uygulama alanı³⁵³ gerekse birer temel hak ve özgürlük olarak özel yaşamın gizliliği ve iletişimin gizliliği hakkının sınırlandırılmasına ilişkin bir husus olarak yasayla sınırlama kuralıyla³⁵⁴ ilgili yarattığı aykırılık bakımından eleştirilebilir. Zira unutulmamalıdır ki, yürütmenin düzenleyici işlemleri böyle bir konuda, yasanın çizdiği sınırlar dahilinde biçim ve usul ile ilgili kurallar düzenleyebilir.³⁵⁵

Telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesi açısından, bu denetimi mümkün kılacak suçlar da dikkate alındığında, diğer önlemlerin uygulanmasının çok da kolay olmayacağı ve bu başkaca önlemlerin tek tek yasal düzenlemede belirlenme zorluğu da akla gelebilir. Fakat kanımızca, iletişimin denetlenmesinden önce başvurulabilecek daha hafif başkaca tedbirlerin yasada yer alması sağlanamıyor ise; iletişimin denetlenmesine karar verecek hakim diğer önlemlere başvurulsa da elde edilmek istenen sonuca ulaşamayacağı veya başvurulduğunda tehlikeli etkiler doğabileceği konusunda bir değerlendirme yapacağı ve bu yönde bir kanaati oluşmadıkça tedbir kararı veremeyeceğinin yine bir yasal düzenlemede hükme bağlanması düşünülebilir.³⁵⁶

Telekomünikasyon yoluyla yapılan iletişimin denetlenmesinin özel yaşamın ve iletişimin gizliliği temel hak ve özgürlüklerini yakından ilgilendirdiği göz önünde bulundurulursa, aslında yasallık ilkesinin korunmasının başlı başına ne kadar önemli olduğu görülebilir. Kaldı ki, bu koşulun düzenlemelerde ve uygulamada yer almaması, müdahalenin aynı zamanda demokratik toplum düzeninin gereklerine uygun olmadan gerçekleşmesi sonucunu da beraberinde getirebilecektir. Bu noktada sadece AIHM değil,³⁵⁷ özgürlüklerin istisnai olarak ve demokratik toplum düzeninin

³⁵³ Ersan Şen, **Türk Hukuku'nda Telefon Dinleme, Gizli Soruşturmacı, X Muhbir**, 5. bs., Ankara, Seçkin, 2011, s. 112, 113. (Bundan sonra Türk Hukuku'nda Telefon Dinleme olarak anılacaktır.)

³⁵⁴ Tanör, Yüzbaşıoğlu, **a.g.e.**, s. 147-149; Ergun Özbudun, **Türk Anayasa Hukuku**, Ankara, 12. bs., 2011, s. 109, 110; Kaboğlu, **a.g.e.**, s. 89-91; Kemal Gözler, **Türk Anayasa Hukuku Dersleri**, 10. bs., Bursa, Ekin, Ekim 2010, s. 124.

³⁵⁵ Tanör, Yüzbaşıoğlu, **a.g.e.**, s. 148; Gözler, **a.g.e.**, s. 124.

³⁵⁶ Kanada Ceza Kanunu'nun 186/1a, b maddesinde buna paralel bir düzenleme yer almaktadır, Criminal Code, R.S.C., 1985, c. C-46 (1 Ocak 2012'de değiştirilmiş haliyle), (Çevrimiçi) <http://laws-lois.justice.gc.ca/PDF/C-46.pdf>, 1 Şubat 2012.

³⁵⁷ Kaboğlu, **a.g.e.**, s. 92.

sürekliliği için zorunlu olduğu ölçüde sınırlandırılabilirliğini ifade ettiği yaklaşımdan anlaşıldığı gibi,³⁵⁸ Türk Anayasa Mahkemesi de, demokratik bir toplumda gerekli olanın belirlenmesinde ölçülülük ilkesine başvurmaktadır.

Ölçülülük ilkesi bağlamında 5397 sayılı Kanun'un getirdiği hükümlerin elverişlilik, gereklilik (zorunluluk) ve orantılılık açısından bir değerlendirmesi yapılabilir. Buna göre, kullanılan sınırlama aracının amacı gerçekleştirmeye elverişli olması açısından, 5397 sayılı Kanun, öngördüğü suç tiplerinin belirsizliği ile ilgili olarak eleştirilebilir de; bu Kanun'da öngörülen telekomünikasyon yoluyla yapılan iletişimin denetlenmesinin, terörist faaliyetlerin ve devletin güvenliği aleyhine işlenebilecek suçlar gibi ağır suçların işlenmesinin önlenmesi amacını gerçekleştirmeye elverişli olduğu söylenebilir. Burada başvuru olan bu önlemin istenilen amacın gerçekleşmesine katkıda bulunacağı³⁵⁹ ve bu yönüyle elverişlilik ilkesini karşıladığı kabul edilebilir. Ölçülülük ilkesinin gereklilik alt unsuru açısından aynı değerlendirmeyi yapmak pek mümkün görülmeyebilir. Zira yukarıda da açıklandığı üzere, 5397 sayılı Kanun'un, bu önleme en son çare olarak başvurulmasına yer verdiği bir düzenleme ile karşı karşıya olduğumuz söylenemez. Ulaşılmak istenen sonuç için öncelikle başkaca daha hafif önlemlere başvurulabileceği ve istenen amaca bu yollarla ulaşılamayıp, ancak bu önlemle ulaşılabilirdiği durumda, iletişimin denetlenmesi önlemine başvurulacağı düzenlenmemiştir. Bu nedenle, Kanun'un, özel yaşamın gizliliği ve iletişimin gizliliği hakkını daha az sınırlayacak aynı derecede etkili bir önlem varsa da, ağır bir önlem olan iletişimin denetlenmesinin seçilmesine bir başka ifadeyle gerekli veya zorunlu olmayan bir sınırlama aracına imkan vereceği görülebilir.

Son olarak 5397 sayılı Kanun'un, bu tedbire ilişkin kararın en fazla üç ay için verilebileceğini ve bu sürenin aynı usulle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabileceğini hükme bağladığı görülür.³⁶⁰ Bu yönüyle, söz konusu önlemi belli bir süreyle sınırlandırmış olması bakımından 5397 sayılı Kanun'un orantılılık³⁶¹ - araç ile istenen amaç arasında dengeli oran ilişkisi - unsurunu karşıladığı

³⁵⁸ E. 1985/8, K. 1986/27, K.t. 26 Kasım 1986, Resmi Gazete No. 19544, 14 Ağustos 1987.

³⁵⁹ Tanör, Yüzbaşıoğlu, **a.g.e.**, s. 154; Gözler, **a.g.e.**, s. 131; Özbudun, **a.g.e.**, s. 114.

³⁶⁰ 5397 sayılı Kanun'un 1., 2. ve 3. maddesi.

³⁶¹ Tanör, Yüzbaşıoğlu, **a.g.e.**, s. 155; Özbudun, **a.g.e.**, s. 114, 115; Gözler, **a.g.e.**, s. 132.

söylenebilir. Fakat böyle bir değerlendirme yaparken de unutulmamalıdır ki, hükmün devamında terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi durumunda, hakim üç aydan fazla olmamak üzere süreyi müteaddit defalar uzatabileceğinin öngörülmesi ölçüsüz bir oran içinde bulunulması sonucunu doğurabilecektir. Zira henüz suç işlenmemiş olduğundan, öngörülen tehlikenin, terör örgütünün faaliyeti çerçevesinde olup olmadığını yanılığa düşmeden belirlemek çok zor olacaktır. Ayrıca bu tür suçların önlenmesi açısından başvurulacak iletişimin denetlenmesi açısından herhangi bir üst sınır öngörmeme sonucunu da yaratabilecektir.

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI

I. GENEL OLARAK

Kişisel verilerin korunmasının, telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesi konusuna ilişkin önemi, gerek Avrupa Birliği mevzuatında gerek Türk hukukunda telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sonucu elde edilen bilginin “kişisel veri” kapsamında nitelendirilmesi noktasında başlamaktadır. En genel anlatımıyla, bir kişiye ilişkin belirli ya da doğrudan veya dolaylı olarak onu; bir kimlik numarasına veya fiziksel, psikolojik, ruhsal, ekonomik, kültürel ve sosyal kimliğine özgü bir veya birkaç unsura gönderme yaparak belirlenebilir kılan bilgi³⁶² kişisel veri olarak nitelendirilebilir. Bu bağlamda, önleme amaçlı denetim sonucu elde edilen bilginin kişisel veri kapsamında değerlendirilmesinin, bu bilginin amacına uygun olarak kullanılması ve korunması bakımından büyük önem arz ettiği söylenebilir. Nitekim bu tanımlamayla kişisel verilerin korunmasına ilişkin ilkeler, sadece denetim sonunda elde edilen bilgiler değerlendirilirken değil; denetim uygulanırken de göz önünde bulundurulacaktır.

Kişisel verilerin korunması (**data protection**) kavramı, ilk bakışta içeriği tam karşılayan bir kavram gibi gözüküyorsa da, aslında korumanın kime yönelik olduğu sorusunu akla getirmektedir. *Korumaya ihtiyacı olan veri mi, birey mi?* Kavram

³⁶² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050, (Çevrimiçi) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>, Nov. 25, 2010. Bundan sonra 95/46 no’lu Yönerge olarak anılacaktır. OECD’nin Özel Yaşamın Gizliliği ve Kişisel Verilerin Korunmasına İlişkin İlkelerinde de, özel yaşamı aynı şekilde tanımlamıştır, OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part One, 1/b maddesi, (Çevrimiçi) http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html#guidelines, 18 Aralık 2011.

1960’larda Almanya’da dile getirilmiş ve daha sonra da tüm dünyaya yayılmış bir kavram olarak karşımıza çıkıyor.³⁶³ Bu nedenle, gerek kişisel veri kavramının Avrupa Birliği yönergelerinde, Avrupa Konseyi’nin çalışmalarında ve çeşitli uluslararası organizasyonlarda nasıl kabul edildiği, gerekse ilgili devletlerin anayasalarında tanımının ne kapsamda şekillendiğinin incelenmesi yerinde olabilir.

Nitekim karşılaştırmalı hukuk mevzuatı incelendiğinde, gerek Avrupa Birliği’nin verilerin korunmasına dair yönergelerinin gerekse Avrupa Birliği’nin diğer düzenlemelerinin tüm gelişmelerden tecrit edilmiş, hiç ortaya atılmamış yeni fikirlerden oluşan düzenlemeler olmadığı söylenebilir. Aksine, özellikle 1970’lerden beri süregelen yasal düzenlemeleri de beraberinde getiren bir hareketin genişletilmiş bir hukuki çerçevesini oluşturdukları ifade edilebilir.³⁶⁴

Hangi yönüyle incelenirse incelensin, kişisel verilerin korunmasının, bir kişinin bağımsızlığı ve özgür iradesi açısından vazgeçilmez olduğu açıkça görülmektedir. Korumanın bu denli öneminden olsa gerek, uluslararası belgelerin, kişisel verilerin korunmasının kapsamını, kullanılan teknik usullere bağlı olarak yorumlamaktan kaçındığı söylenebilir.³⁶⁵

II. AVRUPA KONSEYİ VE AVRUPA BİRLİĞİ MEVZUATI BAĞLAMINDA KİŞİSEL VERİLER

Dünyada genel olarak, insanın bildiği kadar güçlü olduğu ve bu bildiğini de ulaşabildiği bilginin oluşturduğu yaklaşımı hızla daha da önem kazanırken; bu ulaşılabilirliği sağlamak için bilginin geçirdiği evrelerin özel yaşamın gizliliği hakkına etkisi de aynı hızla başlıca kaygılardan biri haline gelmiştir. Avrupa’nın bu kaygıya neredeyse ilk cevabı, 1981 yılında Avrupa Konseyi’nin “Kişisel Verilerin Otomatik İşlenmesiyle İlgili Olarak Kişilerin Korunmasına Dair” 108 no’lu

³⁶³ Christian Koenig, Andreas Bartosch, Jens-Daniel Braun, Marion Romes, **EC Competition and Telecommunications Law**, 2. bs., the Netherlands, Kluwer Law International, 2009, s. 509.

³⁶⁴ Gutwirth, **a.g.e.**, s. 1.

³⁶⁵ Anne Cammilleri-Subrenat, Claire Levallois-Barth, **Sensitive Data Protection in the European Union**, Bruxelles, Bruylant, 2007, s. 14.

Sözleşmeyi³⁶⁶ kabul etmesiyle kendini göstermiştir. Sözleşme her bir taraf devlette, uyruğu veya yerleşim yeri ne olursa olsun gerçek kişilerin kendileriyle ilgili verilerin otomatik olarak işlenmesi karşısında temel hak ve özgürlüklerinin ve özellikle özel yaşamın gizliliği haklarının korunmasını amaçlamaktadır.³⁶⁷ Kamu ve özel sektörü de içine alacak şekilde, otomatik oluşturulan kişisel veri dosyaları veya kişisel verilerin otomatik işlenmesi sırasında gerçek kişilerin korunması hakkında uygulama alanı bulacak Sözleşme,³⁶⁸ taraf devletlerin Sözleşmenin benimsediği korumadan daha geniş bir koruma getirmelerine de imkan tanımaktadır.³⁶⁹ Nitekim Sözleşme'nin, Avrupa'da birçok ulusal kişisel veri korunmasına dair yasal düzenlemelere temel teşkil ettiği görülebilir. İngiltere'de kabul edilen 1984 tarihli Veri Koruma Yasası (**Data Protection Act**) buna örnek olarak gösterilebilir.³⁷⁰

Avrupa Birliği bağlamında konuya bakılırsa, iki temel husus göze çarpar. Birincisi, üye devletler arasındaki neredeyse sınırsız denebilecek piyasa koşulları ve bilgi aktarımındaki gelişmedir. Diğerisi ise, Avrupa Konseyi'nin 108 no'lu Sözleşmesi'ne rağmen, diğer birçok konuda olduğu gibi, Avrupa Birliği'ne üye devletler arasındaki ulusal hukuk farklılaşmasının önlenememiş olması ve bunun üye devletlerde eşit olmayan koruma düzeylerine yansıyabilecek olmasıdır. Gerçi İrlanda, İspanya ve İngiltere gibi bazı devletler Sözleşme'nin yaklaşımını takip ederek kişisel verilerin korunması kanunları kabul ederken; Almanya ve Fransa gibi Sözleşme'den önce sistemlerini kurmuş ve düzenlemelere sahip olmuş devletler ise bunlara yenileri eklemişlerdir.³⁷¹

³⁶⁶ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981, (Çevrimiçi) <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>, 3 Aralık 2011.

³⁶⁷ 108 No'lu Sözleşme'nin 1. maddesi.

³⁶⁸ 108 No'lu Sözleşme'nin 3/1. maddesi.

³⁶⁹ 108 No'lu Sözleşme'nin 11. maddesi.

³⁷⁰ Data Protection Act 1998, c. 29, (Çevrimiçi) <http://www.legislation.gov.uk/ukpga/1998/29/section/1>, 3 Aralık 2011.

³⁷¹ Spiros Simitis, "From the Market to the Polis: The EU Directive on the Protection of Personal Data," *Iowa Law Review*, C.LXXX, 1994-1995, s. 451, 452.

A. Avrupa Birliđi Yönergeleri

Yaşanan gelişmelerin ışığında, 1990'da ilk Yönergenin ilk taslağı filizlenmeye başlamış olsa da,³⁷² asıl olarak 24 Ekim 1995 tarihinde Avrupa Parlamentosu ve Konsey'in Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Verilerin Serbest Dolaşımına İlişkin Yönergesi (95/46 no'lu Yönerge)³⁷³ kabul ettiđi görülür. Öncelikle şu belirtilmelidir ki, 95/46 no'lu Yönerge, Avrupa Birliđi'nin yetkisi dahilinde olmayan hususlar - örneğin ulusal güvenlik veya ceza hukuku - ve sadece bir kişinin gerçekleştirdiđi bireysel faaliyetler açısından uygulanma alanı bulmayacaktır.³⁷⁴ Ayrıca telefon konuşmaları ve elektronik postaları da (email) kapsayacak şekilde elektronik iletişimde özel yaşamın gizliliğinin ve kişisel verinin korunmasını 2002/58 no'lu Yönerge düzenlemiştir. Konuya ilişkin Avrupa Birliđi Yönergelerinin her birinin temelde birbirinden çok farklı düzenlemeler ve esaslı değişiklikler getirmediđi; gelişmelere uyarlanmış (**updated**) bir yaklaşım sergiledikleri söylenebilir.³⁷⁵ Fakat şu da belirtilmelidir ki, 95/46 no'lu Yönerge 2002/58 no'lu Yönerge'ye adeta temel teşkil etmiş ve esas ilkeleri belirlemiştir. Kaldı ki, genel itibariyle, kişisel verilerin korunmasına dair Avrupa yaklaşımını yansıtmaları ve Türk hukuku bakımından kişisel verilerin korunmasına dair kanun tasarısıyla taşıdığı paralelliklerin de değerlendirilebilecek olması nedeniyle ayrıca ele alınabilir.

Öncelikle elde edilen ne tür verilerin kişisel veri sayılabileceđi irdelenebilir. 95/46 no'lu Yönerge'de kişisel veriler, belirli veya belirlenebilecek bir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır. Bu bağlamda, belirlenebilir gerçek kişi ise, verilerin, doğrudan veya dolaylı olarak, kişinin özellikle kimlik numarasına ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine gönderme

³⁷² David Bainbridge, **Data Protection**, Great Britain, CLT Professional Publishing, 2000, s. ix; Simitis, **From the Market to the Polis: The EU Directive on the Protection of Personal Data**, s. 446.

³⁷³ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031-0050.

³⁷⁴ 95/46 no'lu Yönerge'nin 3/2. maddesi.

³⁷⁵ Robert SK Bell, Neil Ray, **EU Electronic Communications Law**, UK, Richmond, 2004, s. 113.

yapması suretiyle tanımlanabilen kişi olarak kabul edilebilir.³⁷⁶ Yönerge sadece gerçek kişileri koruma kapsamına almaktadır.³⁷⁷ Fakat bununla birlikte İtalya gibi bazı devletlerin Yönergeyi tüzel kişileri de kapsayacak şekilde uyguladığı görülebilmektedir.³⁷⁸ Çalışmamızın konusu bakımından şu hususu ifade etmek yerinde olabilir. Yönerge esas itibariyle kişisel verilerin tamamen veya kısmen veri işlenmesine tabi tutulmasında ve bir dosyanın bir parçası olarak kaydedilmiş veya kaydedilebilecek olan verilerin işlenmesinde uygulanacaktır. Fakat kamu güvenliği, savunma, devletlerin ceza hukuku alanındaki faaliyetleri bakımından ise uygulama alanı bulmamaktadır.³⁷⁹ Kaldı ki, gerçek kişinin kişisel veya ailesiyle ilgili faaliyetler dahilinde gerçekleştirilecek kişisel verilerin işlenmesi durumunu da kapsamamaktadır.³⁸⁰

95/46 sayılı Yönerge bağlamında, kişisel verinin tanımlanması açısından, sadece kişisel verileri belirli veya belirlenebilecek bir gerçek kişiye ilişkin her türlü bilgi olarak tanımlayan 2/a maddesi değil; aynı zamanda Yönergenin 26 numaralı gerekçesi de göz önünde bulundurulmalıdır. Buna göre, Yönerge belirli ve kişiyi tanımlanabilir kılan bilgi bakımından bir başka anlatımla gerçek kişiler hakkında elde edilen veriler açısından uygulanacağından, makul olarak o kişinin belirlenmesini sağlayacak bilgi uygulama alanını oluşturacaktır. Örneğin, kişinin belirlenmesi sonucunu doğurmayacak anonim veriler, Yönerge hükümlerinin kapsama alanı içinde bulunmamaktadır.³⁸¹ Bununla birlikte, dolaylı da olsa fiziksel, psikolojik, zihinsel, ekonomik veya kültürel özellikleri gibi kişiyi ilgilendiren bilgilerin de belirlenebilir kılan veri kapsamında değerlendirildiği dikkate alınırsa; bir kişinin adı-soyadı alınmasa da yaşına, kaç çocuğu olduğuna ve ne iş yaptığına dair bilgilerin kaydedilmesinin bu bağlamda belirlenebilir kılan bilgi olarak kabul edileceği söylenebilir.³⁸²

³⁷⁶ 95/46 no'lu Yönerge'nin 2/a maddesi.

³⁷⁷ 95/46 no'lu Yönerge'nin 2/a maddesi.

³⁷⁸ Maria Veronica Perez Asinari, "Legal Constraints for the Protection of Privacy and Personal Data in Electronic Evidence Handling," **International Review of Law Computers & Technology**, C.XVIII, No:2, Temmuz 2004, s. 232.

³⁷⁹ 95/46 no'lu Yönerge'nin 3. maddesi.

³⁸⁰ 95/46 no'lu Yönerge'nin 3. maddesi.

³⁸¹ 95/46 no'lu Yönerge'nin 26 numaralı gerekçesi.

³⁸² Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, İstanbul, Beta, 2008, s. 43.

Yönerge kapsamında, belirli ya da kişiyi belirlenebilecek kılacak verinin, dijital veya basılı olarak yayımlanmış bir yazılı metin halinde olması gerekmemektedir. Gerek bilgi toplumu olmanın gerektirdikleri gerek teknolojiadaki gelişmeler ışığında, Yönerge'nin hükümlerinden değil ama gerekçesinden anlaşıldığı üzere, kişinin belirlenmesine imkan verecek ses veya resimleri de, işlenmesi durumunda korunacak kişisel veri kapsamında kabul edilmektedir.³⁸³ Yönerge, kişisel verilerin işlenmesi sırasında üye devletlerin, gerçek kişilerin özellikle özel yaşamın gizliliği başta olmak üzere, hak ve özgürlüklerinin korunmasını sağlamaları yükümlülüğünü vurgulamaktadır.³⁸⁴ Öncelikle 95/46 no'lu Yönerge'nin gerçek kişilerin veya kurumların veri işlemlerinde uygulanabileceğini ve bu yönüyle hem özel hem de kamusal veri dosyaları açısından kapsamlı bir özel yaşamın gizliliğinin korunması standardı sunduğu ifade edilebilir.³⁸⁵

Bu bağlamda kişisel verilerin işlenmesi, otomatik veya otomatik olmayan bir süreç içinde, verilerin toplanması, kaydedilmesi, organize edilmesi, saklanması, uyarlanması veya değiştirilmesi, elde edilmesi, sorulması, kullanılması, yayılması veya başka her türlü ulaşılabilir tutulması, verilerin sıralandırılması veya ilişkilendirilmesi, engellenmesi, silinmesi ya da yok edilmesi gibi işlemlere maruz kalması anlamına gelmektedir.³⁸⁶ Veri işleminin bu şekliyle geniş kapsamda düşünüldüğü; örneğin saklama gibi, veriyi sadece elde tutmanın dahi işleme kapsamında nitelendirileceği görülmektedir. Bununla birlikte, görülüyor ki, verileri içeren dosyaları yerleştirmek ve veriye her türlü ulaşım ve kullanma da bu yönde değerlendirilebilir.³⁸⁷

Tek başına veya başkalarıyla birlikte kişisel verilerin işlenme amacı ve şekline karar veren gerçek veya tüzel kişiler, kamu yetkilileri veya başkaca herhangi bir kişi veya

³⁸³ Bainbridge, **a.g.e.**, s. 20; 95/46 no'lu Yönerge'nin 14, 15, 16 ve 17 numaralı gerekçesi.

³⁸⁴ Sebastian Farr, Vanessa Oakley, **EU Communications Law**, 2. bs., London, Sweet&Maxwell, 2006, s. 328; Peter Carey, **E-Privacy and Online Data Protection**, UK, Butterworths Lexis Nexis, t.y., s. 7, 8; Garzaniti, **a.g.e.**, s. 109-115.

³⁸⁵ L. Richard Fischer, **Privacy and Accuracy of Personal Information**, North Carolina Banking Institute, C.III, 1999, s. 17.

³⁸⁶ Perez Asinari, **a.g.m.**, s. 233; 95/46 no'lu Yönerge'nin 2/b maddesi.

³⁸⁷ Bainbridge, **a.g.e.**, s. 20.

kuruluş, 95/46 sayılı Yönerge kapsamında veri işlemeden sorumlu mercii olarak kabul edilmektedir. Eğer ulusal hukuk veya Birlik hukuku bu sorumluyu belirlerse, Yönerge, sorumlunun veya onun atanmasına dair belirli koşulların da ulusal hukuk veya Birlik hukuku tarafından belirtilebileceğini de hükme bağlamaktadır.³⁸⁸ Veri işleme sorumlusu olan kişinin (**controller**), söz konusu kişisel verinin konusu (ilgili/veri sahibi) veya kamu yetkilisine karşı hukuki sorumlulukları olmalıdır. Bir başka ifadeyle bir tüzel kişilikte, ilgili sayfa üzerinden veriyi işleyen sistem sorumlusu değil; o tüzel kişiliğin yöneticisi sorumlu olacaktır. Zira sürece ilişkin bu faaliyetin amacına ve yoluna onun karar verdiği kabul edilir. Bununla birlikte, eğer sistem sorumlusu, sürece ilişkin faaliyetlere karar verme bakımından daha yetkili ise, yönetici yerine o sorumlu olarak nitelendirilebilecektir.³⁸⁹ Şu da unutulmamalıdır ki, veri işleme sorumlusu adına veri işleyebilecek kişileri (**processor**) ise, yine gerçek veya tüzel kişiler, kamusal makamlar veya başkaca kişi veya kuruluşlar oluşturabilecektir. Bu kişilerin veri işleme sorumlusundan farkı, söz konusu veri konusuna karşı doğrudan yasal sorumluluğa sahip olmamalarıdır. O kadar ki, veri işleme sorumlusu adına böyle bir işlemde bulunmak için bu kişi ve sorumlu arasında bir anlaşma ve güven ilişkisi beklenmektedir ki, veri işleme sorumlusunun talimatı üzerine, onun yetkisi altında böyle bir işlem yapılabilir.³⁹⁰

Verilerin işlenmesi bakımından ise, ilgilinin rızası aranmaktadır. Bu bağlamda, ilgili kişinin serbest iradeyle, belirli olay için ve bilgilendirilmiş olarak kendisine ait verilerin işlenebilmesiyle ilgili olarak rızası gerekmektedir.³⁹¹ Böylece belirli (**specific**) rıza aranması, bir kez rıza aldıktan sonra dahi veri işleyenin sonradan başka amaçla kişisel veriyi işleyebilmesinin, tekrar ilgili kişinin olumlu iradesine başvurmasını gerektirir. Bununla birlikte, ilgilinin bilgilendirilmiş olması bakımından da, durumun farkında olması ve ayrıntılardan haberdar edilmiş olması öngörülmektedir.³⁹²

³⁸⁸ 95/46 no'lu Yönerge'nin 2/d maddesi.

³⁸⁹ Perez Asinari, **a.g.m.**, s. 232.

³⁹⁰ Perez Asinari, **a.g.m.**, s. 232; Bainbridge, **a.g.e.**, s. 20.

³⁹¹ 95/46 no'lu Yönerge'nin 2/h maddesi.

³⁹² Perez Asinari, **a.g.m.**, s. 240; Bainbridge, **a.g.e.**, s. 21.

Konuya ilişkin temel belgelerden biri olarak nitelendirilebilecek bu ikincil kaynak, 95/46 no'lu Yönerge, özel yaşamın gizliliği hakkına ilişkin koruma üzerine yoğunlaşmıştır. Fakat şu da belirtilmelidir ki, özel yaşamın gizliliğine dair bir tanım yapmamıştır. Aslında bu yaklaşım dahi, daha önce ifade edilen, sadece A.B.D. hukukunun değil, genel olarak Kıta Avrupası yaklaşımının da özel yaşamın gizliliğini tanımlama kaygısıyla kendisini sınırlamadığı ve genel geçer bir tanımın yeterli olmayacağı üzerine şekillenmiş olduğu şeklinde yorumlanabilir.

Yönerge, özel yaşamın gizliliğinin korunmasına da, kişisel verilerin işlenmesini düzenleyecek olan ilgili düzenlemelerle ulaşılabileceğini kabul etmektedir. Bu bağlamda, Yönerge'nin ve aslında Avrupa Birliği'nin konuya yönelik genel anlayışını daha iyi anlayabilmek ve Yönerge'nin kendisinin geliştirilmesi ihtiyacını daha yakından görebilmek için, İngiliz Veri Koruması Kanunu (**Data Protection Act/DPT**)³⁹³ gibi ulusal düzenlemeler ile karşılaştırıldığı görülür. Bunun nedenlerinden birini, İngiltere'de Bilgi Komisyonu Ofisi'nin hazırladığı bir araştırma raporunda, Yönerge'nin geliştirilmesi gerektiğine dair belirlemelerde de bulunması oluşturmaktadır. Bu raporda, Komisyon genel itibarıyla, özel yaşamın gizliliğine dair yeni gelişmeleri Yönerge'nin karşılayamadığını ve Avrupa veri koruma hukukunun oldukça bürokratik ve aşırı kuralcı bir anlayış sergilediğini dile getirmiştir.³⁹⁴

Bu tartışmalar ışığında 95/46 no'lu Yönerge'ye dair bazı değerlendirmeler yapılabilir. Özel yaşamın gizliliği ve özel bilgi arasında bir ilişkinin olup olmadığı ve her şeyden önce kişisel bilginin özel bilgi anlamında kullanılıp kullanılmadığı, Avrupa Birliği bakımından konuya ilişkin önemli ve sonraki düzenlemelere de temel ilkeler belirleyen bu Yönerge'den anlaşılamamaktadır. Yönerge'de verinin belirlenebilir bir kişiye ait olması ve daha sonra işlenmesi gibi bir yaklaşım benimsenmektedir. Fakat bu noktada örneğin DPT, bu sıralamayı diğer türlü işleterek, öncelikle verinin işlenmesi sorunsalıyla, daha sonra ise ortada belirlenebilir

³⁹³ Data Protection Act 1998, (Çevrimiçi) <http://www.legislation.gov.uk/ukpga/1998/29/contents>, 11 Aralık 2011.

³⁹⁴ UK Privacy Watchdog Spearheads Debate on the Future of European Privacy Law, press release, 7 July 2008, Information Commissioner's Office, (Çevrimiçi) http://www.ico.gov.uk/upload/documents/pressreleases/2008/ico_leads_debate_070708.pdf, 11 Aralık 2011.

bir kiři bulunmakta mıdır kısmıyla ilgilenmektedir. Bunu da 95/46 no’lu Yönerge’nin ve DPT’in kişisel veriyi tanımlamalarındaki farklılıktan dahi anlayabilmek mümkündür. DPT, kişisel veriyi veri işleme sorumlusunun sahip olduđu bir veri veya başkaca bir bilgi olarak, verinin ilgili olduđu kiřiyle ilgili bir fikir beyanını ya da veri işleme sorumlusunun veya başka birinin bu kiřiye dair duygularının belirtisini içeren ve bu özellikleriyle kiřiyi belirlenebilir kılan veri şeklinde tanımlamaktadır.³⁹⁵ Görölüyor ki, “veri” ve “bilgi” arasında bile bir ayrım yapmaktadır. Fakat bu ayrımın uygulamada bir farklılık yaratmadıđı gibi, esasa ilişkin de bir ayrım olmadığı kabul edilmektedir.³⁹⁶

95/46 no’lu Yönerge’nin, bunun yanı sıra, kişisel veriyi tanımlarken, “iliřkin/ilgili” kavramını kullandığı görölür. Bu da aslında kiřiyle bağlantı kurması akla gelebilecek her bilginin kişisel olarak değerdendirilmesi sakıncasını doğurabilecektir. Bu bağlamda iki türlü yorum düşünülebilir. Eğer kiřiye “iliřkin” kavramı dar yorumlanırsa, sadece kendi başına veya başka bir bilgi ile birlikte kiřiyi belirli kılabilen bilgi kişisel veri olarak kabul edilir. Bu kavram geniş bir yoruma tabi tutulur ise, kiřiyi belirleyebilme kapasitesine bakılmaksızın kiřiyi bir şekilde etkileyebilen her bilgi kişisel veri olarak nitelendirilebilir.³⁹⁷ Aslında Yönerge’nin bu iki yorumu da mümkün kılabilecek anlayışının, uygulamada da yer bulduđu ve fakat kendini daha fazla dar yoruma bıraktığı söylenebilir.

İngiltere’de, gerek 95/46 no’lu Yönerge’ye gerek ulusal veri koruma kanunu olan DPT’e gönderme yapılan bir kararda, korunmaya konu olacak kişisel veriyi belirlerken, kiřiyi belirlemeye yardımcı olma açısından değıl de, kiřinin özel yaşamının gizliliğini etkileyebilme açısından kavrama yaklaşıldığı görölür.³⁹⁸ Aslında burada iletişimin denetlenmesi yoluyla elde edilen ve tutulan kişisel veri

³⁹⁵ İngiliz Veri Koruması Kanunu’nun 1/1 maddesi.

³⁹⁶ Karen McCullagh, “Protecting ‘Privacy’ through Control of ‘Personal’ Data Processing: A Flawed Approach,” **International Review of Law, Computers & Technology**, C.XXIII, No:1-2, Mart-Temmuz 2009, s. 14; Data Protection Act 1998 Legal Guidance, (Çevrimiçi) http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf, 11 Aralık 2011.

³⁹⁷ McCullagh, **a.g.m.**, s. 15.

³⁹⁸ *Durant v. FSA* [2003] EWCA Civ 1746, Royal Court of Justices Strand, London, WC2A 2LL, 8 December 2003, (Çevrimiçi) http://www.gov.im/lib/docs/odps/cl_durantvsfsa.pdf, 12 Aralık 2011.

değil de, kişinin bankayla ilgili anlaşmazlığı sonrası finansla ilgili yetkili federal makama bir şikayette bulunması ve bu makamın da bu şikayet üzerine topladığı elle tutulan yazılı dosyaları ve bilgisayar ortamında tutulan dosyaları kişinin talep etmesi ile ilgili bir olay olarak karşımıza çıkmaktadır. Fakat bu olay, 95/46 no'lu Yönerge ve kişisel veriyi bu yönergedeki şekliyle benimseyen diğer düzenlemelerdeki yaklaşımın değerlendirilebilmesi ve Yönerge hükümlerinin uygulama itibarıyla iki yoruma da açık olduğunun belirlenmesi açısından yol gösterici olabilir.

Olayda, yetkili makam, şikayet üzerine elde edilen ve tutulan dosyalardan elektronik ortamda olanları paylaşmış ve fakat elle tutulan dosyaların bir kopyasını teslim etmeyi ise reddetmiştir. Bilgisayar ortamında kişinin adının yazılarak arama yapılması üzerine elde edilecek bilginin kişisel veri olmasını daha belirleyici olarak görmüştür. Fakat o kişiye dair, bazı yerlerde ona sadece değinmiş olan elle tutulan dosyalardaki bilgiyi ise doğrudan kişisel veri olarak değerlendirmemiştir.³⁹⁹ Kararda İngiliz Yüksek Mahkemesi, belirlenebilir kılma üzerine değil de, bilginin o kişiye ilişkin veya o kişiyle ilgili olması üzerine yoğunlaşmaktadır.⁴⁰⁰ Bu bağlamda bir kişinin özel yaşamının gizliliğini etkileyen bilginin kişisel olduğu kabul edilerek iki tür test uygulanabileceği önerilmektedir. Bunlardan ilkinin, genel olarak kişiyi ilgilendirdiği varsayılan bilginin değil de, onun hakikaten yaşamına dair (biyografik/**biographical**), özel yaşamının gizliliğine saygı bağlamında ödün veremeyeceği olaylar ve bunlara dair bilgilerin bu kavramı oluşturacağıdır. İkinci test ise, veri konusu üzerine odaklanılması gerekliliği üzerinedir. Buna göre, söz konusu bilginin asıl konusu, kişiyle bir şekilde ilişkili bulunan veya onunla özel ya da profesyonel iş ilişkisi gibi çeşitli yaşam şekilleri içerisinde ilişkide bulunmuş olanlar değil de, veri konusu bir başka deyişle ilgilinin kendisi olmalıdır. Bu bağlamda, kişisel veri o kişinin özel yaşamını örneğin, onun ailevi veya iş ilişkisini ilgilendirmelidir.⁴⁰¹

³⁹⁹ Durant v. FSA, para 28.

⁴⁰⁰ Information Commissioner's Office, **The 'Durant' Case and Its Impact on the Interpretation of the Data Protection Act 1998**, s.2

⁴⁰¹ Durant v. FSA, para 28-31; **The 'Durant' Case and Its Impact on the Interpretation of the Data Protection Act 1998**, s.2.

Aslında bu şekliyle sınırlayıcı bir yorum ve daha az korumacı bir anlayışın benimsenmiş olabileceği de akla gelebilir. Nitekim Mahkeme, veri koruma kanunu olan DPT altında, kişinin sadece adının yazılı olduğu bir belgeyi istemesi üzerine, sadece adının yazılı olmasının, o belgeyi doğrudan kişisel veri haline dönüştürmeyeceği ve ona bir örneğinin de teslim edilmesini garanti etmeyeceği şeklinde bir değerlendirmede bulunmuştur. Belgenin bu kişiye ait adresi, telefon numarası veya hobileri gibi başkaca bilgilerini de içermesi durumunda kişisel veri olarak nitelendirilebileceği belirtilmiştir.⁴⁰² Ayrıca ikinci test bakımından da, elde edilen bilginin veri sahibi odak alınarak değil de, bir kuruluşa dair bir soruşturma esas alınarak elde edildiği ve bunun da kişisel veri kavramı içinde kabul edilmesini etkileyeceği de ifade edilmiştir.⁴⁰³ Bunun üzerine daha korumacı ve geniş bir yaklaşım benimsenmesi gerekliliği üzerine, DPT'yi uygulamaya dair Mahkeme'nin bu anlayışının eleştirilmiş olduğu da dikkate alınsa bile şu husus unutulmamalıdır. Bahsedilen bu uygulanabilecek testler, bir bilginin kime ait olduğunun açıkça ifade edilemediği durumlarda önem kazanacaktır. Nitekim iletişimin denetlenmesi yoluyla kişisel veri elde edilmesi üzerine tartışmaya yer vermeyecek şekilde o kişiye ait bir bilgi olduğu veya onu belirlenebilir kıldığı anlaşılan bilgi hakkında, elde edilen bilgiyi koruyucu, kişinin bu veri hakkında bilgilendirilmesine özen gösterici ve kavramı daha geniş yorumlayıcı bir yaklaşım sergilenebileceği açıktır.

Özel yaşama yoğunlaşılması ve özel yaşamın gizliliğini korumanın temel amaç haline getirilmesi söz konusu olduğunda, şu hususun da kişisel veri kavramının değerlendirilmesinde yol gösterici olabileceği tartışılmıştır. Kişisel veri olup olamayacağı tartışılan bilgi üzerinde, kişinin belli derecede kontrol imkanının da olması gerekmektedir.⁴⁰⁴ Kanımızca aslında bu yaklaşım temelinin, çalışmanın birinci bölümünde özel yaşamın gizliliğine dair temel yaklaşımlar ifade edilirken açıklandığı gibi, kişinin kişisel gelişimini ve hatta bağımsızlığını sürdürebilmesi için kendisini belirli kılan bilgi üzerinde kontrolünün olması gerektiği anlayışında bulur. Fakat burada şu unutulmamalıdır ki, sadece kontrol odaklı bir kişisel veri anlayışı, kontrol

⁴⁰² Durant v. FSA, para 28, 29.

⁴⁰³ Durant v. FSA, para 28.

⁴⁰⁴ McCullagh, a.g.m., s. 22.

odaklı özel yaşamın gizliliğinin korunması yaklaşımında olduğu gibi tartışmaya esaslı bir yön vermeyebilir ve hatta tartışmayı eksik bırakabilir. Zira kişinin bu tür bilgi üzerinde kontrol imkanı devamlı olarak bulunmayabilmektedir. Kaldı ki, kişi kendisine ait bir bilgiyi örneğin iş veya arkadaşlık ilişkisi bağlamında başkasıyla paylaştığı anda o bilginin açığa çıkarılması veya yayılması açısından bir kontrole sahip olmamaktadır.⁴⁰⁵ Bu nedenle sadece kontrol odaklı bir yaklaşım, hangi bilginin kişisel veri bağlamında kabul edilebileceğine ilişkin eksik bir anlayış sergileyebilir.

95/46 no'lu Yönerge'nin kişisel veri elde edilmesi ve bu verinin işlenmesi konusunda düzenlemeci bir yaklaşım ortaya konulduğu söylenebilir. Fakat aynı anlayışın verinin zararlı olarak kullanılması açısından benimsenmediği görülmektedir. Kaldı ki, Yönerge'ye ilişkin farklı devletlerden uzmanların ve blog yazarların (**blogger**) katıldığı bir çalışmada verinin yanlış toplanmasına ve böylece zarar odaklı bir yaklaşıma geçilebileceği dahi ileri sürülmüştür.⁴⁰⁶ Aynı çalışma çerçevesinde, bunun yanı sıra veri toplamanın da önemli olduğu ve fakat bu tür bilgilerin bir şekilde her zaman toplanacağına; bu nedenle bu bilginin nasıl kullanılacağına dair düzenlemelere de yoğunlaşılması gerektiği şeklinde alternatif düzenleme anlayışlarına yer verilir.⁴⁰⁷

95/46 sayılı Yönerge'nin düzenlediği ilkeleri elektronik haberleşme alanında tamamlamak üzere 15 Aralık 1997 yılında ise, Avrupa Parlamentosu ve Konseyi'nin 97/66 no'lu Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Özel Yaşamın Gizliliğinin Korunmasına Dair Yönerge'yi⁴⁰⁸ kabul ettiği görülmektedir. 97/46 no'lu Yönerge, dijital teknoloji gelişmeler, telekomünikasyon hizmetleri ve interaktif hizmetlerin artması göz önünde tutularak hazırlanmıştır. Yönerge ayrıca,

⁴⁰⁵ McCullagh, **a.g.m.**, s. 21, 22.

⁴⁰⁶ McCullagh, **a.g.m.**, s. 22. Ayrıca bkz.: Sharon Booth, Richard Jenkins, David Moxon, Natasha Semmens, Christopher Spencer, Mark Taylor, David Townend, **What are Personal Data: A Study Conducted for the UK Information Commissioner**, The University of Sheffield, 2004.

⁴⁰⁷ McCullagh, **a.g.m.**, s. 22.

⁴⁰⁸ Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal L 024, 30/01/1998 P. 0001 – 0008, (Çevrimiçi) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML>, 7 Aralık 2011. (Bundan sonra 97/66 no'lu Yönerge olarak anılacaktır.)

yeni hizmetler karşısında bilgi toplumu niteliğinin gelişiminin, telekomünikasyon yoluyla iletişimi tercih edenlerin özel yaşamlarının gizliliğinin risk altında olmadığı yönünde güven duymalarıyla paralel olduğu anlayışıyla hazırlanmış bir belge olarak karşımıza çıkmaktadır.⁴⁰⁹ Bu Yönerge'nin, 95/46 no'lu Yönerge'nin eleştirilen yönlerini içermediği söylenemez; nitekim 95/46 no'lu Yönerge'nin tamamlayıcısı olarak birçok noktada ayrı bir düzenleme getirmeyerek, ona gönderme yapmakla yetindiği ifade edilebilir.

Yönerge, kişisel veri, veri sorumlusu, veri sorumlusunun talimatıyla kişisel veriyi işleyen kişiye ilişkin tanımlar bakımından, 95/46 no'lu Yönerge'ye bir değişiklik getirmemektedir. Bunlara ek olarak, örneğin telekomünikasyon hizmetine dair bir açıklama içermektedir. Buna göre, radyo ve televizyon yayınları hariç, tamamen veya kısmen telekomünikasyon ağındaki sinyallerin aktarılmasını ve gönderilmesini içeren hizmet, Yönerge kapsamında telekomünikasyon hizmeti sayılmaktadır.⁴¹⁰ Üye devletlerin hem iç hukuklarını Yönerge ile uyumlu olarak düzenlemeleri ve uygulamalarını Yönerge ile uyumlu hale getirmeleri hem de bu Yönerge'deki ilkeleri 1998 yılına kadar iç hukuklarına aktarmaları gerektiği hükme bağlanmıştır.⁴¹¹ Devletler bu ilkeleri iç hukuklarında benimserken belirli hususları gözetmelidirler. Bu hususlar aslında Yönerge'nin de içeriğini oluşturmaktadır.

Buna göre öncelikle, telekomünikasyon hizmet sunucuları kamusal telekomünikasyon ağının sağlayıcılarıyla birlikte, hizmetin güvenliğini sağlamak için, teknik ve organizasyonel önlemlerin alınmasını sağlamalıdır.⁴¹² Üye devletler ayrıca iletişimin gizliliğini sağlamakla yükümlü olmakla birlikte,⁴¹³ telekomünikasyon hizmeti çerçevesindeki aramanın yapılabilmesi için yürütülen hizmet sırasında hizmet sağlayıcı tarafından kaydedilen veriler, aramanın sona ermesiyle birlikte ortadan kaldırılmalı veya anonimleştirilmelidir. Bunun yerine bu tür veriler tutmak istenirse, Yönerge hükümleri çerçevesinde faturalandırma işlemi

⁴⁰⁹ "New European Union Privacy Rules Go Into Effect," *The Computer & Internet Lawyer*, C.XXI, No:1, January 2004, s. 21; 97/66 no'lu Yönerge'nin 2 ve 3 numaralı gerekçesi.

⁴¹⁰ 97/66 no'lu Yönerge'nin 2/d maddesi.

⁴¹¹ 97/66 no'lu Yönerge'nin 15/1 maddesi.

⁴¹² 97/66 no'lu Yönerge'nin 4/1 maddesi.

⁴¹³ 97/66 no'lu Yönerge'nin 5. maddesi.

gerçekleştirilmelidir.⁴¹⁴ 97/66 no'lu Yönerge'nin 2003 yılında yürürlükten kaldırıldığı görülmektedir. Zira Avrupa Parlamentosu ve Konseyi'nin 12 Temmuz 2002 tarihinde kabul ettiği, Elektronik Haberleşmenin Gizliliği ve Kişisel Verinin İşlenmesine Dair 2002/58 no'lu Yönerge,⁴¹⁵ 97/66 no'lu Yönerge'nin yerini almıştır.⁴¹⁶ Bu Yönerge'nin düzenlenmesiyle, kamusal olarak ulaşılabilir ağ üzerinden yapılan tüm iletişimler bakımından, kullanılan teknolojiye dair ayırım yapılmaksızın, gizliliğin aynı derecede korunmasını güvence altına almak amacının gözetildiği söylenebilir.⁴¹⁷

Yönerge, benimsediği temel hak ve özgürlüklere saygı gösterilmesi amacının yanı sıra Avrupa Birliği Temel Haklar Şartı'nda düzenlenen hak ve özgürlüklere ilişkin ilkeler göz önünde bulundurma gerekliliğini de hükme bağlamıştır.⁴¹⁸ Bununla birlikte, 95/46 no'lu Yönerge, üye devletlerin tüzel kişileri korumaları imkanını da öngörmektedir ve fakat esas itibarıyla gerçek kişileri korumaktaydı. 2002/58 no'lu Yönerge ile 95/46 no'lu Yönerge tamamlanmış ve bununla birlikte gerçek kişilerin özel yaşamlarının gizliliğinin korunmasının yanı sıra tüzel kişilerin de haklı çıkarlarının korunmasının gözetildiği vurgulanmıştır. Tüzel kişilerin haklı çıkarlarının korunmasının da amaçlandığı belirtilirken ise, böyle bir koruma için üye devletlere 95/46 no'lu Yönerge'nin uygulama alanını genişletme yükümlülüğü yüklenmediği söylenebilir. Nitekim kamusal ulaşılabilirliği olan elektronik iletişim hizmetlerinin sunucuları gerçek kişiler olabileceği gibi; tüzel kişiler de olabilir.⁴¹⁹ Fakat tüm bu hususların, üye devletlerin Yönerge'yi iç hukuklarına aktarma gerekliliğini ortadan kaldırmadığı da açıktır.⁴²⁰

⁴¹⁴ 97/66 no'lu Yönerge'nin 6. ve 7. maddesi.

⁴¹⁵ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002 P. 0037 – 0047, (Çevrimiçi) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>, 7 Aralık 2011. (Bundan sonra 2002/58 no'lu Yönetmelik olarak anılacaktır.)

⁴¹⁶ 2002/58 no'lu Yönerge'nin 4 numaralı gerekçesi.

⁴¹⁷ "New European Union Privacy Rules Go Into Effect," s. 21.

⁴¹⁸ 2002/58 no'lu Yönerge'nin 2 numaralı gerekçesi.

⁴¹⁹ 2002/58 no'lu Yönerge'nin 12 numaralı gerekçesi.

⁴²⁰ 2002/58 no'lu Yönerge'nin 17. maddesi.

2002/58 no'lu Yönerge'nin 95/46 Yönerge ile olan ilişkisi onu tamamlama niteliğini gösterirken, başlangıçta şu ayrım yapılmalıdır. 95/46 no'lu Yönerge, kamu tarafından ulaşılabilir olmayan iletişim; 2002/58 no'lu Yönerge ise kamusal ulaşılabilirliği olan iletişim ile ilgilenmektedir. Kaldı ki, 2002/58 no'lu Yönerge iletişimin gizliliğine daha çok telekomünikasyon sektörü bir başka anlatımla özel iş ilişkisi açısından bakmakta ve bu bağlamda örneğin kamusal iletişimi sağlayan servis sağlayıcılarının sorumluluklarına ilişkin hükümler getirmektedir. Buna rağmen iki Yönerge arasındaki ilişki, birbirini tamamlama özelliğinin yanı sıra, düzenleme konuları açısından da değerlendirilebilir. Bu bağlamda, 2002/58 no'lu Yönerge açıkça, kişilerin hakları ve veri işleme sorumlularının yükümlülükleri de dahil olmak üzere temel hak ve özgürlüklerin korunmasıyla ilgili olarak, özellikle burada düzenlenmeyen konular açısından 95/46 no'lu Yönerge'nin uygulama alanı bulacağını hükme bağlamıştır.⁴²¹

Çalışma konumuz açısından da önem taşıyan kamu güvenliği gibi nedenlerle alınan önlemler ile ilgili olarak ise, 2002/58 no'lu Yönerge'nin önlemlerin uygulanmasıyla ilgili olarak öngördüğü ilkeler ile farklılaştığı söylenebilir. 95/46 no'lu Yönetmelik Birlik hukukunun uygulama alanına girmeyen faaliyetlere ilişkin temel hak ve özgürlüklerin korunması konularını düzenlememektedir. Bu nedenle kişilerin özel yaşamın gizliliği hakları ve AB üyesi devletlerin kamu güvenliği, savunma, devletin güvenliği ve ceza hukuku ile ilgili olarak önlem⁴²² alması olanağı arasındaki dengeyi de değiştirmedığı ifade edilebilir. 2002/58 no'lu Yönerge de, üye devletlerin elektronik iletişimi hukuka uygun olarak denetleme veya AİHS'e uygun olarak başkaca önlem alma imkanlarını etkilememektedir. Fakat bu önlemlerin, AİHS'nin öngördüğü koşullara da uygunluk gösterecek şekilde, demokratik bir toplumda zorunlu, elverişli ve orantılı olması gerektiğini açıkça hükme bağlamıştır.⁴²³

2002/58 no'lu Yönerge altında, üye devletler, iletişimin ve ilgili trafik verilerin gizliliğini sağlamakla yükümlüdürler. Yönerge bağlamında iletişim, kamunun

⁴²¹ 2002/58 no'lu Yönerge'nin 10 numaralı gerekçesi.

⁴²² Bu yasal önlemlerin nitelikleri de yine 2002/58 no'lu Yönerge'nin 15. maddesinde düzenlenmiştir.

⁴²³ 2002/58 no'lu Yönerge'nin 11 numaralı gerekçesi ve 15. maddesi.

ulaşabileceği elektronik hizmet aracılığıyla sınırlı sayıda taraf arasında değiş tokuş edilen veya aktarılan her türlü bilgi olarak tanımlanmaktadır. Bu bilgi, belirlenebilir bir sunucu ya da bilgiyi alan kullanıcıya ilişkin bilgi dışında, elektronik iletişim ağı üzerinden kamuya yapılan yayınları kapsamayacaktır.⁴²⁴ Trafik veri ise, elektronik iletişim ağı üzerinden bir bilginin aktarılması veya faturalama için işlenen veri olarak ifade edilebilir.⁴²⁵ Bu bağlamda üye devletler özellikle bu şekildeki iletişimin ve trafik verilerin, kullanıcının rızası dışında ve ondan farklı bir kişi tarafından dinlenilmesi, kaydedilmesi, depolanması veya başka türlü denetlenmesini yasaklamakla yükümlüdürler. Fakat bu korumanın, ulusal güvenlik, savunma, kamu güvenliği ve suçların önlenmesi gibi nedenlerle sınırlanabileceği öngörülmüştür.⁴²⁶

Kullanıcıların kişisel verilerinin tutulacağı kamuya açık veya istek üzerine ulaşılabilecek basılı veya elektronik rehberler (**directionaries**) hakkında da üye devletler gerekli önlemleri almakla yükümlü kılınmışlardır. Buna göre, kullanıcıların cep telefon veya sabit telefon numaralarının, adreslerinin ve elektronik posta adreslerinin⁴²⁷ bu rehberlerde yer almadan önce, rehberin amacı ve başkaca kullanım imkanları hakkında bilgilendirilmeleri öngörülmektedir. Kullanıcıların bu tür rehberlerde kendilerine ait bilgilerin yer alıp almadığını ve varsa rehberin amacıyla ilişkili olarak hangi kişisel verilerinin bulunduğunu öğrenme; böyle bir kişisel veriyi doğrulamak, düzeltmek veya sildirmek imkanı da üye devletler tarafından güvence altına alınmalıdır. Kaldı ki, bu işlemler herhangi bir ücrete tabi olmayacaktır.⁴²⁸

Söz konusu rehberlerin kamuya açık olduğu da göz önünde bulundurulduğunda, gerçek kişilerin özel yaşamlarının gizliliği hakkının ve tüzel kişilerin de haklı çıkarlarının gereği olarak, kullanıcıların kendisine ait verilerin bu rehberde yer alıp almayacağını belirleyebilecekleri kabul edilmektedir.⁴²⁹ Tüm bu korumalar gerçek kişiler için öngörülürken; tüzel kişiler bakımından da, onların kullanıcı olarak bu tür

⁴²⁴ 2002/58 no'lu Yönerge'nin 2/d maddesi.

⁴²⁵ 2002/58 no'lu Yönerge'nin 2/b maddesi.

⁴²⁶ 2002/58 no'lu Yönerge'nin 5. ve 15. maddesi. Bu sınırlamaların demokratik toplumda zorunlu, elverişli ve orantılı olması gerektiği de kabul edilmiştir.

⁴²⁷ Şimşek, **a.g.e.**, s. 61.

⁴²⁸ 2002/58 no'lu Yönerge'nin 12. maddesi.

⁴²⁹ 2002/58 no'lu Yönerge'nin 8 numaralı gerekçesi.

rehberlerde yer almasına ilişkin yeterli koruma sağlanması için, üye devletler Birlik hukuku çerçevesinde ve fakat ulusal hukukta da uygulanabilecek şekilde önlem almakla yükümlü kılınmışlardır.⁴³⁰

Gerek 95/46 gerek 2002/58 no'lu Yönerge temel hak ve özgürlüklerin korunmasını gözetmekte ve bunlara karşı sınırlayıcı bir müdahale karşısında ne gibi yollar izlenmesi gerektiğini düzenlemektedir. Fakat bu iki düzenlemenin sınırlandırılması söz konusu olduğunda sınırlayıcı unsurun ne olduğunu ise öngörmemektedirler. Bu da öncelikle ilgili sözleşmeler olacaktır.⁴³¹ Nitekim yukarıda da ifade edildiği üzere, üye devletlerin örneğin ceza hukuku alanında kişisel verilerin işlenmesinin öngörülmediği 95/46 no'lu Yönerge'nin kapsamıyla sınırlı kalmayarak, daha geniş bir alanı düzenleme altına alabilmesi mümkündür. Nitekim devletler, tüm ulusal hukukları bakımından uygulanabilir, bağlayıcı olan Avrupa Konseyi'nin "Kişisel Verilerin Otomatik İşlenmesiyle İlgili Olarak Kişilerin Korunmasına Dair Sözleşmesi"ne de bağlılıklarını göz önünde bulundurarak, 95/46 no'lu Yönerge'yi, ulusal hukuklarına aktarırken, ulusal hukuklarının uygulama alanlarını genişletebilmişlerdir.⁴³²

B. Avrupa İnsan Hakları Sözleşmesi

95/46 ve 2002/58 numaralı yönergelerin AİHS'nin ve AİHM'nin yaklaşımını takip ettiği söylenebilir.⁴³³ Öncelikle kişisel verilerin korunmasının, AİHS'de bağımsız bir temel hak ve özgürlük olarak düzenlenmemiş olmasına rağmen, AİHM'nin kararlarından anlaşıldığı üzere, AİHS kapsamında koruma göreceği rahatlıkla söylenebilir. Nitekim Mahkeme, kişisel verilerin elde edilmesi, açıklanması, bu elde etme ve açıklamayı kişinin reddedememesi ve onun bu verilere ulaşımının engellenmesi gibi hususların özel yaşamın gizliliğine müdahale olarak

⁴³⁰ 2002/58 no'lu Yönerge'nin 12/4 maddesi.

⁴³¹ Perez Asinari, *a.g.m.*, s. 242.

⁴³² Perez Asinari, *a.g.m.*, s. 243.

⁴³³ Perez Asinari, *a.g.m.*, s. 241.

nitelendirilebileceğini ve bu bağlamda özel yaşamın gizliliğine saygı hakkının kişisel verinin korunması hakkını da içerdiğini kabul etmektedir.⁴³⁴

AİHM'nin bu yaklaşımının temelini esas itibariyle, kişilerin özel yaşamın gizliliğine saygı hakkı bağlamında bağımsız bireyler olarak kişiliklerine dair ayrıntıları oluşturabilme imkanına sahip olduklarına ve bunu oluştururken de, AİHS'nin 8. maddesi çerçevesinde müdahaleyi haklı kılacak koşullar⁴³⁵ olmadan kamusal makamların bu bilgileri elde etmesi için kişilerin bir engellemeyle karşılaşmalarına dair anlayış oluşturmaktadır.⁴³⁶ Nitekim AİHM, İsviçre'de ulusal güvenlik ile ilgili tutulan indeks bağlamında, Federal Savcılık Ofisinin, başvurusunun Rus büyükelçiliğiyle bağlantılı olduğu ve ticaretle uğraştığına dair bilgileri içeren bir kart düzenlenmesini özel yaşamın gizliliğine saygı çerçevesinde değerlendirmiştir.⁴³⁷ Her şeyden önce, bu iki bilgi, Avrupa Konseyi'nin 108 no'lu Sözleşmesi bağlamında belirli bir kişiye dair veya kişiyi belirlenebilir kılan bilgi bir başka ifadeyle kişisel veri olarak kabul edilmiştir. Bu yönüyle bu kişisel verilerin de özel yaşamı ve AİHS'nin 8. maddesini ilgilendirdiği ileri sürülmüştür.⁴³⁸

Mahkemeye göre, bir siparişte bulunmak üzere eski Sovyet elçiliğinden arayan bir kişiyle telefonda konuşan başvurusunun Federal Savcılık tarafından sadece telefonunun dinlenmesi⁴³⁹ ve bunun üzerine telefonu dinlenen başvuru hakkında kart düzenlenerek, bu kartın da genel indekste tutulması özel yaşamın gizliliği hakkı bağlamında bir müdahale oluşturmaktadır.⁴⁴⁰ Bu nedenle böyle bir kart düzenlenerek kişisel verilerin saklanması, AİHS'nin 8. maddesi çerçevesinde bir değerlendirmeye tabi tutulmuştur ve müdahalenin yasal dayanağı olup olmadığı ve demokratik bir

⁴³⁴ Case of Gaskin v. The United Kingdom, (Application No. 10454/8), Strasbourg, 7 July 1989, para 39; Case of Leander v. Sweden, (Application No. 9248/81), Strasbourg, 26 March 1987, para 48; Case of Rotaru v. Romania, para 44-46.

⁴³⁵ Bu koşullar, daha önce ifade edildiği üzere, genel itibariyle, müdahalenin "yasaya uygunluk / in accordance with the law" koşulunu sağlaması ve böylece açık, belirli ve öngörülebilir bir yasayla temellenmiş olması ve müdahalenin "demokratik bir toplumda gerekli olması / necessary in a democratic society" şeklinde ifade edilebilir, Case of Leander v. Sweden para 49-67; Case of Amann v. Switzerland, para 46-63.

⁴³⁶ Case of Gaskin v. The United Kingdom, para 39 ve 49; Case of Rotaru v. Romania, para 46.

⁴³⁷ Case of Amann v. Switzerland, para 64-80.

⁴³⁸ Case of Amann v. Switzerland, para 65-67.

⁴³⁹ Case of Amann v. Switzerland, para 62 ve 63.

⁴⁴⁰ Case of Amann v. Switzerland, para 75-81.

toplumda gerekli olup olmadığı incelenmiştir. Bu bağlamda da Federal Savcılık yetkililerinin bu alanda gizli telefon dinlemeleri bakımından olduğu gibi, kişisel verileri içeren böyle bir kartı düzenlemelerinde de; onlara bu tür bilgileri elde etme, kaydetme ve saklama yetkisi veren öngörülebilir bir yasal dayanak bulunmadığı sonucuna varılmıştır. Böylece yetkililerin dayanak olarak gösterdikleri ilgili düzenlemelerin, başvurunun özel yaşamın gizliliği hakkına saygıya bu şekilde müdahale edildiğinde yeterli derecede açık ve ayrıntılı bir koruma sağlamadıkları kabul edilmiştir.⁴⁴¹ Bu durumda, AİHS'nin 8. maddesinin ikinci fıkrasına göre müdahalenin demokratik bir toplumda gerekli olup olmadığı bakımından bir inceleme yapılmaya da gerek olmadığı ortaya konulmuştur.⁴⁴² Şu da unutulmamalıdır ki, AİHM bakımından bu şekildeki müdahalenin değerlendirilmesinde, bu kişisel verinin sonradan kullanılıp kullanılmaması bir belirleyicilik oluşturmamaktadır.⁴⁴³

Özetle, bu noktada, AİHM'nin kişisel verilerin elde edilmesini her durumda özel yaşamın gizliliği hakkına bir müdahale olarak görmediği de dikkate alınarak;⁴⁴⁴ kişisel verilere ilişkin 8. madde çerçevesinde yaptığı değerlendirmede şöyle bir yaklaşım sergilediği söylenebilir. AİHM genel olarak iletişimin denetlenmesini özel olarak da telefon dinlemelerini değerlendirdiği gibi, kişisel verilerin korunmasına müdahale edilmesini de özel yaşamın gizliliğine saygı ile ilişkili olarak incelemekte ve iki aşamalı bir değerlendirme yapmaktadır. Öncelikle, müdahalenin yasal dayanağının olup olmadığı, yasanın yeterli açıklıkta olup olmadığı ve ulaşılabilirliği - yasanın kalitesi - incelenmekte ve daha sonra diğer aşamada genellikle ulusal güvenlik gibi bir meşru amaç bağlamında müdahalenin demokratik bir toplumda gerekli olup olmadığı değerlendirilmektedir.⁴⁴⁵

Nitekim İngiltere'de yetkililerin soygun yapılacağı iddiası üzerine, ilgili kişilerin izlenmesi ve gizlice dinlenmesi ile ilgili bir olaya ilişkin başvuruda AİHM, telefon

⁴⁴¹ Case of Amann v. Switzerland, para 75-80.

⁴⁴² Case of Amann v. Switzerland, para 81.

⁴⁴³ Case of Amann v. Switzerland, para 69.

⁴⁴⁴ Case of Leander v. Sweeden, para 52-68; Case of P.G. and J.H. v. The United Kingdom, para 42 ve

⁴⁴⁵

Case of Niemietz v. Germany, para 34-38; Case of Leander v. Sweeden, para 50-67; Case of Rotaru v. Romania, para 45-63; Case of Amann v. Switzerland, para 68-81.

görüşmelerine ilişkin kayıtlara ve soruşturmada kullanılmak üzere polis merkezinde gizlice elde edilen ses kaydına ilişkin değerlendirmede bulunmuştur. Bu olayda, alınan istihbarat üzerine eve cihaz yerleştirilerek konuşmaların dinlenmesi ve telefon kayıtlarının dinlenmesi yoluna başvurulmuştur. Daha sonra kaydedilen seslerle başvurucunun sesini karşılaştırabilmek için de, başvurucunun ses kayıt örneği vermeyi reddetmesi üzerine, başvurucunun hücresine gizlice yerleştirilen cihazla ses örneği alınmıştır.

Mahkeme evde yapılan dinlemelerin bağlayıcı olmayan ve kamunun rahatça ulaşabileceği bir Rehber'e (**Guidelines**) dayandığını belirterek, özel yaşamın gizliliğinin ihlal edildiğini kabul etmiştir. Kişisel veri açısından, olayın ve Mahkeme kararının önem arz eden kısmını, polisin ayrıca Telekomünikasyon Kurumu'ndan başvurucunun kiminle konuştuğuna dair bilgi toplamak için telefon kayıtlarını elde etmesi ve polis merkezinde ses örneği alması oluşturmuştur. Polis merkezinde, soruşturmada kullanılmak üzere ses örneği elde etmek için gizlice ses kaydının alınarak kişisel veri elde edilmesini, AİHS'nin 8. maddesine müdahale olarak değerlendirirken; faturalama amacıyla, bir kişinin telefonla aradığı numaraların neler olduğu ve ne zaman aradığına ilişkin telefon kayıt bilgilerinin elde edilmesini 8. madde çerçevesinde haksız bir müdahale olarak görmemektedir.⁴⁴⁶ Telefon görüşmelerine ilişkin kayıtların alınmasının, Telekomünikasyon Kanunu ve 1984 tarihli Veri Koruması Kanunu faturalama amaçlı böyle bir kayıt tutulmasına olanak verdiğinden ve bu yasal düzenlemelerin de ulaşılabilir ve öngörülebilir olmalarından bahisle yasallık ilkesini karşıladığı kabul edilmiştir.⁴⁴⁷ Ayrıca telefon konuşmalarının içeriğine ilişkin bilgi içermeyen bu tür bir verinin suç işlenmesinin önlenmesi amacıyla polise açıklanmasının da izin verilebilir bir durum olduğu ileri sürülmüştür. Kaldı ki, telefon görüşmelerinin zamanı ile ilgili diğer delillerle birlikte kullanılmak üzere ceza yaptırımlarına ilişkin yargılamada da kullanılması söz konusu ise, bu verinin açıklanması mümkün görülmektedir.⁴⁴⁸

⁴⁴⁶ Case of P.G. and J.H. v. The United Kingdom, para 42-51.

⁴⁴⁷ Mahkeme herhangi bir ölçülülük sorunun olmadığını; demokratik toplumda gereklilik koşulunun da sağlandığını ve 8. madde ihlalinin gerçekleşmediğini ileri sürmüştür, Case of P.G. and J.H. v. The United Kingdom, para 42-51.

⁴⁴⁸ Case of P.G. and J.H. v. The United Kingdom, para 47.

Polis merkezinde, gizlice yapılan dinleme ile ses kayıt örneğinin alınması bakımından ise, başvuru dinlemenin kişilerle ilgili bilgi toplamak yerine, adli (**forensic**) amaçla, karşılaştırma yapmak üzere örnek almak amacıyla olmasının özel yaşamın gizliliği açısından bir fark yaratmadığını ileri sürmüşlerdir. Zira İngiliz kamusal makamları dinlemenin, özel veya esaslı bir bilgi toplamak üzere olmadığını ve herhangi bir müdahale teşkil etmediğini ifade etmişlerdir. Kaldı ki, kişinin sesinin kamusal, dışa dönük bir şey olduğunu ve özel yaşama dair kişisel bir şey olmadığı da vurgulanmıştır. Öyle olmasa bile, suç işlenmesinin önlenmesi ve kamu güvenliği istisnalarının sağlandığı ileri sürülmüştür. Mahkeme ise, aynı fikirde olmamıştır ve gerekçesinde adeta kişisel bilgi ve özel yaşam arasındaki ilişkiyi de açıklığa kavuşturmuştur. Mahkeme'ye göre, özel yaşamın gizliliği sadece kişinin adı ve cinsiyeti gibi bilgileri değil; kişiliğini geliştirme ve dış dünyayla ilişki kurma ve bu ilişkileri geliştirme hususunu da içermektedir. Bu nedenle, kendisine ait ses, görüntü veya başkaca bilgi farklı şekillerde kamu tarafından elde edilebilir. Örneğin, sokakta yürüdüğünde de kamu tarafından görülebilir ve karşı binanın güvenlik kamerasında görüntüsü yer alabilir ve güvenlik görevlisi bu bilgiyi elde etmiş olur. Fakat bu bilginin özel yaşamın gizliliğiyle ilişkisi, kamusal alanlardan böyle bilgilerin alınması sistematik ve kalıcı kayıtlara konu ediliyorsa ortaya çıkar.⁴⁴⁹ Zira bu tür bir ses kaydı, kişisel veri bağlamında kişiyi belirlenebilir kılmaya dair bir analiz sürecine maruz bırakılmaktadır.⁴⁵⁰ Böyle bir faaliyet de, özel yaşamın gizliliği çerçevesinde değerlendirilmektedir.

Görülüyor ki, faturalama amacıyla telefon kayıtlarına dair - içerik elde edilmese de - alınmasının da özel yaşamın ve ayrıca iletişimin gizliliğini ilgilendirdiği kabul edilmektedir.⁴⁵¹ Fakat demokratik bir toplumda suç işlenmesinin önlenmesi gibi 8. madde çerçevesinde müdahaleyi haklı kılacak nedenlere dayanılarak yapılan denetimin doğası ve sınırlı kapsamı da dikkate alındığında, 8. maddeyi ihlal etmediği kanısına varılmaktadır.⁴⁵² Kısacası her iki durumda da - ses kayıt örneği ve telefon kayıtlarının alınması - esasında özel yaşamı ilgilendiren kişisel veriden bahsetmekte

⁴⁴⁹ Case of P.G. and J.H. v. The United Kingdom, para 57.

⁴⁵⁰ Case of P.G. and J.H. v. The United Kingdom, para 59.

⁴⁵¹ Case of P.G. and J.H. v. The United Kingdom, para 42.

⁴⁵² Case of P.G. and J.H. v. The United Kingdom, para 46.

ve fakat aynı içerikte olmayan bilgiden ve aynı koşullarla gerçekleşmeyen bir denetimden söz etmekteyiz. Bu nedenle de, böyle bir durumda yasallık ve demokratik toplumda gereklilik koşullarının belirleyicilik arz ettiğini söyleyebiliriz. Kişisel verilerin korunması özelinde AİHM'nin bu değerlendirmeleri yaparken, sadece kişisel verinin elde edilmesine, kaydedilmesi ve saklanmasına dair bir koruma ile sınırlı bir yaklaşım sergilemediği görülür. Daha geniş bir güvenceden yola çıkarak, örneğin kişisel veriye ulaşılması ve kişinin kendine ait veri üzerindeki bilgi edinme hakkını da bu kapsamda değerlendirdiği söylenebilir. İletişimin gizlice denetlenerek kişisel veriye ulaşılması açısından tam bir örnek sağlamasa da; AİHM'nin bu yaklaşımını anlayabilmek açısından nasıl bir yarar tartımına gittiği şöyle bir örnekle özetlenebilir. Çocuk bakımevlerinde yetişmiş ve çocukluğunda sosyal yardım almış bir kişinin çocukluğuyla, gelişimi ve yetişmesiyle ilgili tutulmuş olan dosyalara ilişkin bilgi istemesi, AİHM tarafından, bir kararında, özel yaşama dair değerlendirilmiştir.⁴⁵³ Böylece, asıl kimliğe ve kişiliğe dair bilgilere ulaşımın engellenmesinin, 8. madde bağlamında gerekçelendirilmesi gerektiği kabul edilmiştir. Bu bilgilerin o dönemki gelişime katkıda bulunmuş öğretmenler, doktorlar ve bakımı üstlenmiş anne-babalardan da alındığı da dikkate alınmıştır.⁴⁵⁴

Bu noktada yararların tartılması tartışılmaktadır. Bu dengelemede de bir yanda gizlilik ilişkisi içinde ve güvene dayalı olarak bu şekilde bilgi vermiş bu kişilerin yararlarının korunması ve bu bağlamda kayıtların gizli tutulmasındaki kamu yararı; diğer yanda da kişinin o döneme ait kendine ilişkin bilgiye ulaşmadaki yararı bulunmaktadır. Böyle bir değerlendirmede kişinin kendine ait veri açısından özel yaşamına saygı duyulması gerektiği kabul edilmekte ve bu bilgiye ulaşmasının engellenmesinin de bu hakkına müdahale olarak nitelendirildiği görülmektedir.⁴⁵⁵

Genel itibarıyla, kişisel veriye ulaşımın kural olarak sınırlanabileceği kabul etmektedir denilebilir. Bu sınırlama için somut olay ve haklı neden araştırmasının birçok Kıta Avrupası mevzuatında da benimsediği görülür. Örneğin, Alman Veri

⁴⁵³ Case of Gaskin v. The United Kingdom, para 34-41.

⁴⁵⁴ Case of Gaskin v. The United Kingdom, para 44.

⁴⁵⁵ Case of Gaskin v. The United Kingdom, para 44.

Koruması Kanunu, veri sahibinin kendisine dair elde edilen ve saklanan bilgi ve saklama nedeni hakkında, isteği üzerine, bilgilendirilmesi olanağını güvence altına almıştır.⁴⁵⁶ Bu, tutulmalarına dair yasal veya sözleşmesel hükümler nedeniyle silinememiş olan ya da münhasıran veri güvenliği veya veri korunması kontrolüne hizmet eden kayıtlı veriler için geçerli olmayacaktır.⁴⁵⁷ Bu bilgilendirilme isteği reddedilirse ve bu reddedilmeye ilişkin hukuki veya gerçek neden açıklanırsa reddedilme nedenini tehlikeye düşürecek nitelikteyse açıklanmaz. Bu durumda da veri sahibi, yetkili federal makama (**Federal Commissioner for Data Protection**) üst başvuruda bulunabilir. Veri sahibine hiçbir bilgi verilmez ise, veri sahibi ona sağlanmayan bilginin yetkili federal makama sağlanmasını talep edebilir. Bu talep de, somut olayda federal yetkili makama bilgi açıklanması devlet güvenliğini tehlikeye düşürecekse reddedilebilir.⁴⁵⁸

C. Avrupa Birliği Temel Haklar Şartı

Kişisel verilerin korunması, sadece AIHS ve Avrupa Birliği yönergelerinde değil; Avrupa Adalet Divanı yaklaşımında ve diğer başkaca bağlayıcı düzenlemelerin hükümlerinde de, temel hak ve özgürlükler ışığında yorumlanması gereken bir kavram olarak dile getirilmektedir.⁴⁵⁹ Bu bağlamda kişisel verilerin korunduğu Avrupa Birliği mevzuatındaki diğer esaslı belge Avrupa Birliği Temel Haklar Şartı⁴⁶⁰ olarak karşımıza çıkmaktadır. Şart, 2000 yılında Avrupa Komisyonu, Konsey ve Avrupa Parlamentosu tarafından Nice Zirvesinde ilan edilmiştir.⁴⁶¹ Şart ilk olarak Avrupa İçin Anayasa Oluşturan Antlaşma (AB Anayasa Taslağı)'ya, bağımsız bölüm

⁴⁵⁶ Simitis, **From the Market to the Polis: The EU Directive on the Protection of Personal Data**, s. 460; Federal Veri Koruma Kanunu'nun 19. maddesi, Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), In the version published on 20 December 20, 1990 (BGBl. I 1990 S.2954), as amended by the law of 14 September, 1994 (BGBl. I S. 2325), (Çevrimiçi) <http://www.iuscomp.org/gla/statutes/BDSG.htm>, 11 Aralık 2011.

⁴⁵⁷ Federal Veri Koruma Kanunu'nun 19. maddesinin 2. fıkrası.

⁴⁵⁸ Federal Veri Koruma Kanunu'nun 19. maddesinin 5. ve 6. fıkrası.

⁴⁵⁹ Christopher Kuner, **European Data Protection Law, Corporate Compliance and Regulation**, 2. bs., New York, Oxford, 2007, s. 18,19.

⁴⁶⁰ Charter of Fundamental Rights of the European Union, 18.12.2000, 2000/C/364, (Çevrimiçi) http://www.europarl.europa.eu/charter/pdf/text_en.pdf, 13 Aralık 2011.

⁴⁶¹ Grainne de Burca, "Beyond the Charter: How Enlargement Has Enlarged the Human Rights Policy of the European Union," **Fordham International Law Journal**, C.XXVII, 2003-2004, s. 688, 689.

oluşturacak şekilde, tam metin olarak dahil edilmiştir.⁴⁶² Reddedilen AB Anayasa Taslağı'nın yerini alan, 2007 yılında kabul edilen ve 2009'da onay süreci tamamlanan Lizbon Antlaşması'na⁴⁶³ yapılan bir atıfla hukuki olarak bağlayıcı hale gelmiştir.⁴⁶⁴ Avrupa Adalet Divanı da,⁴⁶⁵ Lizbon Antlaşması'ndan yaklaşık bir ay sonra verdiği bir kararda, AB Temel Haklar Şartı'na açık bir göndermeyle Şartın hukuki statüsünü belirlemiştir.⁴⁶⁶ Bundan itibaren Şart'a, temel insan hakları kaynaklarından biri olarak açıkça atıfta bulunulmaya özen gösterildiği görülebilir.⁴⁶⁷ Bu durum sadece Şart'ın değil, aynı zamanda verilerin korunmasına dair ilgili yönergelerin, kişisel verileri ve özel yaşamın gizliliğine saygı hakkını korumaya ilişkin yaklaşımının yansıması açısından da önemli kabul edilmelidir.⁴⁶⁸

AB Temel Haklar Şartı, hem herkesin özel yaşamına ve haberleşme özgürlüğüne saygı gösterilmesini hem de kişisel verilerin korunmasını bağımsız birer temel hak olarak güvence altına almaktadır.⁴⁶⁹ Buna göre, AİHS'in 8. maddesinde güvence altına alınan özel yaşamın gizliliği hakkına saygı gösterilmesi, Şart'ın 7. maddesine tekabül etmektedir.⁴⁷⁰ Maddenin gerekçesinde bu hususun dışında, teknolojideki gelişmeler göz önünde bulundurularak haberleşme (**correspondence**) kavramı yerine, iletişim (**communication**) kavramının tercih edildiği de açıklanmıştır. AB Temel Haklar Şartı'na göre, Şart'ta yer alan hakların, anlamı ve kapsamı açısından,

⁴⁶² Bertil Emrah Oder, *Avrupa Birliği'nde Anayasa ve Anayasacılık*, İstanbul, Anahtar, 2004, s. 318, 319.

⁴⁶³ Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, C. LI, Official Journal of the European Union, 9 May 2008, C 115/19.

⁴⁶⁴ Sonia Morano-Foadi, Stelios Andreadakis, "Reflections on the Architecture of the EU after the Treaty of Lisbon: The European Judicial Approach to Fundamental Rights," *European Law Journal*, C.XVII, No:5, Eylül 2011, s. 595. AB Temel Haklar Şartı'nın, AB Anayasa Taslağı'nın kabulünden önce dahi, içeriği ve kapsadığı hukuki esaslar bakımından bağlayıcılık taşıdığının göz ardı edilmemesi gerektiği de ileri sürülmüştür, A. Fusun Arsava, "Avrupa Temel Haklar Şartı," *Ankara Avrupa Çalışmaları Dergisi*, C.V, No: 1, 2005, s. 12.

⁴⁶⁵ Avrupa Adalet Divanı (Court of Justice) ve Lizbon Antlaşması sonrasında Mahkemenin yapısı ve işlevi ile ilgili değişiklikler için bkz.: Josephine Steiner, Lorna Woods, *EU Law*, 10. bs., New York, Oxford, 2009, s. 43-47.

⁴⁶⁶ Anja Wiesbrock, Case Note – Case C-555/07, *Kücükdeveci v. Swedex*, Judgment of the Court (Grand Chamber) of 19 January 2010, s. 541.

⁴⁶⁷ Morano-Foadi, Andreadakis, *a.g.m.*, s. 598.

⁴⁶⁸ Dan Manolescu, "Data Protection as a Fundamental Right," *Effective Justice Solutions*, Published as part of the Effectius Newsletter, Issue 5, 2010, s. 2.

⁴⁶⁹ Avrupa Temel Haklar Şartı'nın 7. ve 8. maddesi, Charter of Fundamental Rights of the European Union, C 364/10.

⁴⁷⁰ Draft Charter of Fundamental Rights of the European Union, Charte 4473/00, Brussels, 11 October 2000, s. 10, (Çevrimiçi) http://www.europarl.europa.eu/charter/pdf/04473_en.pdf, 13 Aralık 2011.

üye devletlerin daha geniş koruma sağlamalarına engel olmayacak şekilde AİHS’de düzenlendiği şekilde ele alınması kabul edilmiştir. Bu bağlamda AİHS’nin 8. maddesinin 2. fıkrasında hükme bağlanan özel yaşamın gizliliği hakkının sınırlandırılmasına dair esasların, Şart’ın bu düzenlemesine karşılık gelecek şekilde uygulanabileceği düşünülebilir.⁴⁷¹

AB Temel Haklar Şartı’na göre kişisel veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak işlenmelidir. Ayrıca herkes, kendisiyle ilgili elde edilmiş verilere ulaşma ve bunları düzelttirme hakkına sahiptir. Bağımsız bir makamın ise, bu kurallara uyulmasını denetlemesi öngörülmüştür.⁴⁷² Korunacak kişisel verinin ne olduğuna dair AB Temel Haklar Şartı’nda bir hüküm olmadığı görülmektedir. Bu nedenle, 95/46 no’lu Yönerge’de düzenlenmiş olan şekliyle belirli veya belirlenebilecek bir gerçek kişiye ilişkin her türlü bilgi, Şart açısından da kabul edilebilir. Zira Şart’ta yer alan kişisel verilerin korunmasına dair güvence dayanağını Avrupa Topluluğu Antlaşması’nın 286. maddesi,⁴⁷³ 95/46 no’lu Yönerge, AİHS’nin 8. maddesi ve Avrupa Konseyi’nin Kişisel Verilerin Otomatik İşlenmesiyle İlgili Olarak Kişilerin Korunmasına Dair 108 no’lu Sözleşmesi’nden almaktadır.⁴⁷⁴ Bu bağlamda, hakkın sınırlanması açısından da, Şart’ın 52. maddesi gereğince yine AİHS’de öngörülen sınırlama nedenleri dikkate alınacaktır. Böylece bu hakkın kullanılmasına yapılacak bir müdahalenin, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda Birliğin güvenliği, ekonomik refahı, düzenin korunması ve suç işlenmesinin

⁴⁷¹ AB Temel Haklar Şartı’nın 7. maddesine ilişkin açıklama (Explanation of article 7), Draft Charter of Fundamental Rights of the European Union, s. 10.

⁴⁷² Avrupa Temel Haklar Şartı’nın 8. maddesinin 2. ve 3. fıkrası, Charter of Fundamental Rights of the European Union, C 364/10.

⁴⁷³ Avrupa Topluluğunu Kuran Antlaşma’nın 286. maddesi, 1 Ocak 1999 tarihinden itibaren kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve kişisel verilerin serbest veri trafiğine Topluluk düzenlemelerinin, bu Antlaşmaya dayanarak veya bu Antlaşma tarafından kurulmuş kuruluşlara ve organlara uygulanacağını hükme bağlamaktadır. Bunun dışında, 1 Ocak 1999’dan önce, Konsey’in, Topluluğun bu hukuki düzenlemelerinin ilgili kuruluşlarda ve organlarda uygulanmasını denetlemek üzere bağımsız bir kontrol organı kurulması için gerekeni yapacağı ve gerekli diğer düzenlemeleri de kabul edeceği düzenlenmiştir, Consolidated Version of the Treaty Establishing the European Community, 24.12.2002, C 325/147.

⁴⁷⁴ AB Temel Haklar Şartı’nın 8. maddesine ilişkin açıklama (Explanation of article 8), Draft Charter of Fundamental Rights of the European Union, s. 11.

önlenmesi veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabileceği düşünülebilir.

Şart'ta kişisel verilen işlenmesinden, kişilerin bu veriye ulaşmasından söz edilmişse de, veri işlemeye dair öngörülecek esaslara yer verilmemiştir. Bu noktada, Şart'ta güvence altına alınan kişisel verilerin korunması hükmünün dayanaklarından biri olan 95/46 no'lu Yönerge'nin kişisel verilerin işlenmesine dair kabul ettiği ilkelerin burada da uygulanması gerektiği söylenebilir. Buna göre somut olayda veri sahibinin rızasının aranması ve bilgilendirilmesine ilişkin şartların gerçekleşmesi beklenebilir.

Sonuç olarak kanımızca, A.B.D. hukukundaki özel yaşamın gizliliği - **privacy** - kavramının tam anlamıyla olmasa da Kıta Avrupası anlayışında kişisel verinin korunması - **data protection** - olarak karşımıza çıktığı şeklindeki daha önce ifade ettiğimiz değerlendirme, kişisel veri ve özel yaşamın gizliliği arasındaki ilişki incelendiğinde aslında teorik temelde de kendini gösterir. Kaldı ki, kişisel verinin korunması, özel yaşamın gizliliğinin her yönünü olmasa da, iletişimin denetlenmesi bağlamında özel yaşamın gizliliğini neredeyse belirlercesine, bu hakla ilişkilidir. Kişisel verilerin korunması ile iletişimin denetlenmesi bağlamında özel yaşamın gizliliği hakkı arasında sıkı bir ilişki olduğu anlayışının, gerek A.B.D. gerek Kıta Avrupası anlayışının, konuya ilişkin, ortak noktalarından birini oluşturduğu söylenebilir. Kişisel verinin özel yaşamın gizliliğini açıklamaya neredeyse temel oluşturduğu anlayışın, özel yaşamın her yönü bakımından aynı kesinlikle söylenememesi, özellikle Amerikan hukukunda kendini gösteren bir anlayışla ve özel yaşamı bilgi üzerindeki kontrol ile bağlantılandıran yaklaşıma⁴⁷⁵ kısaca tekrar değinilerek de ifade edilebilir.

Özel yaşamın gizliliğinin karar verme açısından ele alınmasında - **decisional privacy** - bir kişinin örneğin doğurganlığa veya çocuk yetiştirmeye ilişkin konularda olduğu

⁴⁷⁵ Bu yaklaşımın, özel yaşamın gizliliğini büyük çoğunlukla kişinin bilgi üzerindeki kontrol imkanıyla açıklayan (privacy-control paradigm) görüşten etkilenecek ortaya atılabileceği söylenebilir. Bu nedenle özel yaşamı kontrol unsuruyla sınırladığı gerekçesiyle bu görüşün de eleştirildiği görülmektedir, Anita Allen, **Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm**, s. 866-869.

gibi, hayatına ilişkin belirli önemli kararları almasına müdahale edilmesi söz konusudur.⁴⁷⁶ İletişimin gizliliği bakımından özel yaşamın korunmasında ise - **informational privacy** - çoğunlukla kişinin yaşam ilişkileriyle şekillenen kişisel verinin kullanılması ve el değiştirmesini de içerecek şekilde işlenmesi belirleyici olarak karşımıza çıkmaktadır. Fakat şu da unutulmamalıdır ki, karar vermeye dair, **decisional privacy**, ve iletişimin gizliliği bağlamında özel yaşam, **informational privacy**, birbiriyle hiç de ilgili olmayan kavramlar değildir.⁴⁷⁷ Aslında aralarındaki bağlantı en yalın şekliyle şöyle özetlenebilir: Kişisel verinin kamu veya özel kurum veya kuruluşlarca elde edilmesi, kullanılması veya başkaca şekillerle işlenmesi, hayata dair alacağımız kararları da etkileyebilme özelliği gösterecektir.⁴⁷⁸ Kısacası, kişisel verinin işlenmesi ile özel yaşamın gizliliği arasındaki ilişkinin, kişisel veriye ulaşılmasının hem kişisel özerklik olarak ortaya çıkan kişisel karar alabilme yetkisini hem de demokratik toplum düzeninin devamlılığını sağlamayı etkilediği gerçeğinden temel aldığı ve bir o kadar da bu etkileşimle paralellik gösterdiği söylenebilir.

Aslında, A.B.D. ve Kıta Avrupası hukuku anlayışının kişisel verilerin korunmasının özel yaşamın gizliliğiyle olan ilişkisi konusunda temelde paralellik göstermesi çok da beklenmeyen bir sonuç olarak karşılanmamalıdır. Zira bu iki hukuk anlayışı açısından çatışma içinde olan şey, kişisel verilerin korunmasının özel yaşamla ilişkisi değil; Kıta Avrupası'nın özel yaşamın gizliliğine, A.B.D.'nin de ulusal güvenliğe olan hassasiyeti⁴⁷⁹ olarak değerlendirilebilir.

Kıta Avrupası'nda sosyolojik veya belki tarihi gelişmelerin ve insanların kimliklerinin ve kişisel bilgilerinin yayılmasının kötüye kullanılma örnekleriyle çok fazla karşılaşılması, kişisel verilerin korunmasına duyulan bu hassasiyetin nedenleri

⁴⁷⁶ Roe et al. v. Wade, 410 U.S. 113, 1973; Schwartz, **Property, Privacy, and Personal Data**, s. 2058.

⁴⁷⁷ Schwartz, **Property, Privacy, and Personal Data**, s. 2058, 2059.

⁴⁷⁸ Bu bağlantı özellikle, kürtaj ile ilgili davalarda kurulabilir. Bir kişinin bu imkandan gerekli düzenlemeler dahilinde yararlanabilmesi için kimi durumlarda kişisel bilgilerinin bazılarının kaydedilmesi veya doktorlar tarafından ilgili kurumlarla paylaşılması gerekebilmektedir, Eric Lichtblau, **Defending '03 Law, Justice Dept. Seeks Abortion Records**, The New York Times, 12 Şubat 2004. Bu gibi olaylarda karar vermeye ve iletişimin gizliliğine dair özel yaşam kavramlarının iç içe geçtiği ve her ikisinin de belirleyici olduğu görülebilir.

⁴⁷⁹ Christopher Slobogin, **Privacy at Risk: The New Government Surveillance and the Fourth Amendment**, USA, The University of Chicago, 2007, s. 3, 4.

arasında görülebilir. A.B.D.’de de, yine belki sosyolojik nedenlerle özel yaşamın gizliliğinden Avrupaya nazaran biraz daha fazla ödün verilmesinin olabilir görülmesi, uzun süre devam etmiş ve halen devam eden ulusal güvenlik sorunları ve devamlı hissedilen güvenlik tehdidi olabilir.⁴⁸⁰ Kaldı ki, A.B.D. anlayışında dahi sınırlanması mümkün görülen husus, tam olarak özel yaşamın gizliliğine saygı değildir. Belirleyici olan ulusal güvenliğin sağlanması için kişisel verilerin paylaşılmasının daha makul karşılanmasıdır.⁴⁸¹

III. KİŞİSEL VERİLERİN KORUNMASINA DAİR TEMEL İLKELER

İlgilinin kişisel verilerin hukuka uygun olarak işlenmesi sırasında haberdar edilmesi ve bilgi edinme hakkı, kişisel verilerin düzeltilmesini, silinmesini ve yok edilmesini isteme ve itiraz hakkı, kişisel verilerin işlenmesinde ölçülülük ve ön denetim ilkesi, kişisel verilerin işlenebilmesi için ilgilinin rızasının gerekliliği ilkesi, kişisel verilerin hukuka aykırı işlenmesi halinde tazminat, kişisel verilerin işlenmesinin denetiminin bağımsız denetim organlarınca gerçekleştirilmesi kişisel verilerin korunmasına ilişkin temel esasları belirlemektedir. Bu esaslar aynı zamanda iletişimin denetlenmesi sonucu elde edilen kişisel verilerin işlenmesinde uyulması gereken şartlar olarak da görülmelidir. Bu bağlamda özel yaşamın bir parçası olarak iletişimin gizliliği açısından önemi de dikkate alınarak, kişisel verilerin korunmasına dair ilkeler, Avrupa Birliği mevzuatı kapsamında korumanın hukuki zeminini oluşturan belgeler ışığında incelenebilir. Özellikle 95/46 no’lu ve 2002/58 no’lu Yönerge esas alınacak olmakla birlikte, genel itibariyle AB organları ve kurumlarının kendi faaliyet alanlarında kişisel veriyi işlemelerine dair ilkeleri düzenleyen 45/2001 no’lu Tüzüğün de ilkelere ilişkin benzer yaklaşımı benimsediği söylenebilir.

⁴⁸⁰ Megan Roos, “Definiton of the Problem: The Impossibility of Compliance with Both European Union and United States Law,” *Transnational Law & Contemporary Problems*, C.XIV, t.y., s. 1161, 1162.

⁴⁸¹ Roos, *a.g.m.*, s. 1168.

A. Kişisel Verilerin Kaliteli Olması

Avrupa Konseyi'nin 108 no'lu Sözleşmesi ve 95/46 no'lu Yönerge, kişisel verilerin kaliteli olması ilkesi bağlamında, öncelikle adil ve hukuka uygun olarak elde edilmesi ve işlenmesi gereğini ortaya koymaktadır.⁴⁸² Buna göre, verinin adil işlenmesi, açıklığı beraberinde getirmelidir. Bir kişiye ait veri, gizli bir amaç için işlenemez. Kaldı ki, bu ilke ilgilinin/veri konusunun, veri işleme sorumlusunun kimliği ve bu işlemenin amacı hakkında bilgilendirilmesini de içermektedir.⁴⁸³ Verinin hukuka uygun işlenmesi ise, ulusal düzenlemelerle uyumlu olarak işlenmesini gerektirecektir. Bu bağlamda örneğin saklanan veri trafiği durumlarında, böyle bir verinin açıklanması ancak ulusal hukukun yetkilendirmesi söz konusu ise hukuka uygun gerçekleşmiş sayılacaktır.⁴⁸⁴ Görülüyor ki, yasal dayanağı olmayan ya da yasada düzenlenmiş bir amaca aykırı olarak gizlice kişisel veri elde edilmesi ve işlenmesi, bu adil ve hukuka uygun işleme ilkesine aykırılık teşkil edecektir.

Kişisel veriler bunun yanı sıra, amaca bağlılık ilkesi olarak da özetleyebileceğimiz şekilde, yasal olarak açık ve sınırları belirlenmiş amaçlarla işlenebilecektir. Aslında bu ilkenin uygulamaya yansıyacak önemli taraflarından biri, veri işleme sorumlusunun söz konusu veriyi hangi amaçla elde ettiği ve işlediğinin böylece, sonradan da olsa, amaca uygunluk açısından denetlenebilecek olmasıdır.⁴⁸⁵ Yasayla açıkça ortaya konulmuş amaç ötesinde tarihi, istatistiksel veya bilimsel amaçlarla verinin işlenmesi, devletlerin yeterli güvenceleri sağlamaları halinde, 95/46 no'lu Yönerge ile bağdaşmayan amaçlar olarak nitelendirilmeyebilecektir.⁴⁸⁶ Bir başka anlatımla bu durumda amaca bağlılık ilkesine uygunluğun sağlanmış olduğu kabul edilecektir.

⁴⁸² 108 No'lu Sözleşme'nin 5/a maddesi; 95/46 no'lu Yönerge'nin 6/a maddesi.

⁴⁸³ Perez Asinari, **a.g.m.**, s. 239.

⁴⁸⁴ Perez Asinari, **a.g.m.**, s. 239.

⁴⁸⁵ Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin, 2004, s. 37, 38; Şimşek, **a.g.e.**, s. 83, 84.

⁴⁸⁶ 95/46 no'lu Yönerge'nin 6/1-b maddesi.

Veri kalitesi bağlamında değerlendirilebilecek diğer ilke ise, gereklilik ilkesi olarak da ifade edilen,⁴⁸⁷ kişisel verinin toplanma ve işlenme amacını aşmayacak şekilde, ulaşılmak istenen amaçla ilgili ve yeterli olması şeklinde ifade edilebilir.⁴⁸⁸ Aslında bu ilke, verinin hangi kapsamda ve miktarda toplanacağını belirlenmesi açısından önem arz edecektir. Unutulmamalıdır ki, gereklilik, amaçla bağlantılı olarak belirlenebilecek bir husustur. Örneğin, kaç kişinin bir sistemi kullandığı hakkında bilgi toplanmak isteniyorsa, bu kişilerin kimler olduğu ve nelerle uğraştığıyla da ilgili bilgi toplanmak istenmesi bu ilkeyle bağdaşmayacaktır.⁴⁸⁹ Bununla birlikte, verinin sadece yasayla belirlenmemiş, sınırlı olmayan amaçla toplanması değil; toplama amacı ortadan kalkmış olmasına rağmen saklanması da kişisel verinin hukuka uygun işlenmesi gerektiğine dair ilkeye aykırılık oluşturacaktır.⁴⁹⁰ Aslında bu husus, kişinin kendisine ait bilgi toplandıktan ve istenen amaca ulaşıldıktan sonra, verinin bilgisi dışında ve başka bir amaçla işlenmeyeceği hakkında güvenceye sahip olması gerektiğinin bir uzantısı olarak kabul edilebilir.⁴⁹¹

B. Kişisel Verinin İşlenebilmesi İçin İlgilinin Rızasının Aranması İlkesi

Kişisel verinin işlenebilmesi için, ilgilinin rıza göstermesi aranmaktadır.⁴⁹² Bu bağlamda, 95/46 no'lu Yönerge'nin 2/h maddesinde ifade edildiği üzere, ilgili kişinin serbest iradeyle, belirli olay için ve bilgilendirilmiş olarak kendisine ait verilerin işlenebilmesine dair irade beyanı, ilgilinin rızası olarak kabul edilecektir. Bu rızanın serbest iradeyle verilmiş olması, herhangi bir baskı altında kalmadan verilmesini; rızanın belirli olması ise, veri işleme sorumlusunun, söz konusu veriyi işlemek üzere

⁴⁸⁷ Başalp, **a.g.e.**, s. 38.

⁴⁸⁸ 95/46 no'lu Yönerge'nin 6/1-c maddesi.

⁴⁸⁹ Perez Asinari, **a.g.m.**, s. 239, 240.

⁴⁹⁰ Kaldı ki, verinin amacı gelecekte karşılaması öngörülüyorsa başka bir deyişle sadece gelecekteki olası kullanımı için tutuluyorsa, böyle bir verinin depolanması ve ortadan kaldırılmaması da yasaklanmıştır. Bu tür bir verinin daha fazla saklanmaması ve silinmesi gerektiği ileri sürülebilir, Başalp, **a.g.e.**, s. 38.

⁴⁹¹ Şimşek, **a.g.e.**, s. 85.

⁴⁹² 95/46 no'lu Yönerge'nin 7/a maddesi.

İlgiliden rıza aldıktan sonra aynı veriyi başka bir amaçla ilgili kişinin rızasını tekrar almadan işleminin mümkün olmamasını gerektirmektedir.⁴⁹³

İlgili, veri işleme sorumlusundan gerekli bilgileri almış olarak, kendisine ait bilginin veri işleme faaliyetlerine konu olacağının farkındalığıyla bu rıza beyanında bulunmalıdır. İlgilinin kural olarak yazılı vermesi beklenmekle birlikte, rıza vermemesi halinde bu kararını gerekçelendirmesi zorunlu görülmemektedir.⁴⁹⁴

95/46 no'lu Yönerge bağlamında kişisel verilerin hukuka uygun işlenebilmesi için belli durumlar öngörülmüştür. Bunlardan birinin sağlanması, devletlerin böyle bir veri işleme için kişisel veri toplayabilmelerine olanak verecektir. İlgili kişinin açık bir irade beyanının olması bu durumlardan biri olarak karşımıza çıkmaktadır.⁴⁹⁵ Bununla birlikte veri işleminin gerekli olduğu diğer birkaç durum da bu koşulları oluşturmaktadır. Buna göre, ilgilinin taraf olduğu bir sözleşmenin yerine getirilmesi veya kendi isteğiyle, sözleşme yürürlüğe girmeden önce gerekli işlemlerin yapılması ve veri işleme sorumlusunun hukuki bir yükümlülüğünün yerine getirilmesi bakımından gerekli olması, üye devletlerin veri toplaması açısından sayılan koşullardan bazılarıdır. Bunun dışında, veri işleminin ilgili kişinin hayati çıkarlarının korunması ve kamu çıkarına hizmet eden bir görevin yerine getirilmesi bakımından gerekli olması da veri toplanabilmesi için sağlanacak koşullardandır.⁴⁹⁶

Özellikle kamu yararına hizmet eden bir işlemin gerçekleştirilmesi veya veri işleme sorumlusunda var olan kamusal bir yetkinin yerine getirilmesi için veri toplanması koşulu konumuz açısından önemli sayılabilir. Zira bu ilke, genelde kamusal makamların veri işlemesi, özelde de polis veya başkaca yetkililerin kişisel veri işlemesi açısından uygulanmalıdır.⁴⁹⁷ Son koşul ise, ilgili kişinin temel hak ve özgürlüklerinin korunması menfaati üstün gelmedikçe, veri işleme sorumlusu, üçüncü kişiler veya verinin açıklanacağı diğer kişilerin haklı çıkarlarının korunması

⁴⁹³ Perez Asinari, **a.g.m.**, s. 240.

⁴⁹⁴ Bainbridge, **a.g.e.**, s. 60.

⁴⁹⁵ 95/46 no'lu Yönerge'nin 7/a maddesi.

⁴⁹⁶ 95/46 no'lu Yönerge'nin 7/b, c, d, e maddesi.

⁴⁹⁷ Perez Asinari, **a.g.m.**, s. 241.

için gerekli olması şeklinde ifade edilebilir.⁴⁹⁸ Burada üçüncü kişilerin haklı menfaatlerinin olup olmadığı genellikle üye devletler tarafından belirlenecektir.⁴⁹⁹

C. Hassas Verilerin İşlenmesi

İlgili kişinin etnik kökeni, politik düşüncesi, dini veya felsefi inancı, sağlık veya cinsel durumunu ortaya çıkaran veriler, özel kategorideki (hassas) veriler olarak nitelendirilmekte ve bu tür verilerin işlenmesi kural olarak yasaklanmaktadır.⁵⁰⁰ Kaldı ki, bu kuralın korunduğu tek belge, 95/46 no'lu Yönerge değildir; 108 no'lu Avrupa Konseyi Sözleşmesi de, aynı şekilde bu nitelikteki hassas verilerin ve bu bağlamda kişinin korunmasına hizmet eden bu güvenceyi hükme bağlamaktadır. Buna göre, ulusal hukuk yeterli güvenceyi sağlamadıkça, etnik köken, siyasi düşünce, dini inanç veya başkaca kanaatler ve sağlık veya cinsel yaşamı ortaya çıkaran kişisel verilerin işlenmesi yasaklanmıştır. Bu hassas veriler gibi, ceza mahkumiyetlerine dair kişisel bilgiler de korunmuş ve bu kuralın bu tür mahkumiyetler için de geçerli olacağı kabul edilmiştir.⁵⁰¹

Etnik kökeni, politik düşünce, dini veya felsefi inanç, sağlık veya cinsel durumunu açığa çıkaran veriler niteliğindeki hassas verilerin işlenmesine yasak getiren genel Avrupa yaklaşımının, bazı ulusal düzenlemeler düzeyinde de benimsendiği görülebilir. Örneğin Belçika,⁵⁰² Fransa,⁵⁰³ İspanya⁵⁰⁴ ve Portekiz⁵⁰⁵ hukukunun özel

⁴⁹⁸ 95/46 no'lu Yönerge'nin 7/f maddesi.

⁴⁹⁹ Bu konu kamusal makamların kişisel veri toplamalarından öte, özellikle özel kuruluşların veri toplamaları ve onlara kişisel verilerin ifşa edilmesinde önem kazanabilir. Özellikle ticari hayatın gerekleri içinde böyle bir gerekliliğin olup olmadığına ilişkin dengeyi sağlayacak olan devletlerin kendisi olacaktır. Eğer bu dengelemeye veri sahibi/ilgili itiraz ederse, ilgili ulusal veri koruma makamına ve daha sonra da gerekli olursa yargısal makama başvurulabilecektir, Perez Asinari, **a.g.m.**, s. 241

⁵⁰⁰ 95/46 no'lu Yönerge'nin 8/1 maddesi. Avrupa Birliği hukukunda hassas verilerle ilgili ayrıntılı bilgi için bkz.: (Cammilleri-Subrenat, Levallois-Barth, 2007)

⁵⁰¹ 108 No'lu Sözleşme'nin 6. maddesi.

⁵⁰² Consolidated Text of the Belgian Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the Law of 11 December 1998 implementing Directive 95/46/EC and the Law of 26 February 2003, English translation, madde 6, (Çevrimiçi) https://www.law.kuleuven.be/icri/publications/499Consolidated_Belgian_Privacylaw_v200310.pdf, 21 Aralık 2011.

yaşamın gizliliğinin korunması ve kişisel verilerin işlenmesine dair kanunlarında da etnik köken, dini inanç, sendika üyeliği ve siyasi düşünce niteliği taşıyan verilerin hassas veriler olarak kabul edildiği ve bu verilerin işlenmesinin kural olarak yasaklandığı görülmektedir. Almanya’da ise soyut bir kategorilendirme yerine, belirli veri işlenmesi usulünün verinin hassasiyetini belirleyeceği kabul edilmektedir. Bu yaklaşıma göre örneğin, bir kişinin ismi veya adresi, eğer bir akıl hastanesinin sakinlerinin belirtildiği bir listeye beraber sunuluyorsa, bu da hassas veri olarak değerlendirilebilir.⁵⁰⁶

OECD’nin konuya ilişkin benimsediği ilkeler açısından ise, özel nitelikteki hassas verileri dikkate alarak ayrı bir koruma öngörülmediği söylenebilir. Ama bu tabii ki, genel itibarıyla verilerin elde edilmesi ve bu verilerin işlenmesine dair bir koruma öngörülmediği anlamına gelmemektedir. Zira OECD, devletlere kişisel veriler toplanırken uymaları gereken belli prensipleri işaret ederek tavsiyede bulunmuştur. Buna göre, kişisel veriler toplanırken belli sınırlar konulmalıdır ve bu devletlerin kendi uygulamalarına bırakılmıştır.⁵⁰⁷ Fakat bununla birlikte, AB yönergelerinde de benimsenen, verilerin adil ve hukuka uygun elde edilmesi ve işlenmesi, ilgilinin

⁵⁰³ Act no 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (Amended by the Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data), Annotated text, madde 8, s. 8-10.

⁵⁰⁴ Organic Law 15/1999 of 13 December on the Protection of Personal Data, Unofficial translation that has been updated according to the changes operated in the Act after the Sentence 292/200 of the Spanish Constitutional Court, madde 7, (Çevrimiçi) http://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/SPAIN_Organiclaw_15_9_9.pdf, 21 Aralık 2011.

⁵⁰⁵ Act on the Protection of Personal Data (transposing into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), madde 7/1, (Çevrimiçi) <http://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM>, 21 Aralık 2011.

⁵⁰⁶ Spiros Smitis, “Sensitive Daten”-Zur Geschichte und Wirkung einer Fiktion, in Festschrift für Mario M. Pedrazzini 469, 1990, aktaran Simitis, **From the Market to the Polis: The EU Directive on the Protection of Personal Data**, 35. dipnot, s. 450. Alman Veri Koruması Kanunu’nun 28. maddesinin ikinci fıkrası da bu bağlamda birlikte değerlendirilebilir, Federal Data Protection Act, In the version published on 20 December 20, 1990 (BGBl.I 1990 S.2954), as amended by the law of 14 September, 1994 (BGBl. I S. 2325).

⁵⁰⁷ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data/OECD Özel Yaşamın Gizliliği ve Verilerin Korunmasına Dair Yönerge, madde 7, (Çevrimiçi) http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html#guidelines, 18 Aralık 2011.

rızasının alınması ve güncel olması gibi genel ilkeleri de korumuştur.⁵⁰⁸ Kaldı ki, kişisel verilerin zarara uğraması riski veya yetkisiz elde edilmesi, kullanılması, yayılması ve değiştirilmesine karşı makul güvenlik önlemlerinin alınması yoluyla korunması gerekliliği de kabul edilmiştir.⁵⁰⁹

95/46 no'lu Yönerge, hassas verilerin işlenmesinin kural olarak yasak olduğunu hükme bağlamakla birlikte, bu kuralın istisnalarını da ayrıca düzenlemiştir. Buna göre, ilgili kişinin veri işlemeye açıkça rıza göstermesi durumunda; ilgili ulusal hukukun yeterli koruyucu önlemleri sağlaması koşuluyla, iş hukuku alanında veri işleme sorumlusunun hak ve yükümlülüklerinin yerine getirilmesini sağlamak amacıyla gerekli ise; ilgili kişi fiziksel veya hukuksal nedenlerle rızasını verebilecek durumda değilse ilgili kişinin veya üçüncü bir kişinin yaşamsal çıkarlarını korumak için gerekli ise hassas veriler de işlenebilecektir.⁵¹⁰

Sayılan hallerden, açıkça rıza gösterilmesi koşulu ayrıca ele alınabilir. Zira daha önce de ifade edildiği üzere, aynı Yönerge'nin 7. maddesinde de ilgilinin belirsiz olmayan bir rızasından (**unambiguous consent**) bahsedilmiştir. Fakat görülüyor ki, hassas verilerin işlenmesi söz konusu olduğunda, bu AB düzenlemesinin yaklaşımı daha özel bir korumanın benimsenmesinden ve ancak açık rızanın (**explicit consent**) hassas verinin işlenmesi kuralına bir istisna oluşturacağından yanadır. Bunun dışında siyasi, felsefi, dini veya sendikal nitelikteki vakıf, dernek veya başkaca kar amacı gütmeyen kuruluşların kendi yasal faaliyetleri çerçevesinde olmak ve uygun garantiler sağlamak koşuluyla da hassas veriler işlenebilir. Fakat bu şekildeki veri işleme sadece, sayılan kuruluş veya organların üyeleri ya da amaçları dolayısıyla bu kuruluş veya organlarla düzenli bağlantı içinde olan kişilerle ilgili ise ve ilgili kişinin rızası olmadan üçüncü kişilere yayılmayacaksa söz konusu olabilecektir.⁵¹¹ Bu istisnanın rızaya dayanarak oluşturulan kamunun ulaşabileceği rehberler veya belirli

⁵⁰⁸ OECD Özel Yaşamın Gizliliği ve Verilerin Korunmasına Dair Yönerge'nin 7. ve 8. maddesi.

⁵⁰⁹ OECD Özel Yaşamın Gizliliği ve Verilerin Korunmasına Dair Yönerge'nin 11. maddesi.

⁵¹⁰ 95/46 no'lu Yönerge'nin 8/2 (a), (b) ve (c) maddesi. Bu istisnaların, daha önce ifade edilen ve hassas verilerin işlenememesini kural olarak yasaklayan Fransa, Belçika, İspanya ve Portekiz gibi devletlerin düzenlemelerinde de benzer şekillerde korunduğu söylenebilir.

⁵¹¹ 95/46 no'lu Yönerge'nin 8/2 (d) maddesi.

meslek grubundaki kişilere ilişkin bilgilerin toplandığı kayıtlar açısından uygulanabileceği düşünülebilir.⁵¹²

İlgili kişi açık bir şekilde kişisel veriyi kamuya açıklamışsa veya verinin işlenmesi hukuki talep oluşturmak, kullanmak veya bu talepleri savunmak için zorunlu ise de özel nitelikteki hassas veriler işlenebilecektir.⁵¹³ İlgilinin kendi rızasıyla hassas veriyi kamuya açıklaması, hassas verinin işlenemeyeceğine dair korumadan yararlanmasını engellese de, bu durumda da Yönerge'nin 6. ve 7. maddesinde düzenlendiği - ve yukarıda açıklandığı şekilde - veri işlemeye yönelik genel ilkelere uyulması zorunluluğunun ortadan kalkmadığı unutulmamalıdır.⁵¹⁴ Nitekim asıl amaç kişinin kendine ait bilginin ve bu bağlamda özel yaşamın gizliliği hakkının korunmasının sadece hassas verilerin işlenmemesi ile değil; işlenmesi sırasında gerekli prensiplere uyulması yoluyla da korunması olmalıdır. Suçlara, ceza mahkumiyetlerine ve güvenlik önlemlerine dair verilerin işlenmesi, resmi makamın kontrolü altında veya ulusal hukukun elverişli önlemleri sağlaması halinde yürütülebilir. Ceza mahkumiyetlerinin bütün halindeki kaydı ise ancak resmi makamın kontrolü altında tutulabilir.⁵¹⁵

D. Kişisel Verinin İşlenmesi Sırasında İlgilinin Bilgilendirilmesi

Kişisel verilerin adil bir şekilde işlenmesinin de bir gereği olarak, ilgili kişinin kişisel verinin işlenmesi faaliyetinin varlığına dair bilgilendirilmesi gerekir. Eğer kişisel veri kendisinden alınmışsa, bu veri toplamanın koşulları hakkında güncel ve eksiksiz olarak bilgilendirilmelidir.⁵¹⁶ Eğer kişisel veri doğrudan ilgili kişiden elde ediliyorsa,

⁵¹² Başalp, a.g.e., s. 45.

⁵¹³ 95/46 no'lu Yönerge'nin 8/2 (e) maddesi.

⁵¹⁴ Başalp, a.g.e., s. 45.

⁵¹⁵ 95/46 no'lu Yönerge'nin 8/5 maddesi. Bununla birlikte hassas verilerin işlenmemesi kural olmakla birlikte bu tür verilerin işlenmesi, sağlığın korunması, tıbbi teşhis, bakım veya tedavi tedariki ya da sağlık hizmetlerinin yönetimi için gerekli ise ve bu veriler ulusal hukukun veya meslek sırrı yükümlülüğü bakımından yetkili ulusal kuruluşlar tarafından oluşturulan kurallar dahilinde, profesyonel bir sağlık uzmanı tarafından veya benzer bir sır saklama yükümlülüğü altındaki başka bir kişi tarafından işleniyorsa, hassas verilerin işlenmemesi kuralına tabi olmayacaktır, 95/46 no'lu Yönerge'nin 8/3 maddesi.

⁵¹⁶ 95/46 no'lu Yönerge'nin 38 numaralı gerekçesi.

ilgili kiři, veri iřleme sorumlusu veya onun temsilcisi tarafından öncelikle veri iřleme sorumlusunun kimlięi ve veri iřlemenin amacı hakkında bilgilendirilmelidir. Bunun dıřında, kiřisel veriyi alanlar veya bunların kategorileri ile kendisiyle ilgili veriye ulařma ve bunu düzeltme hakkının varlıęı gibi konularda da bilgilendirilmesi öngörülmektedir.⁵¹⁷

Eęer kiřisel veri, doğrudan ilgili kiřiden elde edilmiyorsa, veri iřleme sorumlusu veya onun temsilcisi kiřisel veriyi toplarken veya üçüncü kiřilere açıklanacaksa bu açıklamadan önce, ilgili kiřiyi verinin toplandıęı veya iřlendięi hakkında bilgilendirmelidir.⁵¹⁸ Aslında bu husus internet ile ilgili olaylarla paralellik kurularak örneklendirilebilir. Veri iřleme sorumlusunun veya temsilcisinin ilgili kiřiye dair olan bu sorumluluęunun, internet aęısından, gizlilik hükümlerinin bildirilmesi ile saęlandıęı söylenebilir. Nitekim bu hükümlere dair bir baęlantı (**link**), ilgili kiřilerin bulunduęu internet sayfasında olmalıdır. Burada da, o sayfayı ziyaret eden kiřiden bir kiřisel bilgi elde edilecekse, bunun amacı, o kiřisel bilgiyi saęlamanın zorunlu olup olmadıęı gibi bilgilerin saęlanması beklenebilir.⁵¹⁹ Kiřisel veri doğrudan ilgili kiřiden elde edilmemiřse, kiřinin verinin toplandıęı veya iřlendięi hakkında bilgilendirilmesinin yanı sıra verinin doğrudan kendisinden elde edildięi durumda olduęu gibi, veri iřleme sorumlusunun veya temsilcisinin kimlięi, veri iřlemenin amacı ve bu veriye ulařma ve düzeltme hakkının varlıęı konusunda da bilgilendirilmesi gerekmektedir.⁵²⁰

Kiřisel verinin iřlenmesinde veri konusunu oluřturan ilgili kiřinin bilgilendirilmesi belli durumlarda söz konusu olmayabilecektir. Eęer ilgili kiřinin bilgilendirilmesi imkansızsa, ölçüsüz bir çabayı gerektiriyorsa veya kaydetme ya da bilgiyi açıklama yasada açık bir yükümlölük olarak düzenlenmiřse ilgili kiřiyi bilgilendirme yükümlölüęü uygulanmamaktadır. Bu durumda devletler de gerekli önlemleri almakla yükümlü kılınmıřlardır.⁵²¹

⁵¹⁷ Perez Asinari, **a.g.m.**, s. 238; 95/46 no'lu Yönerge'nin 10. maddesi.

⁵¹⁸ 95/46 no'lu Yönerge'nin 11/1 maddesi.

⁵¹⁹ Perez Asinari, **a.g.m.**, s. 238.

⁵²⁰ 95/46 no'lu Yönerge'nin 11/1 maddesi.

⁵²¹ 95/46 no'lu Yönerge'nin 11/2 maddesi.

E. Kişisel Verinin İşlenmesi Sırasında Veriye Ulaşma, Veriyi Düzeltme, Silme, Veriye Ulaşmayı Engelleme ve İtiraz Hakkının Korunması

İlgili kişinin veriye ulaşma hakkı, makul aralıklarla ve aşırı gecikme veya harcamalara maruz kalmadan belli bilgileri veri işleme sorumlusundan alması olarak ifade edilebilir. Bu bağlamda veri işleme sorumlusundan elde edilebilecekler, üç grupta toplanabilir: (i) İşlenen kişisel verinin kendisiyle ilgili olup olmadığı, işlemenin amacı, ilgili verinin kategorileri, veri alıcıları, verinin açıklandığı alıcıların kategorileri; (ii) işlenmekte olan veri ve bu verinin kaynağına ilişkin bilgilerin anlaşılabilir bir kalıpta kendisine ulaştırılması ve (iii) otomatik veri işlenmesinde - en azından bazı bireysel kararların otomatik olarak işlenmesi durumunda - bu işlemenin gerekçesi hakkında bilgi.⁵²² Kişinin veriye ulaşma hakkı sadece ulusal güvenlik, savunma, ceza yargılama usulleri ve kamu güvenliği ile devletin öncelikli ekonomik çıkarlarını korumak amacıyla sınırlanabilir.⁵²³

Bu doğrultuda veriye ulaşma hakkı, veri konusunu oluşturan ilgili kişi dolaylı olarak belirlenebilir durumda ise söz konusu olamayacaktır. Zira burada veri işleme sorumlusunun ilgiliyi bizzat belirlemesi durumu söz konusu değildir. Eğer ilgili kişi farklı kaynaklardan toplanan bilgilerle onun belirlendiği gibi bir şüphe taşıyorsa, bu durumda 95/46 no'lu Yönerge'nin bireysel kararların otomatik olarak işlenmesine dair 15. maddesi'ne özel bir önem verilmelidir.⁵²⁴ Buna göre böyle bir durumda, ilgili kişinin onun güvenilirliği, davranışları ve iş yerindeki performansı gibi şahsi yönlerini değerlendirmek amacıyla otomatik olarak veri işlenmesine dayalı olan ve kendisini hukuken veya başkaca önemli bir şekilde etkileyecek olan bir kararın konusu olmama hakkına sahip olduğu ayrıca göz önünde bulundurulmalıdır.⁵²⁵

⁵²² 95/46 no'lu Yönerge'nin 12/a maddesi. Bazı bireysel kararların otomatik olarak işlenmesi açısından, 95/46 no'lu Yönerge 15. maddeye göndermede bulunmaktadır. Buna göre, bir kişi kendisini hukuken veya başkaca önemli şekillerde etkileyecek olan ve onun güvenilirliği, davranışları ve iş yerindeki performansı gibi şahsi yönlerini değerlendirmek amacıyla otomatik olarak veri işlenmesine dayalı olan bir kararın konusu olmama hakkına sahiptir. 12/a maddesinde verinin otomatik olarak işlenmesi durumunda gerekçesi hakkında bilgi verilmesi gereken kararlar olarak da, bu bireysel kararlara gönderme yapılmaktadır.

⁵²³ Cate, *Privacy in the Information Age*, s. 38.

⁵²⁴ Perez Asinari, *a.g.m.*, s. 239.

⁵²⁵ 95/46 no'lu Yönerge'nin 15. maddesi.

İlgili kişinin veriye ulaşma hakkının bir uzantısı, başka bir deyişle uygulamadaki sonucu ise ilgili mevzuat - genel itibariyle 95/46 no'lu Yönerge - çerçevesinde işlenmemişse kişinin veriyi düzeltme, silme veya veriye sonradan ulaşılmasını engelleme hakkı olarak karşımıza çıkmaktadır.⁵²⁶ Böylece ilgili kişi hukukiliği, düzenliliği ve kendisine ait işlenen bilginin doğruluğunu denetleyebilme imkanına da sahip olur.⁵²⁷ Şu da unutulmamalıdır ki, yetkili kamusal makamların veri konusunu oluşturan ilgili kişiyi bilgilendirme yükümlülüğü, kişinin veriye ulaşma ve işlenmesi bakımından bilgi alma hakkından farklıdır. Fakat bunların ikisi birbirini tamamlar nitelikte düşünülebilir. Nitekim ilgili kişinin verinin tabi olduğu işleme faaliyetinden haberinin olmaması, bu konuda bilgilendirilmemesi, onun bilgi alma hakkını kullanmasını da imkansız kılıp, anlamsız hale getirebilecektir.⁵²⁸

İlgili kişinin kişisel verilerin işlenmesi durumunda, veriye ulaşma ve böylece bilgi alma hakkına Avrupa Konseyi'nin 108 no'lu Sözleşmesi'nde ve OECD'nin konuya ilişkin benimsediği ilkelerde de yer verildiği görülmektedir. Gerek Avrupa Konseyi gerek OECD açısından konuya ilişkin benzer prensiplerin kabul edildiği söylenebilir. Buna göre genel itibariyle, veri işlemenin amacı, veri işleme sorumlusunun kimliği ve işyeri adresi / çalıştığı kurumu hakkında bilgi almak ve makul aralıklarla ve aşırı gecikme ve masrafa tabi olmadan, kendisine ait verinin otomatik işleme tabi tutularak veri dosyasında tutulup tutulmadığını teyit etmek (**confirmation**) ve verilerin kendisine anlaşılabilir bir şekilde bildirilmesini sağlamak ilgili kişinin bilgi alma hakkı bağlamında değerlendirilmektedir.⁵²⁹

Bu belgelerde korunan ilgili kişi açısından koruma altına alınan tek hak, kişinin bilgi alma hakkı değildir. Bununla birlikte, 95/46 no'lu Yönerge'de açıkça düzenlendiği gibi, ilgili kişinin veriyi düzeltme, silme ve veriye ulaşılmasını engelleme hakkı da korunmuştur. Burada dikkat edilmesi gereken husus, bu hakkın, bilgi alma hakkının

⁵²⁶ Perez Asinari, **a.g.m.**, s. 239.

⁵²⁷ Rosario Imperiali D'Afflito, "European Union Directive on Personal Privacy Rights and Computerized Information," **Villanova Law Review**, C.XLI, Aralık 1996, s. 318.

⁵²⁸ Şimşek, **a.g.e.**, s. 90, 91.

⁵²⁹ 108 No'lu Sözleşme'nin 8. maddesi; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data/OECD Özel Yaşamın Gizliliği ve Verilerin Korunmasına Dair Yönerge, madde 13.

kullanılmasına bağlı olmayarak bağımsız ve fakat bilgi alma hakkıyla da ilişkili olmasıdır. Nitekim ilgili kişi yetkili kamusal makamlar tarafından bilgilendirilmemiş olsa da, kendisiyle ilgili eksik veya doğru olmayan veri olduğunu öğrenmişse, düzeltme, silme ve engelleme haklarını kullanabilmelidir.⁵³⁰ Kişisel verinin silinmesi durumunda, veri işleme sorumlusunun bu veri üzerinde işlem yapma yetkisinin ortadan kaldırılması amaçlanırken; engellemede bu şekilde yetkinin kullanılmasını tamamen sona erdirmeye yerine, veri işlemeye dair yetkinin kısmen veya tamamen durdurulması amaçlanmaktadır.⁵³¹

İlgili kişinin ayrıca, gerek Avrupa Konseyi'nin 108 no'lu Sözleşmesinde⁵³² gerek 95/46 no'lu Yönerge'de⁵³³ güvence altına alınmış olan itiraz hakkı bulunmaktadır. Buna göre, ilgili kişi zorlayıcı yasal nedenlerle kendisine ait verinin işlenmesine itiraz edebilir. Gerçi özellikle 95/46 no'lu Yönerge'den anlaşıldığı üzere zorunlu nedenlerden çok, aslında ilgili kişinin hakkının uygulanması yönünde tatmin edilmesi için dahi bu itiraz hakkı kullanılabilecektir.⁵³⁴ Buna göre, kişinin tutulan verinin kendisiyle ilgili olup olmadığına dair teyit talebi veya düzeltme ya da silme talebinin yerine getirilmemesi durumunda bu yoldan yararlanabileceği söylenebilir. İlgili kişinin itirazı haklı bulunursa, veri işleme sorumlusu bu veriyle ilgili bir veri işleme faaliyetinde bulunamayacaktır.⁵³⁵ Veri konusu ilgili kişilerin itiraz haklarının olduğu konusunda bilgilerinin olması konusunda da devletlerin, ulusal düzenlemeleriyle gerekli önlemleri almaları öngörülmüştür.⁵³⁶ Görülüyor ki, kamu yararına uygun olarak veya ilgili kişinin haklı çıkarları doğrultusunda ve yetki veren yasal düzenlemeler ışığında veri işleme mümkün olsa da, kişinin itiraz hakkının korunması anlayışı ağır basmaktadır.⁵³⁷

⁵³⁰ Perez Asinari, **a.g.m.**, s. 239.

⁵³¹ Şimşek, **a.g.e.**, s. 93, 94.

⁵³² 108 no'lu Sözleşmenin 8 (d) maddesi.

⁵³³ 95/46 no'lu Yönerge'nin 14 (a) maddesi.

⁵³⁴ Imperiali D'Aflitto, **a.g.m.**, s. 319.

⁵³⁵ 95/46 no'lu Yönerge'nin 14 (a) maddesi.

⁵³⁶ 95/46 no'lu Yönerge'nin 4/2 maddesi.

⁵³⁷ 95/46 no'lu Yönerge'nin 45 numaralı gerekçesi.

F. Veri İşlemenin Gizliliği ve Veri Güvenliği İlkesi

Kişisel veri işleme bağlamında ele alınan işlemlerin gizlilik ilkesi altında güvenceye alındığı söylenebilir. Veri işleme sorumlusunun veya veri işleyen kişinin denetimi altında çalışan ve kişisel veriye ulaşabilecek her kişi ve hatta veriyi işleyen kişi dahi, veri işleme sorumlusunun talimatlarına uygun olarak veriyi işlemelidir. Fakat bu durumda dahi ulusal hukuk böyle bir talimatın beklenmesini öngörmüyor veya buna ilişkin başka bir yükümlülük öngörüyorsa, ulusal hukuk düzenlemesi uygulanacaktır.⁵³⁸ Bu düzenleme özellikle, iç hukuk düzenlemesi şeklindeki kanunlar gereğince, bilgi verme yükümlülüğü olan kişilerin durumuna ilişkin uygulamaya yansiyabilir. Nitekim ulusal hukuk uyarınca, veri işleme sürecinde çalışabilecek bu kişiler bir ceza kovuşturması nedeniyle bilgi verme yükümlülüğüne sahipler ise, veri işlemeye dair bu gizlilik ilkesi onlar için uygulama alanı bulmayacak ve gereken bilgi verildiğine bu ilke ihlal edilmiş sayılmayabilecektir.⁵³⁹

Kişisel verilerin tesadüfen veya hukuka aykırı olarak ortadan kaldırılması, tesadüfen yok edilmesi, değiştirilmesi ve yetkisiz olarak açıklanması veya yetkisiz olarak veriye ulaşımın sağlanması durumlarına karşı veri işleme sorumlusunun uygun teknik ve organizasyonel önlemleri alması gerektiği ise, kişisel verilerin işlenmesinin güvenliği ilkesi olarak değerlendirilebilir.⁵⁴⁰ Bu güvenlik sadece ilgili kişinin hakkını korumakla kalmamakta; aynı zamanda veri işlemenin hukuka uygun olarak yapılması ve yetkisiz veri işlemenin önlenmesi koşullarının da gerçekleşmesi için gerekli bir ilke olarak görülebilir.⁵⁴¹ Nitekim uygulanacak en modern teknikler ve böyle bir uygulamanın masrafiyla ilgili olarak da, devlet, bu tür önlemlerin veri işleme faaliyetinden kaynaklanan risklere ve verinin türüne uygun bir güvenlik düzeyi de sağlamalıdır.⁵⁴² Aslında verinin niteliğine göre güvenlik önlemlerinin varlığı zaten olmazsa olmaz bir koşul gibi görülebilir. Zira kişisel veri örneğin özel nitelikteki

⁵³⁸ 95/46 no'lu Yönerge'nin 16. maddesi.

⁵³⁹ Başalp, a.g.e., s. 55.

⁵⁴⁰ 95/46 no'lu Yönerge'nin 17/1 maddesi. Veri güvenliği Avrupa Konseyi'nin 108 no'lu Sözleşmesi'nde (madde 7) ve OECD'nin Özel Yaşamın Gizliliği ve Verilerin Korunmasına Dair Yönergesi'nde de (madde 11) güvence altına alınmıştır.

⁵⁴¹ 95/46 no'lu Yönerge'nin 46 numaralı gerekçesi.

⁵⁴² 95/46 no'lu Yönerge'nin 46 numaralı gerekçesi.

hassas veri niteliğinde ise güvenlik önlemlerinin daha da artırılması düşünülebilir. Nitekim özellikle bilgisayar ortamında yapılacak faaliyetler ve verinin de bu ortamda kaydedilecek olması durumunda veri işleme sorumlusu, bu faaliyeti gerçekleştirecek çalışanlardan kaynaklanabilecek güvenliği tehdit edecek durumlara karşı gerekli önlemleri almalıdır.⁵⁴³

G. Veri İşleme Faaliyetinin Açıklığı

Veri işleme faaliyetlerine dair sicil tutma zorunluluğu 95/46 no'lu Yönerge bağlamında ilgili devletler için öngörülen yükümlülüklerden biri olarak düzenlenmiştir.⁵⁴⁴ Bu tür bir sicilin tutulması veri işleme faaliyetinin açık bir şekilde yürütülebilmesini de sağlayacaktır. Nitekim bu sicilde asgari olarak, veri işleme sorumlusunun ve varsa temsilcisinin adı ve adresi, veri işleme faaliyetinin amacı, ilgili kişilerin ve onlara ilişkin verilerin kategorisi, verilerin açıklanacağı alıcılar veya alıcıların kategorileri ve planlanan veri aktarımı hususlarına dair bilgilerin bulunması öngörülmüştür. İlgili kişinin bu bilgileri taşıyan sicile ulaşabilmesinin sağlanmasıyla aslında, kişisel verilerinin korunmasına dair haklarını kullanabilmesi için de imkan sağlanmış olmaktadır.

95/46 no'lu Yönerge'de her ne kadar, yetkili kuruma bildirilmesi gereken başka bir deyişle bildirim yükümlülüğüne tabi işlemler açısından, sicil tutulması ve bu sicillere herkesin ulaşabilmesi öngörülmüşse de;⁵⁴⁵ bu bildirim yükümlülüğüne tabi olmayan işlemler bakımından da, istenirse, ilgilinin bu verilere ulaşması için ilgili kurumlar gerekli önlemi almakla yükümlü kılınmışlardır.⁵⁴⁶ Böylece bildirim yükümlülüğü ayrımı gözetilmeksizin, sadece işleme tabi tutulan kişisel veriler değil, bunlara ilişkin sicillerin de ilgili kişilere açık tutulması güvence altına alınmıştır. Ayrıca böyle bir güvenceyle ilgili kişinin, kendisine dair verinin elde edilip edilmediğini, başkaca veri işleme faaliyetine maruz kalıp kalmadığını öğrenmesinin ve bunlar gerçekleşmişse,

⁵⁴³ Bainbridge, **a.g.e.**, s. 63.

⁵⁴⁴ 95/46 no'lu Yönerge'nin 21. maddesi.

⁵⁴⁵ 95/46 no'lu Yönerge'nin 18. maddesi.

⁵⁴⁶ 95/46 no'lu Yönerge'nin 21/3 maddesi.

silme, düzeltme veya engelleme gibi haklarını kullanabilmesinin uygulamada da açıklık ilkesi çerçevesinde gerçekleşmesi sağlanabilecektir.⁵⁴⁷

IV. KİŞİSEL VERİLERİN KORUNMASI BAĞLAMINDA ÖZEL YAŞAMIN GİZLİLİĞİNE DAİR AVRUPA BİRLİĞİ YAKLAŞIMININ A.B.D. YAKLAŞIMIYLA GENEL BİR KARŞILAŞTIRMASI

Genel itibariyle Avrupa Birliği mevzuatı, özel olarak da 95/46 no'lu Yönerge, zamanla artan şekilde kişisel verilerin korunmasına dair Avrupa yaklaşımının özel yaşamın gizliliği hakkına temel bir hak ve özgürlük olarak verdiği önemi yansıtır. Nitekim Avrupa veri koruması hukukunun en önemli uzmanlarından olan ve Avrupa Konseyi Veri Koruması Kurulu üyeliği de yapmış olan Spiros Simitis bu yaklaşımı ve neredeyse 95/46 no'lu Yönerge ile başlayan değişimi şöyle ifade ediyor: “Diğer birçok belgeden farklı olarak ve Topluluk bakımından da neredeyse ilk defa Komisyon, Yönerge taslağını hazırlarken, Topluluk bağlamında kişi haklarını koruma ihtiyacının Yönerge’yi de şekillendiren ihtiyaç olduğunu ifade etmiştir. Bu da, bizim neden Avrupa Birliği içinde kişisel veri korumasından bahsederken, aslında bireylerin temel hak ve özgürlüklerine saygı ihtiyacından söz ettiğimizi açıklar. Bu nedenle, kişiye dair bilgilerin korunması, farklı sorunlar karşısında farklı çözümler getirebilen bir konu olsa da, üzerinde pazarlık yapılabilecek bir husus değildir.”⁵⁴⁸

Neredeyse tüm demokratik toplumlarda iletişimin gizliliğinin, özgür bir toplumun temel unsurlarından biri olduğu düşünülse de, A.B.D. anlayışı, iletişimin gizliliğinin korunmasını hukuki düzenlemelerle güvence altına almaktan çok, konuyu daha çok piyasalara (**markets**)⁵⁴⁹ bırakmıştır. Avrupa’da ise iletişimin gizliliğinin ve bu

⁵⁴⁷ Cate, **Privacy in the Information Age**, s. 39; Şimşek, **a.g.e.**, s. 100, 101.

⁵⁴⁸ Simitis, **Unpublished Address, Information Privacy and the Public Interest**, Aktaran Cate, **Privacy in the Information Age**, s. 42.

⁵⁴⁹ A.B.D. yaklaşımındaki bu piyasa anlayışı, burada, özel yaşamın gizliliğinin ve kişisel verinin korunması söz konusu olduğunda ticari market anlamından farklı olarak da anlaşılabilir. Konuya

bağlamda özel yaşamın gizliliğinin korunması konusu, temel hak ve özgürlüklerle pekiştirilmiş bir siyasi zorunluluk olarak muamele görmektedir. Bu da Avrupa'nın genel itibariyle sosyal koruma anlayışı da dikkate alınarak, kamu özgürlüğünün toplumu oluşturan her bir bireyden kaynaklandığı ve hukuki düzenlemelerin de birey koruması bakımından temel teşkil ettiği kabulüyle bağlantılıdır. Bu anlayışta devlet belirleyici bir oyuncu olarak karşımıza çıkar ve ancak hukukun, aslında daha da özele inerek yasal düzenlemelerin, kapsamlı hak ve yükümlülükler getirerek koruyucu önlemleri sağlayacağı kabul edilir. Kaldı ki, A.B.D.'deki anlayıştan farklı olarak da, kişisel bilgilere sahip devlete, kişisel bilgilere sahip özel kişi ve kuruluşlara nazaran daha fazla güven duyulmaktadır.⁵⁵⁰

Hakikaten de gerek 95/46 no'lu gerek 2002/58 no'lu Yönerge özelinde - çoğunlukla kişisel verilerin korunmasına yoğunlaşmış olmalarına rağmen - özel yaşamın gizliliğinin bir temel hak ve özgürlük olarak öncelikli olarak korunması gerektiği ve bu hakkın aynı zamanda ifade özgürlüğüyle de bağlantılı olduğu anlayışının, hükümlere dahi yansıdığı görülebilir. Örneğin, özel kategorideki hassas verilerin işlenmesi bakımından devletlerin belirli istisnalar getirebileceği öngörülmüştür.⁵⁵¹ Yönergelerde belirli ilkelerin benimsenmiş olması, bunların tüm AB üyesi devletlerde aynı şekilde de benimsendiği anlamına gelmemektedir. Fakat genel anlayış itibariyle, bu devletlerde de benzer anlayışların hakim olduğu söylenebilir.⁵⁵² Buna göre aslında konuya ilişkin Avrupa yaklaşımı dört prensip bağlamında özetlenebilir: (i) kişisel bilgilerle ilgili olarak belirli yükümlülüklerin öngörülmesi, (ii) bu bilgilerin işlenmesinde saydamlığın sağlanması, (iii) hassas veriler için özel koruma yaratılması ve (iv) ihlale karşı yaptırımların uygulamaya konulmasını ve kişisel bilgiye yapılan muameleye karşı etkili bir gözetimi sağlamak.⁵⁵³

ilişkin farklı sorunlar karşısında veya farklı dönemlerde farklı çözümlerin öngörülebilmesi; tartışmaların ve farklı fikirlerin bu sorunları çözmedeki büyük rolünün önemsenmesi şeklinde de anlaşılabilir. Temel hak ve özgürlük söz konusu olduğunda, her fikrin serbestçe ortaya atılabileceği ve adil ortamda yarışabileceği ve o dönem en çok kabul gören ve o fikir yarışından kazanan olarak çıkan cevabın kabul edilmesi olarak da görülebilir.

⁵⁵⁰ Joel R. Reidenberg, "E-Commerce and Trans-Atlantic Privacy," *Houston Law Review*, C.XXXVIII, 2001-2002, s. 730-731.

⁵⁵¹ 95/46 no'lu Yönerge'nin 8. ve 2002/58 no'lu Yönerge'nin 15/1 maddesi.

⁵⁵² Cate, *Privacy in the Information Age*, s. 45.

⁵⁵³ Cate, *Privacy in the Information Age*, s. 45, 46.

İletişimin gizliliği ve kişisel verinin korunması bakımından Avrupa Birliği yaklaşımını değerlendirebilmek için, özellikle elektronik iletişime dair düzenlenmiş olan 2002/58 no'lu Yönerge ele alınabilir. Buna göre, kamusal iletişim ağı ve kamusal olarak ulaşılabilir elektronik iletişim hizmetleri üzerinden yapılan iletişimin ve ilgili trafik verinin gizliliğinin ulusal hukuk düzenlemeleriyle sağlanması başlıca yükümlülüklerden biridir. Bu genel çerçeveyi belirleyen yükümlülüğün yanı sıra, hukuka uygunluk nedeni⁵⁵⁴ olması hariç, ilgili kişinin rızası olmadıkça dinleme, telefon görüşmelerini kaydetme, depolama veya iletişimin başka türlü denetlenmesinin yasaklanması zorunluluğu da bulunmaktadır.⁵⁵⁵ Her ne kadar 2002/58 no'lu Yönerge elektronik iletişime ilişkin ilkeleri düzenlese de, 95/46 no'lu Yönerge'nin temel teşkil ettiği, konuya ilişkin esaslı düzenlemeler bakımından bu Yönerge'ye yapılan açık göndermeden de anlaşılabilir.⁵⁵⁶ 2002/58 no'lu Yönerge 95/46 no'lu Yönerge'nin hangi düzenlemelerinin bu Yönerge kapsamında da uygulanacağını belirtirken; ayrıca elektronik iletişim söz konusu olduğunda hangi hukuka uygunluk nedenlerinin varlığının, devlete, kişisel verilerin işlenmesinde geçerli olan belli kurallara - 95/46 no'lu Yönerge'de yer alan - sınırlamalar getirme yetkisi vereceğini de düzenlemiştir.⁵⁵⁷

Devletlerin devlet güvenliği, savunma, kamu güvenliği ve suç işlenmesinin önlenmesi gibi nedenlerle demokratik bir toplumda zorunlu, elverişli ve orantılı bir ölçüde, 95/46 no'lu Yönerge'de yer alan kişisel verilerin işlenmesinin hukuka uygun gerçekleştirilebilmesi için geçerli olan (veri kalitesi ve güncelliği gibi) ilkeler ve hassas verilerin işlenmesi konusunda öngörülen hak ve yükümlülüklerin kapsamını sınırlayabilecek ve elektronik iletişime müdahale niteliğinde olabilecek yasal önlemler benimseyebileceği öngörülmüştür. Bununla birlikte, hukuka uygunluk koşulları çerçevesinde, kişisel verinin belirli bir süre elde tutulabilmesi için de yasal düzenlemeler kabul edilebilir.⁵⁵⁸

⁵⁵⁴ Bu hukuka uygunluk nedenlerini 2002/58 no'lu Yönerge'nin 15. maddesinde düzenlenmiş olan ulusal güvenlik, savunma ve suç işlenmesinin önlenmesi gibi nedenler oluşturmaktadır.

⁵⁵⁵ 2002/58 no'lu Yönerge'nin 5. maddesi.

⁵⁵⁶ 2002/58 no'lu Yönerge'nin 15. maddesi.

⁵⁵⁷ Solove, Schwartz, **Privacy, Information, and Technology**, s. 1049.

⁵⁵⁸ Solove, Schwartz, **a.y.**

Özelde tüzükleri, yönergeleri ve Temel Haklar Şartı ile Avrupa Birliği, genel olarak da AİHS ve 108 no’lu Sözleşmeler gibi ilgili belgeler,⁵⁵⁹ aslında üst şemsiye olarak Avrupa yaklaşımı altında kişisel verilerin korunması hukukunun, aslında bir hak ve özgürlük olarak özel yaşamın gizliliği hakkını korumaya duyulan hassasiyetin bir yansıması olarak ortaya çıktığını göstermektedir.⁵⁶⁰ Bu noktada Avrupa ve A.B.D. anlayışı arasında açık bir farklılık olduğunun ve bu farklılığın da birebir pozitif düzenlemelerden öte, sosyal koşullar ve uygulama noktasında olduğu da ileri sürülebilir.

Kanımızca aslında farklılık belki de en iyi bu noktadan işaret edilebilir. Buna göre, Avrupa özel yaşamın gizliliği anlayışı, genel itibariyle, insan onuruna saygı üzerine şekillenirken; A.B.D. yaklaşımının ise kişisel serbestliği veya özgürlüğü koruduğu söylenebilir. Nitekim Amerikan Yüksek Mahkemesi’nin kararlarında özel yaşamın gizliliği, evi başkalarının bakışlarından uzak bir şekilde ilişkilerin geliştirilebileceği yer ve adeta özel yaşamın gizliliğinin mabedi olarak gören toplumsal kabulden yola çıkarak değerlendirilir ve kişinin makul bir özel yaşamın gizliliği beklentisi olup olmadığı sorusu üzerine temellenir. Buna karşılık Kıta Avrupası hukuklarındaki ve AİHM’deki özel yaşamın gizliliği kararlarının, daha çok insan onuru ve kişisel bağımsızlığı / özerkliği koruma ile ilgilendiği görülür.⁵⁶¹ Başka bir deyişle, ev korunmuş ve fakat bu değerleri korumak için ev dışındaki yerler ve kişisel konular da aynı şekilde koruma görmesi gereken yerler olarak kabul edilmiştir. Kıta Avrupası ve A.B.D. açısından bu ayrımı yapan bu anlayış aslında A.B.D.’nin toplumsal bir özellik olarak “ev”i korumaya değer en önemli şey olarak gören unsur üzerine temellenir. A.B.D.’liler için bir kişinin evindeki özel yaşamının gizliliği bağlamında devlete karşı özgür olmasının asıl mesele olduğu kabul edilir. Burada evi kutsal mekan ve evdeki özel yaşamın gizliliğini de asıl mesele olarak kabul etmek, A.B.D.

⁵⁵⁹ Jacques Velu, “The European Convention on Human Rights and the Right to Respect for Private Life, the Home and Communications”, **Privacy, and Human Rights, Reports and Communications Presented at the Third International Colloquy About the European Convention on Human Rights, Organised by the Belgian Universities and the Council of Europe, with the Support of the Belgian Government, Brussels, September-3 October 1970**, Ed. by. A. H. Robertson, London, Manshester University Press, 1973, s. 91.

⁵⁶⁰ Solove, Schwartz, **Privacy, Information, and Technology**, s. 999.

⁵⁶¹ Francesca Bignami, “European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,” **Boston College Law Review**, C.XLVIII, 2007, s. 681, 682.

anlayışının farklılaşan yönünü ortaya koymak için ifade edilmektedir. A.B.D. hukukunun özel yaşamın gizliliğini sadece “ev” içinde korumuş olduğu gibi bir sonuç çıkarılmamalıdır. Zira unutulmamalıdır ki, A.B.D. hukukunda özel yaşamın gizliliği ev dışında da korunmuştur.⁵⁶²

Bu durumun Kıta Avrupası’ndaki paralelinin ise insan onurunun korunması olduğu ileri sürülebilir. A.B.D.’nin evdeki özel yaşamın gizliliğini korumaya dair bu sosyal uygulaması ve hassasiyeti, Kıta Avrupa’ında kendini tarihsel koşulların da etkisiyle, ev dışında da korunacak olan saygı, şeref ve insan onuru olarak gösterir.⁵⁶³ İnsan onurunu korumaya duyulan bu hassasiyetin yüzyıllardır Kıta Avrupa’ında var olduğunu; bununla birlikte özellikle tarihsel gelişmeler doğrultusunda faşizme ve özellikle Nazi rejimine karşı tepkinin bu hassasiyeti artırdığı ileri sürülür. Bu bağlamda 1930 ve 1940’lı yıllardaki insan onurunu zedeleyici tecrübenin, Kıta Avrupası’nın bu hassasiyeti yansıttığı düzenlemeler açısından belirleyici olduğu da kabul edilir. Bu farklılığın yanı sıra, özel yaşamın gizliliği hakkı ve kişisel verilerin korunmasına dair ilkeler açısından A.B.D. ve Kıta Avrupası hukukunun hiç de benzerlik göstermediği düşünülmemelidir. Daha doğrusu şöyle ifade edilebilir ki, A.B.D. özel yaşamın gizliliği ve Kıta Avrupası’nın kişisel verilerin korunması anlayışları, geçmiş tecrübelerin ve sosyal farklılığın etkisiyle konuya yaklaşma tarzı ve koruma seviyeleri açısından farklılıklar gösterebilmektedir ve fakat ilkeler bazında benzerlikler mevcuttur.⁵⁶⁴

Nitekim A.B.D. Özel Yaşamın Gizliliği Kanunu (U.S. **Privacy Act**) ve AİHS konuya ilişkin, birbirinden çok da uzak bir anlatım yansıtmaz. Kaldı ki, A.B.D.⁵⁶⁵

⁵⁶² Griswold et al. v. Connecticut, No. 496, 381 U.S. 479. Kararla ilgili ayrıntılı bilgi için bkz.: Jeffery L. Johnson, “Constitutional Privacy,” **Law and Philosophy**, C.XIII, No:2, 1994, s. 171-181.

⁵⁶³ James Q. Whitman, “The Two Western Cultures of Privacy: Dignity versus Liberty,” **Yale Law Journal**, 113.6, Nisan 2004; Bignami, **a.g.m.**, s. 687, 688.

⁵⁶⁴ Bennett, **a.g.e.**, s. 150-153.

⁵⁶⁵ 5 USCS § 552a, Current through PL 112-73, approved 12/20/11, Title 5. Government Organization and Employees, Part I. The Agencies Generally, Chapter 5. Administrative Procedure, Subchapter II. Administrative Procedure.

Alman,⁵⁶⁶ İngiliz⁵⁶⁷ ve İsveç⁵⁶⁸ kişisel veri koruması mevzuatı karşılaştırıldığında, belirli ortak unsurlar göze çarpar. Bu düzenlemelerde gelişen bilgi teknolojisinin yabancılaştıran yönlerine karşı insan onurunu koruyan bir insancıl boyut; bilgi teknolojisini ve özelde de kişisel bilgiyi baskı aracı olarak kullanabilecek zorba devlet oluşumunu engellemeye yönelik siyasi boyut; eşitlik ve güncellik gibi özel yaşamın gizliliğini doğrudan ilgilendirmeyen değerleri geliştirmeye dair araçsal boyut ortak hususlar olarak görülebilir.⁵⁶⁹

Böyle bakıldığında asıl farklılığın düzenleme yöntemlerinde olduğu da ileri sürülebilir. Nitekim Almanya ve İngiltere’de daha görüşmeci ve pazarlıklar sonucuna dair (**negotiated**) yöntemle, İsveç’te daha bürokratik yollarla ve A.B.D.’de daha fazla yargıç hukuku yoluyla özel yaşamın gizliliğine ilişkin amaçların geliştirilmeye çalışıldığı değerlendirilmektedir. Bununla birlikte, bunlardan A.B.D. Özel Yaşamın Gizliliği Kanunu, Kıta Avrupası’nın kişisel veri mevzuatının birçoğundan farklı olarak sadece kamusal makamların faaliyetlerini düzenler. Kıta Avrupası düzenlemelerinde ise, özel sektör kurum ve kuruluşlarının veri işleme faaliyetleri de düzenlenmiştir. Gerçi düzenlenen ilkelerin genel itibarıyla kamusal makamların veri işleme faaliyetlerine de genişletilebileceği öngörülmektedir ve diğer önemli farklılığın büyük ölçüde uygulamada (**enforcement**) olduğu dahi ileri sürülebilir.⁵⁷⁰

⁵⁶⁶ Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), In the version published on 20 December 20, 1990 (BGBl.I 1990 S.2954), as amended by the law of 14 September, 1994 (BGBl. I S. 2325), (Çevrimiçi) <http://www.iuscomp.org/gla/statutes/BDSG.htm>, 28 Aralık 2011.

⁵⁶⁷ Data Protection Act 1998, <http://www.legislation.gov.uk/ukpga/1998/29/contents>, 28 Aralık 2011

⁵⁶⁸ Personal Data Act (1998:204); issued 29 April 1998, (Çevrimiçi) <http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf>, 28 Aralık 2011.

⁵⁶⁹ Bignami, **a.g.m.**, s. 683.

⁵⁷⁰ Uygulama bakımından A.B.D.’lilerin daha çok mahkemelerde haklarının uygulanması yoluna başvurduğu; Avrupalıların ise çoğunlukla kamu makamlarıyla pazarlık veya uzlaşma halinde olduğu ifade edilir. Avrupa’da yetkili idari makamların sadece kuralı uygulayan değil aynı zamanda, uygulanacak politikayı ve kimi zaman kuralı da belirleyen makamlar olduğu ileri sürülür. Bu makamlar ayrıca kurallara uygun veri işlemesi yapıp yapılmadığını da denetleme yetkisine sahip olabilmektedirler. A.B.D.’de ise bu tür kamusal makamların (**privacy agency**) eksik olması eleştirilir, Bignami, **a.g.m.**, s. 684-686.

V. TÜRK HUKUKUNDA ÖZEL YAŞAMIN GİZLİLİĞİ HAKKININ KORUNMASI BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI

A. 1982 Anayasası ve Yürürlükteki İlgili Diğer Mevzuat Bakımından

1982 Anayasası, herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğunu güvence altına almaktadır.⁵⁷¹ Kişisel verilerin korunması hakkı 1982 Anayasası'nın özel hayatın gizliliğini hükme bağladığı 20. maddede, “kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de” kapsayacak şekilde düzenlenmiştir.⁵⁷² Aslında 2010 değişikliğiyle 1982 Anayasası'na eklenen kişisel verilerin korunması hakkına ilişkin bir düzenleme yapma anlayışında, AB'deki bu yöndeki genel eğilimin de etkili olduğu söylenebilir. AB'de de önce AB Anayasa Taslağı, sonra da AB Temel Haklar Şartı'yla aynı eğilimi göstermiştir. Nitekim AB Anayasa Taslağı'nın I-50. maddesinde,⁵⁷³ herkesin kendisiyle ilgili kişisel bilginin korunmasını isteme hakkına sahip olduğunu güvence altına aldığı görülmektedir.⁵⁷⁴

AB Temel Haklar Şartı'na gelindiğinde de, 8. maddeyle kişisel verinin korunması hakkının garanti altına alındığı ve AB Anayasa Taslağı'nın öngördüğü genel yaklaşımın korunduğu ve kaldı ki, kişisel verilerin korunmasına ilişkin kurallara uygunluğun bağımsız bir makam tarafından denetlendiğinin düzenlendiği

⁵⁷¹ 1982 Anayasası'nın 07/05/2010 tarihli 5982 sayılı Kanun'un 2. maddesiyle değişen 20/3. maddesi. 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun, Resmi Gazete No. 27580, Resmi Gazete tarihi: 13/05/2010.

⁵⁷² 1982 Anayasası m. 20/3.

⁵⁷³ AB Anayasa Taslağının kişisel veriye dair bu hükmü ayrıca, bir Avrupa yasasının Birlik hukuku kapsamına giren faaliyetler gerçekleştirilirken, Birlik Kurumları, organları ve daireleri ile üye devletler tarafından kişisel verinin işlenmesi halinde, bireylerin korunması ve bu tür verinin serbest dolaşımıyla ilgili kuralları belirleyeceği öngörülmüştür. Bu kurallara uyumluluk ise bağımsız bir makamın denetimine tabi olacaktır, Draft Treaty establishing a Constitution for Europe, Submitted to the President of the European Council in Rome, Conv 850/03, Brüksel, 18 Temmuz 2003.

⁵⁷⁴ AB Anayasa Taslağı'nın genel yaklaşımıyla ilgili ayrıntılı bilgi için bkz.: Oder, a.e.. Saadet Yüksel, “Avrupa Birliği'nin Anayasa Süreci,” Ergon A. Çetingil ve Rayegan Kender'e 50. Birlikte Çalışma Yılı Armağanı, İstanbul, 2007, s. 1256-1276.

görülebılır.⁵⁷⁵ Temel Haklar Şartı'nda ayrıca, hangi şartlar gerçekleştirilerek kişisel verinin elde edilebileceği ve kişilerin kendileriyle ilgili elde edilen bu bilgilere dair ne yapabileceği de düzenleme altına alınmıştır.⁵⁷⁶

Kişisel verilerin korunması Türk hukukunda sadece 1982 Anayasası'nda değil, Türk Ceza Kanunu (TCK)'nda da düzenleme altına alınmıştır. TCK, aslında kişisel verilerle ilişkili suçlara ve ayrıca kişisel verilerin korunmasına dair suçlara yer vermektedir.⁵⁷⁷ Buna göre, öncelikle özel hayata ve hayatın gizli alanına karşı suçların düzenlendiği ve bu bağlamda haberleşmenin gizliliğini ihlal (TCK m. 132), öngörülen şartlara⁵⁷⁸ uyulmadan kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (TCK m. 133) ve özel hayatın gizliliğini ihlal (TCK m. 134) suç olarak hükme bağlanmaktadır. Ayrıca, kişisel verilerin hukuka aykırı olarak kaydedilmesi (TCK m. 135), kişisel verileri hukuka aykırı olarak verme veya ele geçirme (TCK m. 136) ile kanunların belirlediği sürelerin geçmiş olmasına karşın kişisel verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmemeleri (TCK m. 138) suç olarak düzenlenmiştir. Kişisel verilerin korunmasına dair bu tür güvencelerin kişisel verilerin korunmasına dair kanun tasarısı ile güvencelerin hayata geçmesi bakımından daha da fazla anlam kazanacağı açıktır. Tasarının halen kanunlaşmamış olmasının, kişisel veriler ile ilgili olarak cezalandırılan bu fiillere yönelik bir belirsizlik yarattığı ve bu belirsizliğin halen devam ettiği göz ardı edilemez.⁵⁷⁹ Fakat şu da unutulmamalıdır ki, Tasarının halen kanunlaşmamış olması, TCK'nın yürürlükte olan bu hükümlerini dikkate alarak, söz konusu faaliyetleri

⁵⁷⁵ Avrupa Temel Haklar Şartı'nın 8. maddesinin 1. ve 3. fıkrası, Charter of Fundamental Rights of the European Union, C 364/10.

⁵⁷⁶ Avrupa Temel Haklar Şartı'nın 8. maddesinin 2. fıkrası, kişisel verinin adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulacağını; herkesin, kendisi hakkında elde edilmiş verilere erişme ve bunları düzelttirme hakkına sahip olduğunu öngörmektedir, Charter of Fundamental Rights of the European Union, C 364/10.

⁵⁷⁷ Fatih Selami Mahmutoğlu, "Ceza ve Ceza Yargılamada Hukukunda Özel Yaşam", **Özel Yaşamın Gizliliği Paneli**, 18 Ekim 2008, TTB Yayını 154, s. 104 vd.

⁵⁷⁸ "Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi; katıldığı aleni olmayan bir söyleyişi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi" ve bu "fiillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişinin" cezalandırılması öngörülmüştür, (TCK m. 133).

⁵⁷⁹ Elif Küzeci, **Kişisel Verilerin Korunması**, Ankara, Turhan, 2010, s. 295.

gerçekleştiren ilgili kişi ve kuruluşların bu düzenlemeleri göz önünde bulundurmaları ve buna göre gerekli önlemleri almaları gerektiğine dair gerçeği değiştirmemektedir. Kişisel verilerin korunmasının, kişilik hakkının korunmasına dair bir husus olduğu da açıktır. Zira hak sahibi olabilen ve borç altına girebilen bir varlık olan “kişi”nin, kişiliğini oluşturan değerler üzerindeki hakkı, kişilik hakkı olarak nitelendirilebilir.⁵⁸⁰ Bu değerleri ise, bir yandan kişi olmaya bağlı olarak tanınan hak ve fiil ehliyeti, ismi, hayatı, vücut tamlığı, şerefi, haysiyeti oluştururken; diğer yandan, serbest karar vererek, kişiliğini serbestçe geliştirebilmesi ile gizli ve özel hayat alanı oluşturmaktadır.⁵⁸¹ Yargıtay, kişisel değerlerin maddi ve manevi değerleri kapsadığını dile getirmekle birlikte; kişinin yaşam ve sağlığı gibi maddi değerler ile onur, saygınlık, özgürlükler ve özel yaşam gibi manevi değerlerin kişisel değerler olarak kabul edilmesi gerektiğini belirtmektedir.⁵⁸² Aslında kişinin, hukukun korumaya değer bulduğu bu değerlerin varlığı itibariyle hukuk alanında yer bulduğu da ifade edilebilir.⁵⁸³

Kişilik hakkını oluşturan değerlerin birden fazla olması nedeniyle, doktrinde birden fazla mı veya tek bir kişilik hakkı mı olduğu tartışması yapılmakta; Türk hukukunda genel eğilim ise, tek bir genel kişilik hakkı olduğunu yansıtmaktadır.⁵⁸⁴ Buna göre, hakkı oluşturan bu değerler, tek bir genel kişilik hakkının çeşitli görünümüleri olarak ortaya çıkmaktadır. Nitekim kişilik hakkına dair sınırlayıcı olarak, bu hakkı oluşturan kişisel değerlerin sayıldığı bir tanımlama yapılmadığı ve bunların neler olduklarına dair belirlemenin hakime bırakıldığı kabul edilmektedir.⁵⁸⁵ Yargıtay da kişilik değerlerinin nelerden ibaret olduğuna dair sınırın çizilmediğini dile getirdiği

⁵⁸⁰ Abdülkadir Arpacı, **Kişiler Hukuku (Gerçek Kişiler)**, İstanbul, Beta, 2. bs., 2000, s. 103; Serap Helvacı, **Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar** (MK md. 24/a I/İMK md. 28a fıkra I), İstanbul, Beta, 2001, s. 41.

⁵⁸¹ Mahmutoglu, “Ceza ve Ceza Yargılama Hukukunda Özel Yaşam”, s. 100-103; M. Kemal Oğuzman, Özer Seliçi, **Kişiler Hukuku (Gerçek ve Tüzel Kişiler)**, İstanbul, Filiz, 2011, s. 2; Doruk Gönen, **Tüzel Kişilerde Kişilik Hakkı ve Korunması**, İstanbul, XII Levha, 2011, s. 19; Mustafa Dural, Tufan Ögüz, **Türk Özel Hukuku, Cilt II, Kişiler Hukuku**, İstanbul, Filiz, 2011, s. 8, 9; Bilge Öztan, **Şahsın Hukuku, Hakiki Şahıslar**, 7. bs, Ankara, Turhan, 1997, s. 111, 112; Hüseyin Hatemi, **Gerçek Kişiler Hukuku (Kısa Ders Kitabı)**, İstanbul, Vedat, 2005, s. 59.

⁵⁸² Yargıtay Hukuk Genel Kurulu, E. 2010/751, K. 2011/96, K.t. 13/04/2011.

⁵⁸³ Dural, Ögüz, **a.g.e.**, s. 8.

⁵⁸⁴ Helvacı, **a.g.e.**, s. 42, 43; Gönen, **a.g.e.**, s. 21; Hatemi, **a.g.e.**, s. 59; Oğuzman, Seliçi, Oktay-Özdemir, **a.g.e.**, s. 144.

⁵⁸⁵ **A.e.**

kararında; fiziki, duygusal ve sosyal kişilik değerleri bu tür değerlerden bazıları olarak nitelendirmiştir.⁵⁸⁶

Kişilik hakkının niteliklerinden ilki, para ile değerlendirilememeleri ve maddi değere sahip olmamaları olarak ifade edilebilir. Ancak bu özellik, kişilik hakkına saldırının maddi veya manevi zarara neden olmasını engellemez.⁵⁸⁷ Bunun dışında, kişilik hakkı, bu hakka saldıran herkese karşı ileri sürebilme imkanı veren; mutlak bir hak olarak görülmelidir.⁵⁸⁸ Bu yönüyle, bu hakkın korunması, özel yaşamın gizliliğinin koruduğu alana yapılabilecek müdahaleleri kural olarak yasaklar. Kişilik hakkı, kişinin kişiliğinden ayrılmaz, ona sıkı sıkıya bağlı haklardandır.⁵⁸⁹

Gerek kişilik hakkının genel özellikleri, gerek bu hakkı oluşturan kişisel değerler göz önünde bulundurulduğunda; kişisel verinin kişilik hakkına dahil olduğu açıkça görülür.⁵⁹⁰ Kaldı ki, kişisel verilerle ilişkili olan kişisel varlıklar sadece kişinin ismi, vücut tamlığı, şeref ve haysiyeti değil; aynı zamanda yaşam alanıdır. Bu bağlamda, kişinin yaşam alanlarına dair doktrinde yapılan üçlü ayrım hatırlatılmalıdır: (i) Toplum içinde meydana gelen veya kişinin kendisinin paylaştığı, herkesçe bilinen olayların oluşturduğu ortak yaşam alanı, kamuya açık alan olarak kabul edilmektedir.

⁵⁸⁶ Yargıtay vatandaşlık bağı ile bağlı bulunulan Türk Milletine yönelik sözleriyle ilgili olarak aktif dava ehliyetine ilişkin bir kişiye dair kararında, kişilik hakkına saldırı ve sosyal kişilik değeri hususlarına değinmektedir. Buna göre, “hukukumuzda kişilik haklarını tanıma yapılmamış ve bu hakkın hangi değerleri kapsadığı da açıklanmamıştır. Böyle kişilik haklarının diğer bir anlatımla kişilik haklarının nelerden ibaret olduğunun belirlenmesi ve sınırının çizilmesi uygulamaya bir başka ifadeyle yargıya bırakılmıştır. Gerek öğretide gerekse yargısal kararlarda kişisel değerlerin; fiziki, duygusal ve sosyal kişilik değerleri olarak belirlendiği, kişinin toplum içindeki mesleki kimliği şeref ve haysiyeti, özgürlüğü vücut ve ruh bütünlüğü ve sağlığı, ırk din ve vatandaşlık gibi bağları kapsadığı kabul edilmektedir. (...) Kişilerin onur ve şerefleri gibi mensubu bulundukları ve Anayasa ile çerçevesi belirlenmiş bir millete aidiyeti duygularında yukarıdaki açıklamalar nazara alındığında; kişilik değerleri kapsamında ve hukuki koruma altındadırlar.” şeklinde bir açıklama yapıldığı görülmektedir, Yargıtay 4. Hukuk Dairesi, E. 2006/12581, K. 2007/15816, K.t. 11712/2007. Yargıtay bir başka kararında da, evli bir kimsenin evlilik dışı birlikteliğini, diğer eşin sosyal kişilik değerlerine saldırı niteliğinde değerlendirmiştir, Yargıtay Hukuk Genel Kurulu, E. 2010/129, K. 2010/173, K.t. 24/03/2010.

⁵⁸⁷ Helvacı, **a.g.e.**, s. 46, 47; Oğuzman, Seliçi, Oktay-Özdemir, **a.g.e.**, s. 144; Arpacı, **a.g.e.**, s. 106; Dural, Ögüz, **a.g.e.**, s. 97.

⁵⁸⁸ Helvacı, **a.g.e.**, s. 46; Oğuzman, Seliçi, Oktay-Özdemir, **a.g.e.**, s. 144; Arpacı, **a.g.e.**, s. 106; Dural, Ögüz, **a.g.e.**, s. 97.

⁵⁸⁹ Kişilik hakkının, bu şekilde vazgeçilmesi, devredilmesi mümkün olmayan yönünün, bu hakka saldırı sonucu elde edilen örneğin tazminat gibi alacakların da devredilememesi anlamına gelmediği kabul edilmektedir, Oğuzman, Seliçi, Oktay-Özdemir, **a.g.e.**, s. 142.

⁵⁹⁰ Küzeci, **a.g.e.**, s. 275, 276.

(ii) Kişinin yakın çevresi ve ailesi gibi sınırlı kişilerce bilinmesini istediği ve bunun dışındakilerden, kamudan, gizli tuttuğu olayların oluşturduğu alan, özel yaşam alanı olarak nitelendirilmektedir. (iii) Kişinin sadece açıkladığı kişilerce bilinmesini istediği, bunun dışındaki kişilerden gizli tuttuğu olayların meydana getirdiği - aile, ev yaşamı gibi - yaşam alanı da gizlilik alanını oluşturmaktadır.⁵⁹¹

Kural olarak, kişinin özel (**private**) ve gizli (**intimate**)⁵⁹² yaşam alanına yapılan müdahalelerin kişilik hakkını ihlal olarak değerlendirilebileceği söylenebilir. Bu alanlarda kişiye ait veya onu belirlenebilir kılan bilginin kişisel verinin elde edilmesi, kaydedilmesi, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi ya da üçüncü kişilere aktarılması işlemlerinin bu tür ihlalleri oluşturabileceği açıktır. Özel ve gizli alanın kimi zaman belirli kişilere açık olması;⁵⁹³ kişinin rızası gibi hukuka uygunluk şartlarının bulunması gibi durumlar dışında özel veya gizli alana yapılacak hukuka aykırı müdahalenin - örneğin iletişimin gizlice denetlenmesi ve kişisel verinin, başkalarına dağıtılmasa da sadece elde edilmesi - kural olarak kişilik hakkının ihlali niteliğinde kabul edilmesini engellemeyecektir.⁵⁹⁴ Kişilik hakkının ihlali iddiası karşısında, söz konusu kişisel verinin, hukuk düzeni tarafından korunan, bir başka deyişle kişilik hakkını oluşturan bir kişilik değeri olup olmadığı araştırılacaktır. Aslında böyle bir araştırmada sadece Türk Medeni Kanunu (TMK) veya başkaca özel hukuk hükümleri değil; anayasal hükümler⁵⁹⁵ gibi başkaca düzenlemelerin de göz önünde bulundurulması gerekeceği söylenebilir.⁵⁹⁶

⁵⁹¹ Oğuzman, Seliçi, Oktay-Özdemir, **a.g.e.**, s. 157-162; Dural, Ögüz, **a.g.e.**, s. 127, 128; Küzeci, **a.g.e.**, s. 276; Helvacı, **a.g.e.**, s. 62.

⁵⁹² Gizli yaşam alanının sır alan olarak ifade edildiği de görülür. Bkz.: Küzeci, **a.g.e.**, s. 277.

⁵⁹³ Kanımızca bu duruma, bir restraaurantın bir köşesine çekilerek birisiyle gizlice konuşmak veya bir telefon kulübesinde kapıyı kapatarak telefonla konuşmak örnek gösterilebilir. Bu durumda da orada bir özel yaşam veya gizli yaşam alanı oluşturulduğu söylenebilir. Nitekim bu kişilik hakkına müdahalede açısından da, özel yaşamın gizliliği hakkında açıkladığımız, yalnız başına kalabilme (right to be let alone) hakkının ihlali hukuka aykırı olarak müdahale olarak nitelendirilebilmektedir, Dural, Ögüz, **a.g.e.**, s. 129.

⁵⁹⁴ Oğuzman, Seliçi, Oktay-Özdemir, **a.g.e.**, s. 157-162; Dural, Ögüz, **a.g.e.**, s. 129, 130; Helvacı, **a.g.e.**, s. 62-67.

⁵⁹⁵ 1982 Anayasası'nın herkesin kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahip olduğunu düzenleyen 12. maddesi ve temel hak ve özgürlüklere dair hükümler bu bağlamda düşünülebilir.

⁵⁹⁶ Dural, Ögüz, **a.g.e.**, s. 95.

TMK'nın özel ve gizli yaşam alanını ve böylece kişisel verileri, kural olarak, koruduğu söylenebilir. TMK'nın 24. maddesi, hukuka aykırı olarak kişilik hakkına saldırılan bir kişinin, hakimden, saldırıda bulunanlara karşı korunmasını isteyebileceğini hükme bağlamaktadır.⁵⁹⁷ Bunun yanı sıra, “hakimden saldırı tehlikesinin önlenmesi, sürmekte olan saldırıya son verilmesi, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespiti” istenebilecektir.⁵⁹⁸ Bunlarla birlikte, kişinin düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması, maddi ve manevi tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekaletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakları da bulunmaktadır.⁵⁹⁹

Kişisel verilere dair TMK'nın belirli bir koruma getirdiği söylenebilir. Fakat asıl kapsamlı koruma, TMK'daki konuya ilişkin hükümleri de tamamlayacak olan ayrı, özel bir kişisel verilerin korunması kanunun kabul edilmesiyle olacaktır.⁶⁰⁰ Mevcut hukuk düzenimiz bakımından daha doğru bir ifadeyle, halen tasarı halinde olan kişisel verilerin korunması kanununa dair metnin kanunlaşmasıyla bu bütünlüğün sağlanacağı ve mevzuat bağlamında yapılacak yerinde uygulamalarla da birçok belirsizliğin usulüne uygun olarak kalkacağı beklenebilir.

B. Kişisel Verilerin Korunması Kanunu Tasarısı

Önleme amaçlı denetim uygulanırken kişisel verilerin korunmasının pratik önemi, çok yakın bir zamanda hukuki düzenlemeye kavuşturulması bakımından, artık Türk hukukunda da büyük bir dikkatle göz önünde bulundurulmalıdır. Zira 2010 yılında,

⁵⁹⁷ 22/11/2001 tarihli, 4721 sayılı Türk Medeni Kanunu, Resmi Gazete No. 24607, Resmi Gazete tarihi: 08/12/2001. TMK, 23. maddesinde de kişiliğin korunmasından vazgeçme ve aşırı sınırlamaya karşı şunu düzenlemiştir: “Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez. Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlâka aykırı olarak sınırlayamaz. (...)”.

⁵⁹⁸ TMK m. 25/1.

⁵⁹⁹ TMK m. 25/2, 3.

⁶⁰⁰ Bu husus, İsviçre’de de medeni kanunun kişisel verilerin korunmasına dair güvencelere yer vermesine rağmen, ayrı bir kişisel verilerin korunması kanununun kabul edilmesi açısından da geçerli olabilecek nedenlerden biri olarak ifade edilmektedir, Küzeci, **a.g.e.**, s. 277. İsviçre’de yürürlükte olan Kişisel Verilerin Korunması Kanunu için bkz.: Swiss Federal Act on Data Protection of 19th June 1992 (Status as per 3rd October 2000), (Çevrimiçi) <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.CH>, 27 Ocak 2011.

1982 Anayasası'nın 20. maddesinde yapılan değişiklikle kişisel verilerin korunmasını isteme hakkı anayasal güvenceye kavuşturulmuştur.⁶⁰¹ Unutulmamalıdır ki, genel olarak bu korumanın ve özelde de kişisel verilerin korunmasına ilişkin ilkelerin iletişimin denetlenmesini gerçekleştirecek kamu görevlileri tarafından uygulamaya geçirilmesi, halen TBMM Komisyonu'nda olan "Kişisel Verilerin Korunması Kanunu Tasarısı"⁶⁰²'nin kanunlaşması ve her şeyden önemlisi gereği gibi uygulanması ile sağlanacaktır. Kişisel Verilerin Korunması Kanunu Tasarısı, hukukumuzda kişisel verilerin işlenmesi ve bu işlemenin özel yaşamın gizliliğini ilgilendiren boyutu bağlamında değerlendirilmelidir. Tasarı'nın değerlendirilmesi, sadece metnin içerdiği düzenlemelerin belirtilmesi değil, aynı zamanda Türk hukuku yaklaşımının yansıtılması ve daha da önemlisi AB mevzuatının, Tasarının genel yaklaşımı ve hatta benimsediği ilkeler açısından ne kadar belirleyici olduğunun anlaşılabilmesi açısından önem taşır. O kadar ki, yukarıda incelenen kavramlar ve özellikle 95/46 no'lu Yönerge çerçevesinde incelenen ilkelerin büyük bir kısmı neredeyse tekrar oluşturacak şekilde burada yeniden vurgulanacaktır.

Öncelikle belirtilmelidir ki, CMK'nın 135. vd. maddeleri bağlamında, bir başka deyişle önleme amaçlı değil adli denetim sonucu elde edilen veriler açısından, kişisel verilerin hukuka aykırı olarak kaydedilmesi, üçüncü kişilere verilmesi ve yayılması fiillerinin yaptırım altına alınmış olduğu vurgulanmıştır. Fakat bununla birlikte, TMK'da korunan kişilik hakkı ve AİHS'nin 8. maddesiyle korunan özel yaşamın gizliliği hakkının da korunması gerektiği gözetilmiştir.⁶⁰³ Nitekim kişisel verilerin korunmasının, kişilik hakkının korunmasına da dair bir husus olduğu açıktır.

Kişisel verinin korunmasının gerek kişilik hakkı ve özel yaşamın gizliliği hakkının korunması ile ilişkisi gerek 1982 Anayasası'nda korunan kişisel verilerin korunması hakkının uygulanması göz önünde bulundurulduğunda, kişisel verilerin korunmasına ilişkin temel ilkeleri - iletişimin adli ve önleme amaçlı denetimi bakımından bir

⁶⁰¹ 1982 Anayasası'nın 20. maddesinin 3. fıkrası, (Çevrimiçi) http://heinonline.org.ezp-prod1.hul.harvard.edu/HeinDocs/cowdocs/tr_1982_2010_turk.pdf, 26 Kasım 2010.

⁶⁰² Kişisel Verilerin Korunması Kanun Tasarısı, T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, Sayı: 1812, 22 Nisan 2008, (Çevrimiçi) <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf>, 3 Ocak 2011.

⁶⁰³ Kişisel Verilerin Korunması Kanun Tasarısının genel gerekçesi.

ayırma gitmese de - düzenleyen Tasarı'nın önemi dikkat çeker. Nitekim Tasarı'da çeşitli kurum ve kuruluşları dikkate alarak sektörel bazda bir düzenleme yöntemi benimsenmemiştir. Burada belirlenen esasların temel ilkeler niteliğinde dikkate alınarak, ilgili kurum ve kuruluşlarca düzenlemelerin yapılması öngörülmüştür.⁶⁰⁴

Tasarı'da göz önünde bulundurulan temel ilkelerin genel itibariyle, OECD'nin veri korunmasına ilişkin benimsediği ilkelerle de uyum gösterdiği görülebilir. Nitekim Tasarı'nın gerekçesinde de OECD'nin benimsediği ilkelerle Tasarı'nın düzenlediği ilkelerin birbirini tamamlayıcı nitelikte olduğu vurgulanmış ve bunların nelerden ibaret olduğu açıkça ifade edilmiştir. Buna göre, kişisel verilerin toplanması ve işlenmesinin sınırlı olması ve ilkelere bağlılık, kişisel veride kalite ilkesi, kişisel veri toplama ve işlenmesinde amacın belirginliği ilkesi, amaca uygun kullanım ilkesi, kişisel verilerin korunması için gereken tedbirlerin alınması ilkesi, açıklık ilkesi, ilgili kişinin bireysel katılımı ilkesi ve sorumlu tutulabilirlik ilkesi OECD'nin benimsediği ve Tasarı'ya yansıyan esaslı ilkeler olarak ortaya çıkmaktadır.⁶⁰⁵

Temel ilkeler itibariyle dikkate alınan bir diğer belgenin 108 no'lu Avrupa Konseyi Sözleşmesi olduğu söylenebilir. Tasarı, Türkiye tarafından da imzalanan ve fakat henüz onaylanmamış olan Sözleşme'nin onay süreci bakımından gerekli ulusal yükümlülüğü yerine getirme bağlamında da ele alınmıştır.⁶⁰⁶ Böylece Tasarı'nın kanunlaşmasıyla gerekli ulusal düzenleme gerekliliğinin yerine getirilmiş olacağı vurgulanmıştır. Bununla birlikte AB'ye üyelik sürecinde olan bir devlet olarak, Türk mevzuatıyla Birlik mevzuatı arasında uyum sağlanması ve ileride üye olduğunda doğabilecek sorunların önlenmesi açısından 95/46 no'lu Yönerge'nin de göz önünde bulundurulduğu belirtilmiştir.⁶⁰⁷ Nitekim paralellikler, Tasarı'nın içeriği incelenirken de açıkça göze çarpacaktır.

⁶⁰⁴ A.e.

⁶⁰⁵ Kişisel Verilerin Korunması Kanun Tasarısının genel gerekçesi.

⁶⁰⁶ 108 no'lu Sözleşme'nin 4. maddesine göre, Sözleşme tarafı devletler verilerin korunmasına yönelik temel ilkelere işlerlik kazandırmak için kendi iç hukuklarında gerekli önlemleri almakla yükümlü kılınmışlardır, Council of Europe - ETS no. 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981, (Çevrimiçi) <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>, 1 Ocak 2011.

⁶⁰⁷ Kişisel Verilerin Korunması Kanunu Tasarısının genel gerekçesi.

Geleneksel dosyalama şeklinde veya otomatik olarak kişisel verileri işleme tabi tutulan kişilerin yanı sıra bu yollarla verileri işleyen kamu kurum veya kuruluşları ile gerçek ve özel hukuk tüzel kişileri de Tasarı'nın düzenleme alanında bulunmaktadır.⁶⁰⁸ Böylece, 95/46 no'lu Yönerge'nin gerçek kişileri, 2002/58 no'lu Yönerge'nin de tüzel kişileri koruma kapsamına aldığı gerekçe gösterilerek;⁶⁰⁹ kişisel verilerin korunması ile ilgili düzenlemeler bakımından tüzel kişilerin de koruma kapsamına alınabileceği vurgulanmış olmaktadır.

Hangi verinin kişisel veri olarak kabul edileceği noktasında da Tasarı, AB Yönergeleriyle gösterdiği paralelliği bozmamakta ve kişisel veriyi “belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler”⁶¹⁰ olarak kabul etmektedir. Bu bağlamda kişiyi belirlenebilir kılabilecek bilgi açısından da 95/46 no'lu Yönerge'de olduğu gibi, fiziksel, ekonomik, kültürel, sosyal ve psikolojik kimliği ifade eden ve kişiyi belirlenebilir kılan bilgi veya kişinin, resim, ses ve görüntü kayıtları, parmak izleri kişisel veri olarak nitelendirilebilecektir.⁶¹¹ Türk hukukundaki uygulaması açısından bu sayılan bilgilerin ve ad-soyad veya işyeri bilgilerinin yanı sıra vergi numarası, T.C. kimlik numarası, malvarlığı veya okulu da kişisel veri olarak kabul edilebilecektir.⁶¹²

Tasarı, kişisel verilerin işlenmesini kişisel verilerin elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, işaretilmesi, tasniflenmesi veya engellenmesini de içerek işlemler olarak ele almaktadır. Gerekçe'de, bu nedenle, kişisel verilerin toplanmasından başlayarak tüm işlemleri içermesi dolayısıyla, geniş kapsamlı bir tanımlamanın kabul edildiği belirtilmektedir. Fakat kişisel verilerin toplanmasını da işleme olarak düzenlemek veya Tasarıda ifade edildiği üzere böyle geniş bir kapsamda

⁶⁰⁸ A.e.

⁶⁰⁹ Kişisel Verilerin Korunması Kanunu Tasarısı, m. 2 ve gerekçesi.

⁶¹⁰ Kişisel Verilerin Korunması Kanunu Tasarısı, m. 3/ç. Ayrıca bkz.: 95/46 no'lu Yönerge m. 2/a.

⁶¹¹ Kişisel Verilerin Korunması Kanunu Tasarısı'nın 3. maddesinin gerekçesi.

⁶¹² Dilek Yüksel Civelek, **Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi**, T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı, Bilgi Toplumu Dairesi Başkanlığı, Nisan 2011, s. 16.

düzenlemek, Tasarı'ya özgü bir husus değildir. Unutulmamalıdır ki, 95/46 no'lu Yönerge de, kişisel verilerin işlenmesini toplamadan (**collection**) başlayarak tüm işlemleri içine alacak şekilde düzenlemektedir.⁶¹³

Yasallık ilkesini de güvence altına alacak şekilde, kişisel verilerin bu Kanun'da ya da ilgili diğer kanunlarda öngörülen hallerde işlenebileceğini öngören Tasarı,⁶¹⁴ kişisel verilerin işlenmesine dair ilkeleri de yine Avrupa Birliği Yönergeleri ve Avrupa Konseyi'nin 108 no'lu Sözleşmesi çerçevesinde düzenlemiştir. Buna göre, kişisel verilerin hukuka ve dürüstlük kuralına uygun olarak işlenmesi, belirli, açık ve meşru amaçlar için toplanması ve bu amaçlara aykırı olarak yeniden işlenmemesi, toplandıkları amaçla bağlantılı, yeterli ve orantılı olması, doğru olması ve gerektiğinde güncellenmesi, ilgili kişilerin kimliklerini belirtecek biçimde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar saklanması zorunlu olduğu hükme bağlanmıştır.⁶¹⁵ Kaldı ki, kişisel veri kamunun yararlanmasına açık da olsa veya ilgili kişinin veri işlenmesine itirazı olmasa da, bu ilkelere uyulmasının aranması gerekecektir.⁶¹⁶

Çalışma konumuz bakımından da önem taşıyacak nitelikte, Tasarı'da hukuka uygunluk nedenlerinin de düzenlendiği görülmektedir. Öncelikle kişisel verinin konusu ilgili kişi bakımından da koruma sağlayacak şekilde, kişisel verilerin ancak ilgili kişinin açık rızasıyla işlenebileceği ilkesi gözetilmelidir. Aranacak rızanın da 95/46 no'lu Yönerge'de düzenlendiği şekliyle,⁶¹⁷ ilgili kişinin serbest iradesiyle, kendisiyle ilgili belirli bir veri işleme faaliyeti ile ilgili olarak ve yeterli şekilde bilgilendirilmiş olarak ve tereddüte yer bırakmayacak şekilde verilmiş olmasının arandığı söylenebilir.⁶¹⁸ Yasal düzenlemelerde öngörülen yükümlülüklerin yerine getirilmesi hariç, ilgili kişinin bir itirazının bulunması durumunda ise kişisel veri işlenemeyecektir.⁶¹⁹

⁶¹³ 95/46 no'lu Yönerge'nin 2/b maddesi.

⁶¹⁴ Kişisel Verilerin Korunması Kanunu Tasarısı, m. 4.

⁶¹⁵ Kişisel Verilerin Korunması Kanunu Tasarısı m. 5/1.

⁶¹⁶ Kişisel Verilerin Korunması Kanunu Tasarısı'nın 5. maddesinin gerekçesi.

⁶¹⁷ 95/46 no'lu Yönerge'nin 7. maddesi.

⁶¹⁸ Kişisel Verilerin Korunması Kanunu Tasarısı'nın 6. maddesinin gerekçesi.

⁶¹⁹ Kişisel Verilerin Korunması Kanunu Tasarısı m. 6/2.

Veri işleme için ilgili kişinin rızasının aranmasını gerektirmeyecek hukuka uygunluk sebepleri Tasarı'da ayrıca ele alınmıştır. Buna göre, kamu yararı veya resmi bir görevin yerine getirilmesi, ilgili kişi rızasını açıklayamayacak durumda iken kendisinin veya başkasının hayatını veya beden bütünlüğünü korumak, bir sözleşmenin kurulması ve ifası, ilgili kişiler tarafından açıklanmış veya açık sicillerde mevcut bilgiler olması diğer bir deyişle verinin herkesçe bilinmesi, ilgili kişinin temel hak ve özgürlüklerine zarar gelmeyecek şekilde veri kütüğü sahibinin haklı çıkarları⁶²⁰ ilgili kişinin rızası aranmadan verinin işlenmesine olanak sağlayacaktır. İletişimin önleme amaçlı denetimi sonucunda kişisel veri elde edilmesi bakımından bu hüküm uygulama alanı bulamayacaktır. Zira Tasarı'nın 22. maddesi milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbari faaliyetlerin yürütülmesi, kamu düzeninin korunması yanında suçun önlenmesi için gerekli olması durumunda 6. maddenin, Tasarı'nın uygulama alanı dışında kalacağını açıkça hükme bağlamıştır.⁶²¹ Kaldı ki, ilgili kişinin önceden rızasının alınması, önleme amaçlı denetim faaliyetinin niteliği ile de örtüşmemektedir.

Kişilerin ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkumiyetleri ile ilgili kişisel verileri, 95/46 no'lu Yönerge gibi⁶²² Tasarıda da özel niteliği olan veri olarak kabul etmiştir. Kural olarak, özel verilerin işlenmesi yasaklanmıştır. Bu verilerin işlenebilmesi de, öğrenilmesi durumunda ayrımcılık ve mağduriyet yaratabilme tehlikesi dolayısıyla sadece belli hallerde mümkündür.⁶²³ Bu hallerden

⁶²⁰ Kişisel Verilerin Korunması Kanunu Tasarısı m. 6/3.

⁶²¹ Kişisel Verilerin Korunması Kanunu Tasarısı'nın belli hükümlerinin, Tasarı'nın uygulama alanı dışında kalacağını hükme bağladığı 22. maddesi, 95/46 no'lu Yönerge'nin istisnaları öngören 13. maddesiyle paralellik gösterir.

⁶²² 95/46 no'lu Yönerge m. 8/1.

⁶²³ - Kanunla yasaklanmayan hallerde kişinin yazılı rızasının alınması,

- hukuki veya fiili nedenlerle rızasını açıklayamayacak durumda bulunan bir kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün idamesi için veri işlemenin zorunlu olması,

- ilgili kişiye yeterli koruma imkanının sağlanması şartıyla, veri kütüğü sahibinin, bu Kanunla veya diğer kanunlarla tanınan hak ve yetkileri kullananabilmesi veya yükümlülükleri yerine getirebilmesi için veri işlemenin zorunlu olması,

- vakıf, dernek, sendika ve siyasi partilerce, kuruluş amaçlarına ve tabi oldukları mevzuata uygun ve faaliyet alanıyla sınırlı olmak şartıyla, üye ve mensuplarına yönelik ve ilgili kişinin rızası olmadan üçüncü kişilere açıklanmamak kaydıyla veri işlenmesi,

biri de, suçun soruşturulmasına, koruma ve kontrol tedbirlerine ve ceza mahkumiyetlerine dair özel nitelikteki kişisel verilerin işlenebilmesidir. İlgili kanunlarda yeterli koruma tedbirinin bulunması koşulu da bu işleme için öngörülmüş ve ceza mahkumiyetlerine dair sicilin sadece Adalet Bakanlığı'nın kontrolü altında tutulabileceği da hükme bağlanmıştır.⁶²⁴ Suçun önlenmesi amacı söz konusu olduğunda, özel nitelikteki kişisel verinin işlenip işlenemeyeceğine dair bir düzenlenme söz konusu değildir. Bu durum 5397 sayılı Kanun ve ilgili diğer yasal düzenlemeler çerçevesinde⁶²⁵ yetkili makamların suçun önlenmesi amacıyla özel nitelikteki kişisel verileri işlemesine de olanak yaratıp yaratmadığına dair bir belirsizlik tehlikesi de yaratmaktadır. Böylece Tasarı'daki belirsizlik de göz önünde bulundurulduğunda, suç işlenebilir kanaatiyle dahi kişisel verinin toplanabilmesi ve kişilerin ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkumiyetlerine dair hassas kişisel verilerinin işlenebilmesi tehlikesinin ortaya çıkabileceği düşünülebilir.

Kişisel Verilerin Korunması Kanunu Tasarısı, kural olarak kişisel verilerin üçüncü kişilere aktarılamayacağını kabul etmiştir.⁶²⁶ Bununla birlikte, belirli istisnai durumlarda kişisel verinin üçüncü kişiye aktarılması mümkün olacaktır. Bu bağlamda, ulusal güvenliğin ve savunmanın sağlanması, suçun önlenmesi ya da soruşturulması amacıyla yapılan istihbari faaliyetlerle ilgili olarak kanundan doğan

-ilgili kişi tarafından alenen açıklanmış olan veriler hakkında olması,
-hukuken bir hakkı tesis, kullanma veya korunması için veri işlemenin zorunlu olması,
-koruyucu hekimlik, tıbbi teşhis, tedavi, bakım veya sağlık hizmetlerinin yürütülmesi amacıyla kişisel verilerin sağlık kurumları, sigorta şirketleri, sosyal güvenlik kurumları, işyeri sağlık birimi oluşturmakla yükümlü işverenler, sağlıkla ilgili okul ve üniversiteler tarafından ilgili kanunlara uygun olarak, hukuken veya meslek kurallarına göre sır saklama yükümlülüğü altında bulunan sağlık personeli veya eşdeğer seviyede sır saklama yükümlülüğü altındaki bir başka kişinin gözetimi altında işlenmesi halleri özel nitelikteki kişisel verilerin işlenmemesi kuralının istisnalarını oluşturmaktadır. Bununla birlikte, özel hayatın ve aile hayatının gizliliğine dokunmamak şartıyla, temel kamu yararlarının gerektirmesi halinde, ilgili mevzuatta yeterli koruma tedbiri bulunması kaydıyla, Kurul'un özel nitelikteki kişisel verilerin işlenmesine karar verebileceği ve idari nitelikteki yaptırımlar ile özel hukuk alanındaki mahkeme kararlarına dair verilerin de resmi makamların kontrolü altında işlenebileceği de kabul edilmiştir, Kişisel Verilerin Korunması Kanunu Tasarısı m. 7/2, 3, 5. Ayrıca bkz.: 95/56 no'lu Yönerge m. 8/2, 3, 4.

⁶²⁴ Kişisel Verilerin Korunması Kanunu Tasarısı m. 7/4.

⁶²⁵ 4.7.1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi, 10.3.1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi, 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 6. maddesi.

⁶²⁶ Kişisel Verilerin Korunması Kanunu Tasarısı m. 8/1.

bir görevin yerine getirilmesi için gerekli olması durumunda kamu kurum veya kuruluşu kişisel veriyi ilgili kamu kurum veya kuruluşuna aktarabilecektir. Kamu yararı, sır saklama yükümlülüğü, kişinin meşru menfaati veya kişisel verilere dair özel koruma kuralları dolayısıyla kişisel verinin üçüncü kişilere aktarılması kamu kurum veya kuruluşunca reddedilebilir, sınırlandırılabilir ya da şarta bağlanabilir.⁶²⁷

Tasarı aydınlatma yükümlülüğü çerçevesinde veri kütüğü sahibinin⁶²⁸ kendisi ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, kimlere aktarılacağı, veri toplamanın yöntemi, hukuki sebebi ve muhtemel sonuçları, kişisel verileri öğrenme hakkı ve düzeltme hakkı konusunda ilgili kişiyi bilgilendirmekle yükümlü kılındığı kabul edilmiştir.⁶²⁹ Bu bağlamda kişisel verilerin korunmasında şeffaflık ve ilgili kişinin hiçbir tereddüte yer bırakmayacak rızasının alınabilmesi de amaçlanmaktadır. Nitekim bu yükümlülük çerçevesinde kişisel veriler daha sonra da kullanılacaksa, ilgili kişiye bu konuda bilgi verilip, böyle bir kullanıma izin verip vermeyeceği hususunda iradesi alınacaktır. Bununla birlikte, eldeki veri daha sonradan, veri elde edildiği zaman belirtilmeyen bir amaç için kullanılacaksa da ilgili kişinin bilgilendirilmesi ve bu konudaki rızasının aranması söz konusu olacaktır.⁶³⁰ Bu güvenceler düzenlenmiş olmakla birlikte, ilgili kişinin rızasının aranmasına dair de istisna oluşturan milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbari faaliyetlerin yürütülmesi, kamu düzeninin korunması ve konumuz açısından önem taşıyacak şekilde suçun önlenmesi amacıyla kişisel verinin işlenmesi açısından, bu hükmün de - aydınlatma yükümlülüğünün - uygulama alanı bulmayacağı Tasarı'da açıkça kabul edilmiştir.⁶³¹

⁶²⁷ Kişisel Verilerin Korunması Kanunu Tasarısı m. 8/2, 3.

⁶²⁸ Kişisel Verilerin Korunması Kanunu Tasarısında veri kütüğü, gerçek ve tüzel kişilere dair belirli bir kriter gereği kişisel verilere ulaşımı kolaylaştıracak şekilde yapılandırılmış herhangi bir kişisel veri grubunu; veri kütüğü sahibi ise kişisel verilerin işlenmesinin amaç ve metodlarını tek başına ya da başkalarıyla birlikte belirleyen gerçek ve tüzel kişiler olarak nitelendirilmiştir, Kişisel Verilerin Korunması Kanunu Tasarısı m. 3/h ve 3/ı.

⁶²⁹ Kişisel Verilerin Korunması Kanunu Tasarısı m. 11/1. Ayrıca bkz.: 95/46 no'lu Yönerge m. 10.

⁶³⁰ Kişisel Verilerin Korunması Kanunu Tasarısı'nın 11. maddesinin gerekçesi.

⁶³¹ Kişisel Verilerin Korunması Kanunu Tasarısı m. 22.

Tasarı veri kütüğü sistemi dahilinde ilgili kişinin haklarını da düzenlemiştir. Bu bağlamda, ilgili kişiler, veri kütüğü sistemi sahibine başvurarak kendisiyle ilgili kişisel verinin kaydedilip kaydedilmediğini öğrenebilecek ve kaydedilmişse bunları talep edebilecek, düzeltilmesini, hukuka aykırı olması halinde silinmesini, yok edilmesini veya engellenmesini ve bu çerçevede yapılacak işlemlerin verinin açıklandığı üçüncü kişilere de bildirilmesini isteyebileceklerdir.⁶³²

İlgili kişinin bu hakları, önleme amaçlı denetim yoluyla verilerin işlenmesi söz konusu olduğunda sınırlandırılabilir. Zira Tasarı, suçun önlenmesi veya istihbarat amacıyla yapılan faaliyetlerle ilgili olarak kanundan doğan bir görevin yerine getirilmesi durumunda bu hakların sınırlandırılabilirliğini öngörmektedir.⁶³³

Tasarı ile ayrıca kamuoyuna açık tutulacak “Veri Kütüğü Sistemi Sicili” kurulmaktadır. Unutulmamalıdır ki, kamuoyuna açık böyle bir sicil sistemi de, telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetimi yoluyla elde edilen veriler bakımından uygulanmayacaktır. Nitekim Tasarı 22. maddesinde bu durumu istisna olarak düzenlemektedir.⁶³⁴ Bu bağlamda sadece Veri Kütüğü Sicili tutulması değil, aynı zamanda bu sicile bir bildirimle yapılacak kayıt başvurusu da⁶³⁵ aynı şekilde milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbari faaliyetlerin yürütülmesi, kamu düzeninin korunması ile suçun önlenmesi için gerekli olması amacıyla kişisel verinin işlenmesi durumu açısından uygulama alanı dışında kalmaktadır.⁶³⁶

Tasarı’da ayrıca bir ön inceleme usulü öngörülmüştür. Buna göre, veri kütüğü sahibi veya varsa temsilcisi tarafından Sicile kayıt başvurusundan itibaren en geç bir ay içinde Kişisel Verileri Koruma Kurulu tarafından ön inceleme yapılacaktır. Ön

⁶³² Kişisel Verilerin Korunması Kanunu Tasarısı m. 12/1.

⁶³³ Kişisel Verilerin Korunması Kanunu Tasarısı m. 12/3.

⁶³⁴ Kişisel Verilerin Korunması Kanunu Tasarısı m. 22.

⁶³⁵ Kayıt başvurusu için gerekli olan bildirimde, veri kütüğü sahibi veya varsa temsilcisinin kimlik ve adres bilgileri; kişisel veri işlemenin amaçları; veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar; verilerin açıklanabileceği alıcılar veya alıcı grupları; üçüncü ülkelere aktarımı öngörülen veriler; 15. madde uyarınca alınan tedbirlere ilişkin genel açıklama yer almalıdır, Kişisel Verilerin Korunması Kanunu Tasarısı m. 17/1, a-e.

⁶³⁶ A.e.

inceleme sonuçlanmadan da veri işlemesi gerçekleşemeyecektir.⁶³⁷ Böyle bir usulle kişinin temel hak ve özgürlüklerine önemli ölçüde zarar verebilecek işlemlerin veri işlemeyi önce belirlenerek engellenmesi amaçlanmaktadır. Nitekim bu ön inceleme sonucunda ortaya çıkan sonuçlar, verinin niteliği, kategorisi ve işleme amacı değerlendirilebilecektir.⁶³⁸ Kurul'un bu ön incelemeyi veri konusu ilgili kişilerin kişiliklerine ve temel hak ve özgürlüklerine ilişkin risk taşıma ihtimali olan ve kişisel verilerin işlenmesine dair belirlenen ilkelere uymayan ve Tasarı'nın kişisel verilerin işlenmesi için açık rızayı arayan ve hangi hallerde hukuka uygunluk nedenlerinin varolacağını düzenleyen 6. maddesinde ve özel nitelikteki kişisel verilerin işlenmesine dair koşulları belirleyen 7. maddesinde düzenlenen koşulları taşımayan veri işlemlerini belirlemek üzere yapması öngörülmüştür.⁶³⁹ Fakat milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbari faaliyetlerin yürütülmesi, kamu düzeninin korunması ve suçun önlenmesi için gerekli olması durumunda Kurul'un böyle bir ön inceleme yapması beklenmeyecektir.⁶⁴⁰

Verilerin hukuka aykırı olarak işlenmesi, yasal düzenlemeye uygun olarak veri kütüğüne işlenmiş verilerin korunması veya verileri gerekli süre dahilinde sistem içinde yok etme yükümlülüğünün ihmali Tasarı'da TCK'nun 135 vd. maddelerine paralel olarak ceza yaptırımına bağlanmıştır.⁶⁴¹ Bunun yanı sıra idari para cezaları ve gerçek kişilerin bu şekilde cezalandırılacak olmalarının yanı sıra, bu suçların tüzel kişiler tarafından işlenmesi durumu için tüzel kişilere özgü güvenlik tedbirleri de Tasarı kapsamında öngörülen yaptırımlar olarak değerlendirilebilir.⁶⁴²

Görülüyor ki, Tasarı'da genel itibariyle 95/46 no'lu Yönerge ve 108 sayılı Avrupa Konseyi Sözleşmesi'nin ilkeleri ve genel anlayışı benimsenmiştir. Kaldı ki, ilgili hükümlerin uygulama alanları açısından istisna oluşturabilecek hususlarda da bir paralellik farkedilebilir. Buna göre, telekomünikasyon yoluyla gerçekleştirilen iletişimin önleme amaçlı denetimi yoluyla kişisel verinin işlenmesi açısından da

⁶³⁷ Kişisel Verilerin Korunması Kanunu Tasarısı m. 19/2.

⁶³⁸ Kişisel Verilerin Korunması Kanunu Tasarısı'nın 19. maddesinin gerekçesi.

⁶³⁹ Kişisel Verilerin Korunması Kanunu Tasarısı m. 19/1.

⁶⁴⁰ Kişisel Verilerin Korunması Kanunu Tasarısı m. 22.

⁶⁴¹ Kişisel Verilerin Korunması Kanunu Tasarısı m. 34, 35.

⁶⁴² Kişisel Verilerin Korunması Kanunu Tasarısı m. 36, 37.

anlamlı olabilecek şekilde; (i) kişisel verinin işlenmesi için kişinin rızasının aranması, (ii) veri işleme sırasında ilgili kişinin aydınlatılması yükümlülüğü ve bu bağlamda kişinin haklarının uygulanması, (iii) veri kütüğü sicilinin tutulması ve bu sicile başvuru zorunluluğu ve (iv) ilgili veri işlemleri yapılmadan önce ön inceleme yapılması hallerinin milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbari faaliyetlerin yürütülmesi, kamu düzeninin korunması ve suçun önlenmesi için gerekli olması durumunda uygulanmayacağı söylenebilir.

DÖRDÜNCÜ BÖLÜM

TÜRK HUKUKUNDA TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN ÖNLEME AMAÇLI DENETLENMESİNİN ŞARTLARI VE UYGULANMASI

I. TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN ÖNLEME AMAÇLI DENETLENMESİNİN AMACI, KAPSAMI VE TÜRLERİ

A. Genel Olarak

Türk hukukunda önleme amaçlı denetim 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, adli amaçlı koruma tedbiri niteliğindeki iletişimin denetlenmesi ise CMK hükümleri bağlamında uygulanmaktadır.⁶⁴³ Çalışma konumuzu oluşturan önleme amaçlı denetim yoluyla, suç işlenmesinin önlenmesi amacıyla ve ulusal güvenlikle ilgili istihbarat faaliyeti bağlamında telekomünikasyon yoluyla yapılan iletişim denetlenmektedir. İdari nitelikte olan ve ilke olarak da gizli olarak uygulanan bu önleme tedbiri uygulanırken, demokratik rejimin ve önemli anayasal esasların korunması önem arz etmektedir.⁶⁴⁴ Koruma tedbiri olarak uygulanan, iletişimin adli amaçlı denetlenmesinde de uygulamanın gizli olduğu, aksi takdirde uygulamanın anlamsız kalacağı söz konusu olmakla birlikte; suç soruşturma ve kovuşturması çerçevesinde maddi gerçeğin araştırılması, ceza muhakemesinin sağlıklı bir şekilde yapılabilmesi ve maddi gerçeğin ortaya çıkarılmasının amaçlandığı ifade edilebilir.⁶⁴⁵

5397 sayılı Kanun'un 2005 yılında yürürlüğe girmesine kadar yasal dayanaktan yoksun olarak gerçekleştirildiği ve bu yolla kişilerin temel hak ve özgürlüklerinin

⁶⁴³ Öztürk ve diğerleri, *a.g.e.*, s. 466 vd.

⁶⁴⁴ Sözüer, *a.g.m.*, s. 86, 87.

⁶⁴⁵ Cumhur Şahin, *Ceza Muhakemesi Hukuku I*, 2. bs., Ankara, Seçkin, 2011, s. 262, 263; Sözüer, *a.g.m.*, s. 70; Mehmet Saydam, *Ceza Muhakemesi Kanununa Göre Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi*, İstanbul, On İki Levha, 2011, s. 83; Kaymaz, *a.g.e.*, s. 55.

ihlal edildiği de göz önünde bulundurulursa; telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesinin amacı, kapsamı ve türlerini 5397 sayılı Kanunu dikkate alarak polis, jandarma ve milli istihbarat teşkilatı açısından ayrı ayrı incelemek yerinde olabilir. Nitekim henüz ortada bir suç yok iken, belirli amaçların gerçekleştirilmesi için telekomünikasyon yoluyla gerçekleşen iletişimi denetleyebilme olanağı polis, jandarma ve milli istihbarat teşkilatı yetkililerine verilmiştir.

B. İletişimin Önleme Amaçlı Denetlenmesinin Amacı

1. Polis Bakımından

2559 sayılı PVSK,⁶⁴⁶ ek 7. maddesinin birinci fıkrasında belirtilen görevlerin yerine getirilmesine yönelik olarak telekomünikasyon yoluyla yapılan iletişimin denetlenebileceğini kabul etmektedir.⁶⁴⁷ Buna göre, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişini sağlamak üzere ve ülke seviyesinde istihbarat faaliyetlerinde bulunmak amacıyla iletişimin denetlenmesi söz konusu olabilecektir. Polis, bu amaçla bilgi toplamak, değerlendirmek, yetkili mercilere veya kullanma alanına ulaştırmak ve Devletin diğer istihbarat kuruluşlarıyla da işbirliği de yapabilmek üzere yetkili kılınmıştır.⁶⁴⁸ Kaldı ki, polisin “suç öncesi polis fonksiyonu”⁶⁴⁹ olarak ifade edilebilecek görevi dahilinde genel itibariyle kamu düzenini korumanın yanı sıra suçun önlenmesinin de yer aldığı kabul edilir.⁶⁵⁰

⁶⁴⁶ 2559 sayılı, 04/07/1934 tarihli Polis Vazife ve Salahiyet Kanunu, R.G. tarih: 14/7/1934, Sayı: 2751.

⁶⁴⁷ 5397 sayılı Kanun ile 2559 sayılı Polis Vazife ve Salahiyet Kanunu’nun ek 7. maddesine dahil edilen ikinci fıkra.

⁶⁴⁸ 2559 sayılı Polis Vazife ve Salahiyet Kanunu’nun ek 7. maddesinin birinci fıkrası.

⁶⁴⁹ R. Füsün Sokullu-Akıncı, **Polis: Toplumsal Bir Kurum Olarak Gelişmesi, Polis Alt-Kültürü ve İnsan Hakları**, İstanbul, 1990, s. 97-122.

⁶⁵⁰ Sokullu-Akıncı, **a.g.e.**, s. 97-102.

2. Jandarma Bakımından

2803 sayılı Jandarma Kanunu,⁶⁵¹ 7/a maddesinde belirtilen görevler yerine getirilirken önleyici tedbir almak üzere⁶⁵² telekomünikasyon yoluyla yapılan iletişimin denetlenebileceğini hükme bağlamaktadır.⁶⁵³ Buna göre, Jandarma, emniyet ve asayiş ile kamu düzenini sağlamak, korumak ve kollamak, kaçakçılığı men, takip ve tahkik etmek, suç işlenmesini önlemek için gerekli tedbirleri almak ve uygulamak, ceza infaz kurumları ve tutukevlerinin dış korunmalarını yapmak şeklinde ortaya çıkan mülki görevlerini⁶⁵⁴ yerine getirmek üzere; sadece kendi sorumluluk alanında, belirli suçların işlenmesinin önlenmesi amacıyla bu denetim yoluna başvurabilecektir.⁶⁵⁵

3. Milli İstihbarat Teşkilatı Bakımından

2937 sayılı MİT Kanunu, 4. maddesinde düzenlenen ve Türkiye Cumhuriyetinin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı yöneltilen mevcut ve muhtemel faaliyetlere dair milli güvenlik istihbaratını Devlet çapında oluşturmak görevini kapsayan ve genel itibarıyla ulusal güvenlik ve istihbarat ile ilgili görevlerin⁶⁵⁶ yerine getirilmesi amacıyla telekomünikasyon yoluyla yapılan

⁶⁵¹ 2803 sayılı, 10/03/1983 tarihli Jandarma Teşkilat, Görev ve Yetkileri Kanunu, R.G. tarih: 12/03/1983, Sayı: 17985.

⁶⁵² Koruyucu tedbir alınması açısından da aynı esas benimsenmiştir. Buna göre, koruyucu tedbirleri almak üzere de telekomünikasyon yoluyla iletişimin denetlenmesi için de sayılan görevlerin yerine getirilmesi esası kabul edilmiştir, 2803 sayılı Jandarma Kanunu'nun ek 5. maddesi.

⁶⁵³ 2803 sayılı Jandarma Kanunu'nun ek 5. maddesi.

⁶⁵⁴ Jandarma'nın bu görevleri dışında, işlenmiş suçlarla ilgili olarak kanunlarda belirtilen işlemleri yapmak ve bunlara ilişkin adli hizmetleri yerine getirmek şeklinde adli; askeri kanun ve nizamların gereği görevlerle Genelkurmay Başkanlığınca verilen görevleri yapmak üzere askeri ve belirtilen bu görevler dışında kalan ve diğer kanun ve nizam hükümlerinin icrası ile bunlara dayalı emir ve kararlarla Jandarmaya verilen görevleri yapmak şeklinde diğer görevleri bulunmaktadır, 2803 sayılı Jandarma Kanunu m. 7/b, c ve d. Fakat bu görevler telekomünikasyon yoluyla yapılan iletişimi denetleme tedbirini uygulayabileceği görevleri arasından sayılmamıştır.

⁶⁵⁵ 5397 sayılı Kanun ile 2803 sayılı Jandarma Kanunu'na dahil edilmiş ek 5. madde.

⁶⁵⁶ MİT'in bu görevleri a) Türkiye Cumhuriyetinin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı Cumhurbaşkanlığı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak; b) Devletin milli güvenlik

iletişimin önleme amaçlı denetlenmesine MİT tarafından başvurulabileceğini öngörmektedir. Bu görevlerin yerine getirilmesi amacıyla 1982 Anayasası'nın ikinci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak bu tedbire başvurulabilmesi söz konusu olabilecektir.⁶⁵⁷

C. İletişimin Önleme Amaçlı Denetlenmesinin Kapsamı

Telekomünikasyon kavramının “işaret, sembol, ses ve görüntü ile elektrik sinyallerine dönüştürülebilen her türlü verinin; kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektro kimyasal, elektro mekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması” olarak açıklandığı da dikkate alındığında;⁶⁵⁸ telekomünikasyon kavramının aslında iletişimin tel, radyo, optik vb. elektromanyetik sistemlerle yapılanı olduğu tespitini daha önce yapmıştık. Bu tespitin iletişimin denetlenmesinin kapsamını belirleyeceğimiz bu noktada tekrarlanması şu açıdan yerinde olabilir. Görülüyor ki, genel tanımlama itibariyle örneğin, telgraf gibi iletişim araçları ile radyo ve televizyon gibi kitle iletişim araçları da telekomünikasyon kapsamında kalmaktadır. Fakat konumuzu oluşturan telekomünikasyon yoluyla yapılan iletişimin denetlenmesi bakımından radyo, televizyon gibi kitle iletişim araçları kapsam dışında kalmaktadır.⁶⁵⁹ Kaldı ki, telgraf veya çeşitli elektromanyetik araçlarla gönderilen bilgi şeklindeki posta hizmeti bağlamındaki iletişim araçları da kapsam dışındadır. Nitekim suçun delillerini oluşturduğundan şüphe edilen ve gerçeğin ortaya çıkarılması için soruşturma ve

siyasetiyle ilgili planların hazırlanması ve yürütülmesinde; Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamak; c) Kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için Milli Güvenlik Kurulu ve Başbakana tekliflerde bulunmak; d) Kamu kurum ve kuruluşlarının istihbarat ve istihbarata karşı koyma faaliyetlerine teknik konularda müşavirlik yapmak ve koordinasyonun sağlanmasında yardımcı olmak; e) Genelkurmay Başkanlığınca Silahlı Kuvvetler için lüzum görülecek haber ve istihbaratı, yapılacak protokole göre Genelkurmay Başkanlığına ulaştırmak; f) Milli Güvenlik Kurulunda belirlenecek diğer görevleri yapmak ve g) istihbarata karşı koymak olarak düzenlenmiştir, MİT Kanunu m. 4.

⁶⁵⁷ MİT Kanunu'nun, 5397 sayılı Kanunla değiştirilmiş, 6. maddesi.

⁶⁵⁸ TİB Yönetmeliği'nin 3/r maddesi ve İletişimin Denetlenmesi Yönetmeliği'nin 4/j maddesi.

⁶⁵⁹ Sözüer, a.g.m., s. 70.

kovuşturmada adliyenin eli altında olması zorunlu sayılıp, posta hizmeti veren her türlü resmi veya özel kuruluşta bulunan gönderilere el konulması, CMK tarafından postada el koyma tedbiri şeklinde ayrı bir tedbir olarak düzenlenmiştir.⁶⁶⁰ Bu bağlamda örneğin posta hizmeti veren kuruluşta olan telgraf, gönderi olarak kabul edilebilecek ve postada el koyma tedbirine konu olabilecektir.⁶⁶¹

Önleme amaçlı denetime konu olabilecek telekomünikasyon yoluyla yapılan iletişim kapsamına sadece telefon konuşmaları değil, teleks, faks,⁶⁶² email ve kablolu veya kablosuz birbirine bağlı bilgisayarlar ile yürütülen iletişim dahil edilebilecektir.⁶⁶³ Bununla birlikte mobil telefonlar aracılığıyla yapılan iletişim ve belirtilen kapsam dahilinde kalan hakkında tedbir uygulanacak kişinin üzerine kayıtlı ya da kullandığı iletişim araçlarının tümü açısından da söz konusu olabilecektir.⁶⁶⁴

D. İletişimin Önleme Amaçlı Denetlenmesinin Türleri

1. Genel Olarak

Telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesi bağlamında dört tür denetleme işleminin düzenlendiği söylenebilir. Buna göre, iletişimin tespiti, iletişimin dinlenilmesi, iletişimin kaydedilmesi, sinyal bilgilerinin dinlenilmesi ve kayda alınması iletişimin önleme amaçlı denetlenmesinin türleri

⁶⁶⁰ CMK m. 129.

⁶⁶¹ El koyma konusu gönderiler için bkz. Kunter, Yenisey, Nuhoglu, **a.e.**, s. 635, 636.

⁶⁶² Faks açısından, posta hizmeti veren resmi veya özel kuruluşta bulunan faksın (faks metninin) postada el koyma tedbiri hükümlerine göre değerlendirilmesi gerektiği söylenebilir. Fakat kişilerin kendi cihazlarıyla birbirlerine gönderdikleri faksın iletimi sırasında telekomünikasyon yoluyla yapılan iletişimin denetimi söz konusu olacaktır. Nitekim faksın iletimiyle içeriğinin okunması iletişimin denetlenmesi kapsamında nitelendirilebilmektedir, Kaymaz, **a.g.e.**, s. 138, 139; Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 51.

⁶⁶³ Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 44, Taşkın, **a.g.e.**, s. 75; Sözüer, **a.g.m.**, s. 72.

⁶⁶⁴ İletişimin Denetlenmesi Yönetmeliği, m. 7/2. Bu bağlamda, bir kişinin kendi kullandığı şebeke üzerinden veya hizmet aldığı operatörün başka bir operatörle yaptığı anlaşmaya dayanarak mobil telefonunu yurtdışında kullanması durumunda, bu mobil telefonla yurtdışında gerçekleştirilen iletişimin denetlenmesi düşünülebilir.

olarak ortaya çıkmaktadır.⁶⁶⁵ CMK kapsamında bir koruma tedbiri olarak yer alan mobil telefonun yerinin tespiti önleme amaçlı denetimin türleri arasında yer almamaktadır. Nitekim mobil telefonun yerinin tespiti, delil elde etme amacıyla değil, şüpheli veya sanığın yakalanması amacıyla başvurulmuş bir tedbir olarak düzenlenmiştir.⁶⁶⁶ Kaldı ki, sadece şüpheli veya sanığın kullanmakta olduğu mobil telefon değil,⁶⁶⁷ şüpheli veya sanığın yakalanmasını sağlayabilecek şekilde diğer kişilere ait mobil telefonların yerinin tespiti de mümkün olabilecektir.⁶⁶⁸ Önleme amaçlı denetimde ise, işlenmiş bir suç ve şüpheli veya sanık bulunmamakta ve bu nedenle böyle bir kişinin yakalanmasına yönelik olarak mobil telefonun yerinin tespiti, uygulanan bir denetim işlemi olarak karşımıza çıkmamaktadır.

5397 sayılı Kanun, teknik araçla izlemeye de yer vermiştir. Önleme amaçlı teknik izleme polise ve jandarmaya PYSK'nun ek 7. maddesi ve Jandarma Kanunu'nun ek 5 maddesiyle tanınırken, MİT Kanunu ile istihbarat teşkilatı yetkilileri için bu yetki düzenlenmemiştir. Polis ve jandarmanın başvurabileceği teknik araçlarla izlemenin de, ses ve görüntü kaydını içermeyip⁶⁶⁹ sadece izlemeye olanak tanıdığı kabul edilebilir.⁶⁷⁰ Teknik araçla izleme telekomünikasyon yoluyla yapılmayıp, bu yönüyle iletişimin denetlenmesi kapsamında bulunmadığı için burada telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesinin türleri arasında incelenmeyecektir. CMK'nın 135. maddesi bağlamında öngörülen iletişimin denetlenmesi tedbirlerine benzeyen veya ondan ayrılan yönlerine ise, genel esasların daha iyi anlaşılabilmesi açısından yeri geldikçe değinilecektir.

⁶⁶⁵ 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7 nci maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 6 ncı maddesi.

⁶⁶⁶ CMK m. 135/4.

⁶⁶⁷ CMK'nın 135/4. maddesinin ilk şeklinde "kullanmakta olduğu" mobil telefonun yerinin tespitinden söz edilmekteydi. 25/5/2005 tarihli ve 5353 sayılı Kanunun 17. maddesiyle, dördüncü fıkradaki "kullanmakta olduğu" ve "kullanılan" ibareleri madde metninden çıkarılmıştır.

⁶⁶⁸ Mobil telefonun yerinin tespitini bağımsız bir iletişimin denetlenmesi türünden çok, iletişimin tespiti ile sinyal bilgilerinin değerlendirilmesi olarak kabul eden görüş için bkz.: Şahin, **a.g.e.**, s. 263; Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 45-47.

⁶⁶⁹ CMK'nın 140. maddesi kapsamındaki teknik araçlarla izlemeye ise, belirli koşullar dahilinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyerinin teknik araçlarla izlenebileceği ve ses veya görüntü kaydının alınabileceği açıkça düzenlenmiştir.

⁶⁷⁰ Ersan Şen, **a.g.e.**, s. 80.

2. İletişimin Tespiti

İletişimin tespiti gerek TİB Yönetmeliği'nde gerek İletişimin Denetlenmesi Yönetmeliği'nde iletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemler olarak nitelendirilmektedir.⁶⁷¹ Bu bağlamda, bir telefon numarasından kimlerin ne zaman arandığının, ne kadar süreyle görüşüldüğünün ve e-mailer bakımından da email gönderenin veya alıcının internet adresi, bağlantının zamanı ve bağlantı için kullanılan sistem ve bağlantı yollarının belirlenmesi iletişimin tespiti olarak kabul edilebilir.⁶⁷² Nitekim bilgisayar sistemi kullanılarak yapılan bir iletişime ilişkin olarak, bu iletişim zincirinin bir parçası durumundaki bilgisayar sistemi tarafından üretilen ve bu iletişimin başlangıç noktasını,⁶⁷³ varış noktasını,⁶⁷⁴ izlediği yolu, tarihini, saatini, boyutlarını ve süresini ya da bu iletişimde kullanılan hizmetin türünü gösteren ve trafik verisi olarak nitelendirilen bilgisayar verilerinin⁶⁷⁵ tespiti de iletişimin tespiti olarak değerlendirilebilir.

İletişimin tespiti, AİHM yaklaşımında **metering** olarak adlandırılan kavramla paralellik göstermektedir.⁶⁷⁶ AİHM bir kararında,⁶⁷⁷ İngiliz Telekomünikasyon Kurumu'nun, bir telefonda hangi numaraların arandığını, bu aramaların saati ve süresini kaydedecek bir araç kullanarak uyguladığı bir usul olan **metering** hakkında

⁶⁷¹ TİB Yönetmeliği, m. 3/i; İletişimin Denetlenmesi Yönetmeliği m. 4/f.

⁶⁷² Şahin, **a.g.e.**, s. 263; Şen, **a.g.e.**, s. 84; Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 45.

⁶⁷³ Başlangıç noktası, "hizmet sağlayıcının hizmet verdiği iletişim aracını tanımlayacak bir telefon numarası, internet protokol adresi (IP numarası) ya da benzeri bir bilgi" olarak kabul edilebilir, Serap Keskin, "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi," **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C.LIX, No:1-2, 2001, s. 173.

⁶⁷⁴ Keskin varış noktasını "iletinin aktarıldığı iletişim aracına ait benzer bilgi" şeklinde açıklamaktadır, Keskin, **a.g.m.**, s. 173.

⁶⁷⁵ 2002/58 no'lu Yönetmelik m. 2/b; Council of Europe ETS No. 185, Convention on CyberCrime (Avrupa Konseyi Siber Suç Sözleşmesi), m. 1/d, Budapest, 23.11.2001, (Çevrimiçi) <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>, 10 Ocak 2012.

⁶⁷⁶ Metering kelime anlamıyla Türkçeye ölçme olarak çevrilebilir. Bu bağlamda suyun veya gazın ne kadar kullanıldığı ya da bir yolculuk ücretinin ne kadar tuttuğunun ölçülmesi de metering kavramını örneklemek olarak kullanılmaktadır, Cambridge Dictionaries Online, (Çevrimiçi) http://dictionary.cambridge.org/dictionary/business-english/meter_2, 10 Ocak 2012.

⁶⁷⁷ Case of Malone v. The United Kingdom (Application No. 8691/79), Strasbourg, 2 Ağustos 1984, para 83-88.

değerlendirmede bulunmuştur. Mahkeme, burada ilgili kurumun sadece servis sağlayıcı olarak kendisine gönderilen sinyalleri kullanarak bu kayıtları yaptığını ve böylece telefon konuşmalarının izlenmesinin veya içeriğine müdahale edilmesinin söz konusu olmadığını belirtmiştir. İlgili Devlet ise aslında bu noktadan hareketle, bu yolla iletişimin denetlenmesini oluşturacak bir faaliyette bulunmadığı ve herhangi bir hak ve özgürlüğün ihlal edilmediğini ileri sürmüştür.⁶⁷⁸ Fakat Mahkeme aynı şekilde düşünmediğini genel itibarıyla şu gerekçelerle açıklamaktadır: Bu ölçme yöntemi eğer örneğin faturalama amacıyla uygulanmışsa, hukuka uygunluk nedenlerini taşımayan, iletişimin içeriğine yapılan haksız müdahalelerden farklılık arz eder. Bir başka ifadeyle, bu yöntemle elde edilen verinin hangi amaçla olursa olsun kullanılması, AIHS'nin 8. maddesine dair bir sorunu gündeme getirebilir. Nitekim bir kişinin hangi numaraları aradığına ilişkin bilginin kaydedilmesi, kişinin telefonla kurduğu iletişimin tamamlayıcı unsurlarından biri olarak değerlendirilmelidir. Bu bağlamda, Mahkeme böyle bir bilginin abonenin rızası olmadan polise verilmesinin, AIHS'nin 8. maddesinde garanti altına alınan hakka müdahale teşkil edeceğini hükme bağlamıştır.⁶⁷⁹

Kısacası, AIHM tarafından da iletişimin bu şekilde tespiti - **metering** - iletişimin içeriğine müdahale edilen denetim yollarından ayrı tutulmuş ve fakat iletişimin ve bu bağlamda özel yaşamın gizliliği ile yakından ilgili olduğu kabul edilmiştir. Hakikaten de, iletişimin tespiti ile elde edilen yer, kimlik, aranma ve arama bilgileri kişisel veri olarak nitelendirilebilecek bilgileri oluşturmaktadır. Bununla birlikte, kişinin kurduğu iletişimin içeriğine ulaşılmasa da, kimleri aradığı, kimler tarafından arandığı gibi bilgiler dahi kişinin tek başına olabilmesi ve kişisel bağımsızlığı ile bağlantılı kabul edilmelidir. Ayrıca kendisine ait bilgiyi ne zaman, ne şekilde ve ne kapsamda başkalarıyla paylaşacağını belirleyebilmelerine ilişkin taleplerinin korunması olarak⁶⁸⁰ kendini gösteren özel yaşamın gizliliği hakkının diğer yönüyle de doğrudan ilişkili olarak değerlendirilmelidir.

⁶⁷⁸ Case of Malone v. The United Kingdom, para 83.

⁶⁷⁹ Case of Malone v. The United Kingdom, para 83-88.

⁶⁸⁰ Özel yaşamın gizliliğine dair yaklaşımlar ve özel yaşamın gizliliğinin koruduğu değerler açısından ayrıntılı değerlendirme için çalışmanın ilk bölümüne bakınız.

İletişimin tespiti Türk hukukunda hem telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesinin türlerinden hem de CMK'nın 135. maddesi kapsamında iletişimin denetlenmesi türlerinden biri olarak karşımıza çıkmaktadır. CMK'nın 135. maddesi bağlamında, gerek iletişimin tespiti gerek mobil telefonun yerinin tespiti şeklinde iki ayrı yerde tespit kavramıyla karşılaştık da, iki farklı tedbirin ifade edildiğini söyleyebiliriz.⁶⁸¹ Bu bağlamda, CMK'nın 135. maddesinin birinci fıkrası açısından, örneğin telefonun bulunduğu veya telefonu kullanan kişinin bulunduğu yer ve kimlik bilgisinin belirlenmesi; dördüncü fıkrası bakımından ise,⁶⁸² mobil telefonun yerinin belirlenmesinin düzenlendiği değerlendirilmiştir.⁶⁸³ CMK bağlamında iletişimin tespitine tüm suçlar bakımından başvurulabileceği ve sadece katalog suçlarla sınırlı olunmayacağı ifade edilebilir. Nitekim CMK'nın 135/1 maddesinde bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, diğer tedbirlerle birlikte telekomünikasyon yoluyla iletişimin tespiti tedbirine de başvurulabileceği belirtilmektedir. Ayrıca 135. maddenin altıncı fıkrasında da, katalog suçlar bakımından uygulanabilecek tedbirler⁶⁸⁴ sayılırken iletişimin tespiti belirtilmemiştir. Bu bağlamda sadece katalog suçlar değil, tüm suçlar açısından ilgili usul ve esaslar dahilinde iletişimin tespiti tedbirine başvurulmasının öngörüldüğü düşünülebilir.⁶⁸⁵

Önleme amaçlı iletişimin tespiti ise, 5397 sayılı Kanun'a göre, polis ve jandarma bakımından CMK'nın 250. maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde

⁶⁸¹ Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 45, 46.

⁶⁸² CMK m. 135/4 ile mobil telefonun yerinin tespitini düzenlemiş ve "şüpheli veya sanığın yakalanabilmesi için, mobil telefonun yerinin, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararına istinaden tespit edilebileceğini; bu hususa ilişkin olarak verilen kararda, mobil telefon numarası ve tespit işleminin süresinin belirtileceğini; tespit işleminin en çok üç ay için yapılabileceğini ve bu sürenin, bir defa daha uzatılabileceğini" kabul etmiştir.

⁶⁸³ Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 46; Şahin, **a.g.e.**, s. 263 ve 269. İletişimin içeriğine müdahale edilmeden elde edilen arama, aranma, yer bilgisi ve kimlik bilgilerini dış bağlantı verileri olarak değerlendiren ve böylece CMK m. 135'e tabi tutulamayacağını belirten görüş için bkz.: Öztürk ve diğerleri, **a.g.e.**, s. 473.

⁶⁸⁴ CMK m. 135/6'da bu madde çerçevesinde dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümlerin ancak sayılan suçlarla ilgili olarak uygulanabileceği düzenlenmiştir.

⁶⁸⁵ Özbek ve diğerleri, **a.g.e.**, s. 402. İletişimin tespiti ve mobil telefonun yerinin tespiti gibi özel hayatın gizliliğine müdahaleyi daha hafif gerçekleştiren tedbirlerin, tüm suçlar açısından uygulanabilmesine imkan tanıma amacının benimsendiği de ileri sürülmüştür, Kaymaz, **a.g.e.**, s. 119.

yazılı suçlar;⁶⁸⁶ MİT açısından ise MİT Kanun'un 4. maddesinde sayılan görevlerin görevlerin yerine getirilmesi amacıyla Anayasanın 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 için uygulama alanı bulacaktır.⁶⁸⁷ Bu bağlamda uygulanacak suçlar açısından tedbirlere göre bir ayrılma da bulunmamakta ve iletişimin tespiti de, aynı suçların önlenmesi amacıyla söz konusu olabileceği görülmektedir. İletişimin tespitine dair kararlar ise TİB tarafından yerine getirilecektir.⁶⁸⁸ Uygulamada TİB, 23.07.2006 tarihinden⁶⁸⁹ sonraki iletişimin tespitine dair bilgilere sahip bulunmaktadır. Bu nedenle, iletişimin tespiti kararı verildiğinde bu bilgiler, ilgili birimlere aktarılmaktadır. Fakat 23.07.2006 tarihinden önceki iletişimin tespiti işleminin konusunu oluşturacak iletişim bilgilerinin iletişimin tespiti tedbiri çerçevesinde elde edilmesi gerekli ise, TİB tarafından işletmecilere bir talimat gönderilmektedir. Bu durumda dahi, kararın kendisi işletmecilere verilmemektedir.⁶⁹⁰

⁶⁸⁶ Bunlar Türk Ceza Kanunu'nda yer alan a) örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imâl ve ticareti suçu veya suçtan kaynaklanan malvarlığı değeri aklama suçu, b) haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar, c) ikinci kitap dördüncü kısmın dört, beş, altı ve yedinci bölümünde tanımlanan suçlar (305, 318, 319, 323, 324, 325 ve 332. maddeler hariç) olarak düzenlenmiştir.

⁶⁸⁷ 5397 sayılı Kanun'un 1., 2. ve 3. maddesi.

⁶⁸⁸ TİB Yönetmeliği m. 17.

⁶⁸⁹ TİB'in kuruluşu için 6 ay ek süre tanınmasını düzenleyen 1.2.2006 tarihli ve 5453 sayılı Kanun 7 Şubat 2006 tarihli ve 26073 sayılı Resmi Gazete'de yayımlandı. "Faaliyete geçiş dönemi uygulamalarına ilişkin olarak Yönetmeliğe geçici madde eklenmesini öngören "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" 24 Şubat 2006 tarihli Resmi Gazetede yayımlandı.", (Çevrimiçi) <http://www.tib.gov.tr/kat/tarihce.html>, 29 Ocak 2012.

⁶⁹⁰ TİB ayrıca adli soruşturmalar ve kovuşturmalar kapsamında TİB'e posta veya faks ile gönderilen ya da elden teslim edilen iletişimin tespiti talep ve kararlarının işlemsiz iade edilmemesi için dikkat edilmesi gereken noktaları da yayımlamıştır. Buna göre, adli bir soruşturma veya kovuşturma kapsamında TİB'e intikal eden iletişimin tespiti talebine dair başvuruda, "1) Adalet Bakanlığı Yönetmeliğinin 6. maddesi gereğince; Cumhuriyet savcısı, hâkim ve mahkeme kararlarında aşağıda sayılan hususların bulunması gerektiği, bu bağlamda; soruşturma numarası veya kovuşturmaya geçilmişse mahkeme esas numarası, kararın hangi suçun soruşturması için istendiği ve bu suçun işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığına ilişkin açıklama, başka suretle delil elde edilmesi imkânının bulunmadığı hakkındaki açıklama, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü ile numarası veya iletişim bağlantısının tespitine imkân veren kodu, tedbirin türü, tedbirin kapsamı, tedbirin süresi; 2) tedbir kararı, 5271 sayılı Ceza Muhakemesi Kanununun 135 inci maddesinin üçüncü fıkrası gereğince, en çok üç ay için verilebilmekte, gerekiyorsa bir defaya mahsus olmak üzere üç ay daha uzatılabilmektedir. Ancak, bir örgüt faaliyeti çerçevesinde işlenen suçlarla ilgili olarak, gerekli görülmesi halinde hâkim bir aydan fazla olmamak üzere sürenin

3. İletişimin Dinlenmesi

Telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmalar ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi iletişimin dinlenmesi olarak nitelendirilebilir.⁶⁹¹ Buna göre, dinlemenin konuşmayla eş zamanlı olarak ve teknik araçla, yetkili kılınan üçüncü kişi tarafından yapılması gerektiği ifade edilebilir. Fakat uygulamada, üçüncü bir kişinin eş zamanlı dinlemesi yerine çoğunlukla, konuşmanın kayıt altına alınması söz konusu olmaktadır. Nitekim teknik araç kullanılmadan bir yerde bulunarak konuşmaların çıplak kulakla dinlenmesi, bu çerçevede iletişimin dinlenmesi olarak değerlendirilmeyecektir.⁶⁹² Telefon konuşmaları gibi, internet üzerinden yapılan konuşmaların dinlenmesi de iletişimin dinlenmesi kapsamında bulunmaktadır.⁶⁹³ Zira telekomünikasyon kavramı kapsamındaki araçlarla yapılan bir iletişimden ve iletişimin gerçekleştiği sırada uygun bir teknik araçla yapılan dinlemeden söz edilmektedir. Bu nedenle gerek

müteaddit defalar uzatılmasına karar verebilmektedir. Evrakın süre nedeniyle iade edilmemesi için, kararlarda belirtilen tarih veya tarih aralığında yukarıdaki hususlara azami dikkat edilmesi, tedbirin süresi ile ilgili olarak, karışıklığa mahal verilmeyecek şekilde açık ve net bir tarih ya da tarih aralığı (Örneğin 01.08.2009 ila 30.08.2009 arası gibi) verilmesi, eksik, belirsiz ve muğlak ifadeler kullanılmaması gerektiği; 3) yetkili imzaların, özellikle de Savcılık kararlarında, Cumhuriyet savcısının adı-soyadı, sicil numarası, savcılık mührü ve imzasının eksik olmaması gerektiği; 4) şayet tutuklu iş/gözlem altında bulunma/kayıp şahıs ile ilgili bir durum varsa, evrakın gereğinin ivedi olarak yerine getirilmesi için bu durumun evrakta açıkça belirtilmesi gerektiği, (Ayrıca kovuşturma safhasına ilişkin mahkeme kararlarında “duruşma tarihinin” belirtilmesi işlem sürecini hızlandıracaktır.); 5) resmi yazışma kuralları gereğince, TİB’i muhatap bir üst yazının (talep yazısı) yazılması gerektiği, (Örneğin bir hâkim ya da mahkeme kararının bir üst (talep yazısı) olmaksızın TİB’e gönderilmesi ya da faks çekilmesi durumunda, evrakın gereği yapıldıktan sonra muhatap merci bilinmediğinden evrak ilgisine intikal ettirilememektedir.); 6) yetkili ve görevli Cumhuriyet savcısının görevlendirmesiyle kolluk birimleri tarafından TİB’e intikal ettirilen evrakta da, (a), (b), (c), (d) ve (e) maddelerinde belirtilen hususlar eksiksiz olarak yer almalıdır. Sadece kolluğa ait evrakın alt kısmına Cumhuriyet savcıları tarafından yapılan ve özellikle de soruşturma numarasını haiz olmayan bir havale, evrakın gereğinin yapılması için yeterli olamamakta ve TİB tarafından soruşturma numarası eksik olduğundan iade edilmektedir. Bu nedenle özellikle cinayet, terör, örgütlü suçlar, çocuk kaçırma, kaybolma vb. gibi niteliği gereği ivedilik arz eden evrakın iade edilmemesi için yukarıdaki hususların eksik olmaması gerektiği; 7) TİB’e intikal ettirilen evrakta, soruşturma numarası ya da esas numarasının bulunması ilgili mevzuat gereği zorunluluk arz ettiğinden, talep numaralı, muhabere numaralı, kabahat numaralı, el koyma numaralı, kolluk suç no vb. talepler gönderilmemesi gerektiği; 8) 5271 sayılı Ceza Muhakemesi Kanunu uyarınca, iletişimin tespiti taleplerinde hakkında tedbir uygulanacak kişinin/kişilerin, şüpheli ya da sanık sıfatını haiz olması gerektiğinden, bu sıfatı haiz olmayan kişilere (tanık, müdahil, ihbarcı, maktulün yakınları, müştekinin arkadaşı vb.) ilişkin iletişimin tespiti talebinde bulunulmaması gerektiğinin (...)” değerlendirildiği ifade edilmektedir, İletişimin Tespiti Taleplerine İlişkin Açıklamalar, (Çevrimiçi) <http://www.tib.gov.tr/evraklar.html>, 30 Ocak 2012.

⁶⁹¹ TİB Yönetmeliği m. 3/h; İletişimin Denetlenmesi Yönetmeliği m. 4/e.

⁶⁹² Şahin, a.g.e., s. 263, 264; Kunter, Yenisey, Nuhoglu, a.g.e., s. 45; Şen, a.g.e., s. 84.

⁶⁹³ Şahin, a.g.e., s. 263; Taşkın, a.g.e., s. 194.

hiçbir araç kullanılmadan yapılan bir konuşmanın teknik araçla dinlenilmesi⁶⁹⁴ gerek telekomünikasyon yoluyla yapılan iletişim dahilindeki bir araçla yapılan konuşmanın bu sefer hiçbir teknik araç kullanılmadan dinlenilmesi iletişimin dinlenmesi tedbirini oluşturmayacaktır.

Gerek TİB Yönetmeliği gerek İletişimin Denetlenmesi Yönetmeliği, iletişimin dinlenmesinin yanı sıra iletişimin kaydedilmesine de yer vermiştir.⁶⁹⁵ Bu bağlamda iletişimin dinlenmesi ve kaydedilmesi farklı iki tedbir türünü oluşturmaktadır. İletişimin dinlenmesinde canlı dinleme söz konusu iken,⁶⁹⁶ kayda almada konuşmaların bir kayıt cihazına kaydı söz konusudur.⁶⁹⁷ Her dinlenen iletişimin kaydedilmesi zorunluluğu bulunmamaktadır. Bununla birlikte, şu da belirtilmelidir ki, dinlenen iletişimin kaydedilmesinin iletişimin denetlenmesi tedbirinden yeterli bir şekilde yararlanılması için gerekli olabileceği de ileri sürülür. Nitekim iletişimi dinlenen kişilerin söylediklerinin tam belirlenebilmesini, gerekiyorsa birden fazla kez dinlenebilmesini, başka konuşmalarla birlikte değerlendirilebilmesini sağlamak üzere dinlemenin yanında iletişimin kayda da alınması gerekliliği olabilir.⁶⁹⁸ İletişimin dinlenilmesi yanında kaydı da yapılacaksa, denetimin usulüne göre gerçekleşmesi açısından ilgili kararda kaydedileceği de belirtilmelidir.⁶⁹⁹

4. İletişimin Kayda Alınması

İletişimin kaydedilmesi, telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmaların ve diğer her türlü iletişimin kayda alınmasını ifade etmektedir.⁷⁰⁰ İletişimin dinlenmesine paralel olarak, iletişimin kayda alınması için de konuşmayla eş zamanlı olarak ve uygun bir teknik araçla kaydın yapılması zorunluluğu

⁶⁹⁴ Böyle bir uygulama CMK m. 140 bağlamında teknik araçla izlemeyi düşündürebilir.

⁶⁹⁵ TİB Yönetmeliği m. 3/h; İletişimin Denetlenmesi Yönetmeliği m. 4/e.

⁶⁹⁶ İletişimin dinlenmesi böyle bir canlı dinlemeyi gerekli kıldığından, kaydedilen iletişimin daha sonra tekrar dinlenmesi yeni bir dinleme olarak kabul edilmeyebilir. Nitekim konuşmayla eş zamanlı, canlı dinlemenin gerçekleşmemiş olduğu söylenebilir, Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 45.

⁶⁹⁷ Şen, **a.g.e.**, s. 84; Şahin, **a.g.e.**, s. 264; Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 45.

⁶⁹⁸ Şahin, **a.g.e.**, s. 264; Kaymaz, **a.g.e.**, s. 111, 112.

⁶⁹⁹ **A.e.**

⁷⁰⁰ TİB Yönetmeliği m. 3/h; İletişimin Denetlenmesi Yönetmeliği m. 4/e.

bulunmaktadır.⁷⁰¹ Bu bağlamda, iletişimi kayda almaya yetkili kişinin duyduğu konuşmayı teknik araç olmadan el yazısıyla veya şekille kayda alması bu kapsamda kabul edilmeyebilecektir.⁷⁰²

Sadece telefonla yapılan konuşmalardaki ses veya görüntünün kaydedilmesi değil, faks ile yapılan haberleşmeler, internet üzerinden yapılan konuşmalardaki ses veya görüntü ve email yoluyla gerçekleşen iletişimin içeriği açısından da iletişimin kayda alınması söz konusu olabilir.⁷⁰³ İletişimin kaydedilmesi, telefon dışındaki diğer telekomünikasyon araçlarıyla gerçekleşen iletişimin denetimi açısından önem arz eder. Nitekim iletim anında faksın ele geçirilmesi, kaydetme olarak kabul edilebileceği gibi, internet üzerinden gönderilen anında mesaj ya da email gibi hizmet tipi şeklindeki verilerin elde edilmesi, anında elde etme şeklinde gerçekleşir. Zira bu verilerin elde edilmesi, verinin iletişim sürecindeki akışına engel olunmadan birer kopyasının üretilmesi şeklinde gerçekleştiğinden iletişimin kaydedilmesi şeklindeki denetim türünün kapsamında kabul edilebilir.⁷⁰⁴ Bu nedenle bu şekildeki ilgili tarafından henüz bilgisayarına depolanmamış, kaydedilmemiş, ileti halindeki email veya mesaj gibi bilgilerin, iletişim içerikli veri olarak kabul edilerek; geçmişe yönelik iletişimin denetlenmesi kararı çıkarılmasına olanak sağlaması gerektiği ifade edilmektedir.

Burada, iletişimin denetlenmesi açısından, ileriye veya geriye dönük bir denetim ayrımına gidilmediği hususundan hareketle böyle bir değerlendirme yapılmasının düşünülebileceği ileri sürülmektedir.⁷⁰⁵ Fakat bu görüşe tam da bu noktadan katılmamaktayız. İleriye veya geriye dönük bir denetim ayrımına gidilmemiş olsa da, uygulamada internet üzerinden gerçekleşen iletişimin denetlenmesi, telefon dinleme gibi değerlendirildiğinden, aslında geçmişe yönelik bir denetim kararının verilmesi

⁷⁰¹ Şahin, **a.g.e.**, s. 264; Şen, **a.g.e.**, s. 84; Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 45.

⁷⁰² Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 45.

⁷⁰³ Şahin, **a.g.e.**, s. 264.

⁷⁰⁴ Keskin, **a.g.m.**, s. 172, 173.

⁷⁰⁵ Adli amaçlı denetimle ilgili olmak üzere, bilgisayardaki iletişim içerikli bu verinin depolanması durumunda ise, CMK'nın 134. maddesinde öngörülen koruma tedbirinden yola çıkarak; bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına karar verilebileceği de ileri sürülmüştür, Şen, **a.g.e.**, s. 210.

zaten söz konusu olamayacaktır. Kaldı ki, geçmişe yönelik denetim kararı, iletişim içeriklerinin önceden depolanmasını gerektirerek; özel yaşamın gizliliği hakkını zedeleyecek ve hakkın kullanılmasını imkansız hale getirecek bir anlayışı da beraberinde getirebilir.

5. Sinyal Bilgilerinin Değerlendirilmesi

Bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veri sinyal bilgisi olarak nitelendirilebilir.⁷⁰⁶ İletişimin içeriğine müdahale etmeyerek, yetkili makamdan alınan karar kapsamında bu sinyal bilgilerinin iletişim sistemleri üzerinde bıraktığı izlerin tespit edilerek, bunlardan anlamlandırılan sonuçlar çıkarmak üzere gerçekleştirilen değerlendirme işlemleri ise sinyal bilgilerinin değerlendirilmesi olarak değerlendirilmektedir.⁷⁰⁷

Sinyal bilgilerinin değerlendirilmesi ile iletişimin tespiti tedbiri kavramlarının özellikle CMK'nın 135. maddesi bağlamında belirsizlik yaratacak şekilde içiçe geçtiği ileri sürülmüştür.⁷⁰⁸ Kanımızca sinyal bilgilerinin değerlendirilmesi işlemi göz önünde bulundurulduğunda, sadece adli amaçlı denetim değil, önleme amaçlı denetim açısından da iki kavram arasındaki aynı belirsizlikten söz edilebilir. Nitekim sinyal bilgilerinin değerlendirilmesi, özellikle İletişimin Denetlenmesi Yönetmeliği dikkate alındığında, elektrik sinyallerinden oluşan verinin telekomünikasyon sistemi üzerinde bıraktığı izlerin anlamlandırılan sonuçlar haline getirilmesi olarak karşımıza çıkmaktadır. Bu iletişim sistemi içerisinde ilk kullanıcı ile diğer kullanıcı arasında kurulan iletişimin belirlenmesi ise zaten "iletişimin tespiti" olarak belirmektedir.⁷⁰⁹

⁷⁰⁶ TİB Yönetmeliği m. 3/p; İletişimin Denetlenmesi Yönetmeliği m. 4/h.

⁷⁰⁷ İletişimin Denetlenmesi Yönetmeliği m. 4/1.

⁷⁰⁸ Özbek ve diğerleri, **a.g.e.**, s. 400; Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 47.

⁷⁰⁹ Bu yönüyle sinyal bilgilerinin değerlendirilmesinin sadece iletişimin tespiti ile değil, mobil telefonun yerinin tespiti ile de içiçe geçmiş olduğu ve açıklığa kavuşturulması gerektiği ileri sürülmektedir. Nitekim elektrik sinyalleri şeklindeki verinin, telekomünikasyon sistemi içerisinde en son kullanıcısının belirlenmesi de aslında mobil telefonun yerinin tespitini de oluşturmaktadır, Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 47.

Gerek sinyal bilgilerinin değerlendirilmesi gerek iletişimin dinlenmesi ve kayda alınması tedbirleri hakkında daha anlaşılır bir çerçeve çizmesi açısından, telefon görüşmeleri ile bağlantı kurularak açıklama yapılabilir. Buna göre, telefon görüşmelerinin içeriklerinin elde edilmesi daha önce açıklanan iletişimin dinlenmesi ve kayda alınması tedbirlerini ilgilendirmektedir. Telefon görüşmelerinin konumuz bakımından diğer boyutunu ise faturalandırma bilgisi oluşturmaktadır. Faturalama bilgisinin genel itibarıyla hizmeti sunan telefon şirketinin bu hizmet karşılığı alacağı ücrete temel teşkil edecek bilgileri ifade ettiği kabul edilir. Nitekim AİHM de faturalama bilgilerini, bir kişinin telefonla aradığı numaraların neler olduğu ve ne zaman aradığına ilişkin telefon kayıt bilgilerinin elde edilmesi olarak görmektedir.⁷¹⁰ Bu bağlamda, iletişimin içeriğini veya aramayı kimin yaptığı ve arananın da kim olduğunu kapsayan bir bilgi olmadığı değerlendirilmiştir.⁷¹¹

Telefonla sağlanan bu iletişim şeklinde GSM (Global System for Mobile Communications/Mobil İletişim İçin Küresel Sistem) firmalarının ülke genelinde kurmuş oldukları baz istasyonu kapsamındaki kişi, telefonunun baz istasyonuna düzenli olarak gönderdiği sinyalle baz istasyonunun verdiği iletişimini sağlamaktadır. Bir başka anlatımla, baz istasyonu ile sinyal alışverişi sağlanarak iletişim gerçekleşmektedir. Bu sinyal bilgileri de telefon numarası, telefon seri numarası, görüşmenin olduğu yer bilgisi ve aranan kişiyle ilgili bu yöndeki bilgileri içermektedir. Bu bilgiler de fatura bilgisine çevrilerek firma tarafından saklanmaktadır.⁷¹² Telefon kayıt bilgileri olarak gerektiğinde yararlanılabilecek bu bilgiler mesaj ve ses bilgisi gibi içerik bilgilerini kapsamamaktadır. Sinyal bilgisi gerek haberleşmenin iletimi gerek faturalama amacıyla işlenen her türlü veriyi ifade ettiğinden, görülüyor ki, bu gibi fatura bilgisi de sinyal bilgisini oluşturmaktadır. Sinyal bilgilerinin değerlendirilmesiyle de, ilgili kişiler hakkında adeta geriye dönük bir incelemeyle bilgiye ulaşılmaya çalışılmaktadır.⁷¹³

⁷¹⁰ Case of P.G. and J.H. v. The United Kingdom, para 42-51.

⁷¹¹ Case of P.G. and J.H. v. The United Kingdom, para 46.

⁷¹² Şahin, a.g.e., s. 264, 265.

⁷¹³ Şahin, a.g.e., s. 265.

E. A.B.D. Hukukundaki İletişimin Denetlenmesi Tedbirlerinin Türk Hukukuyla Paralellik Kurularak Genel Olarak Değerlendirilmesi

1. Genel Olarak

Hukukumuzda telekomünikasyon yoluyla yapılan iletişim; A.B.D. hukukunda tel aracılığıyla yapılan iletişim ve elektronik iletişim olarak nitelendirilmekte ve iletişimin denetlenmesine dair hukuk başlıca iki düzenleme ile şekillenmektedir: Elektronik İletişimin Gizliliği Kanunu / **Electronic Communications Privacy Act** (ECPA) ve Yabancı İstihbarat Denetimi Kanunu / **Foreign Intelligence Surveillance Act** (FISA).

2. Elektronik İletişimin Gizliliği Kanunu / The Electronic Communications Privacy Act (ECPA)

A.B.D.'de elektronik denetim hukukunu federal düzeyde düzenleyen ECPA'nın 3 yasayı içerdiği görülmektedir: the Wiretap Act / Tel ile Gerçekleştirilen İletişimin Dinlenmesine Dair Kanun, the Stored Communications Act / Depolanmış İletişime Dair Kanun (SCA) ve the Pen Register Act / Teknik Bilgileri İçeren Kayıtlara Dair Kanun.⁷¹⁴ ECPA, iletişimi 3 tür olarak düzenlemektedir: (i) tel aracılığıyla yapılan iletişim (**wire communications**), (ii) sözlü iletişim (**oral communications**) ve (iii) elektronik iletişim (**electronic communications**). Tel ile yapılan iletişim, ECPA'da, bir başlangıç noktasıyla alıcı nokta arasında bulunan tel, kablo veya bunun gibi başkaca bir bağlantının yardımıyla iletişimin aktarılması / taşınması için imkanların kullanılması yoluyla tamamen veya kısmen gerçekleştirilen işitsel transfer olarak nitelendirilmektedir.⁷¹⁵ Bu şekilde tel ile yapılan iletişim bakımından, işitsel aktarım (**aural transfer**), iletişimin herhangi bir yerinde insan sesinin var olmasını gerektirir

⁷¹⁴ ECPA ile ilgili ayrıntılı bilgi için bkz.: Patricia L. Bellia, "Surveillance Law Through Cyberlaw's Lens," **George Washington Law Review**, C.LXXII, 2003-2004, s. 1391-1396; Deirdre K. Mulligan, "Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act," **George Washington Law Review**, C.LXXII, 2003-2004.

⁷¹⁵ The Wiretap Act, 18 USCS § 2510 (1).

ve telefon teli veya başkaca kablo teli üzerinden aktarım gerçekleşmelidir. Nitekim telefon ile yapılan görüşmeler, en belirgin örnek olarak görülebilir.

ECPA’da sözlü iletişim ise, herhangi bir denetime tabi olmayacağına dair haklı beklentisi olan bir kişinin sözleri, konuşması olarak kabul edilmiştir.⁷¹⁶ Burada, arada bir araç olmadan yapılan sözlü iletişimden bahsedildiği görülebilir. Bu nedenle örneğin bir kişinin sesinin - A.B.D. hukukunda çoğunlukla “böcek (**bug**)” denilen - gizli dinleme cihazlarıyla kaydedilmesi buna örnek gösterilebilir.⁷¹⁷ Elektronik iletişim ise aynı kanunda, her türlü telsiz ve sözlü olmayan iletişimi kapsayacak şekilde düzenlenmiştir. Buna göre, elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü, yazı ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla tamamen veya kısmen iletilmesi elektronik iletişim olarak kabul edilmektedir.⁷¹⁸ Elektronik iletişimin bu bağlamda en tipik örneğini email oluşturmaktadır.⁷¹⁹

a. Tel İle Gerçekleştirilen İletişimin Dinlenmesine Dair Kanun / The Wiretap Act

The Wiretap Act, tel ile yapılan, sözlü ve elektronik iletişime müdahale edilmesini (**intercept**) düzenlemektedir. Bu müdahalenin aslında, dinlemeyi de içine alacak şekilde hukukumuzdaki denetim kavramıyla da paralellik kurulabilerek değerlendirilmesine de yol açan yönü, telli, sözlü veya elektronik iletişimin içeriğinin de elektronik, mekanik veya başkaca bir cihazla elde edilebilecek olmasıdır. Bu nedenle, bir telefon konuşmasının devam ederken dinlenmesi, bu tür müdahalenin ve Wiretap Act’in kapsadığı bir hususun tipik örneği olarak değerlendirilebilir. Nitekim iletişim sona erip de, bilgilerin kaydedilmesinden itibaren Wiretap Act uygulama

⁷¹⁶ The Wiretap Act, 18 USCS § 2510 (2).

⁷¹⁷ Türk Ceza Kanunu’nun 133. maddesinde düzenlenen kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması yönündeki düzenleme bu hususa paralel olarak değerlendirilebilir. Karşılıklı yapılan konuşmaların gizlice kaydedilmesiyle ilgili bkz.: Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 65, 66.

⁷¹⁸ The Wiretap Act, 18 USCS § 2510 (12). Ayrıca bkz.: Freiwald, **a.g.m.**, s. 15

⁷¹⁹ Solove, Schwartz, **Privacy, Information, and Technology**, s. 142.

alanı bulamayacaktır. A.B.D. hukukunda bu Kanun'a aykırılıkların beş yılı bulabilecek hapis cezasıyla cezalandırılabilceğı de hükme bağlanmıştır.⁷²⁰

İletişimi dinlemek için öncelikle hakimden karar almak üzere başvuruda bulunulması gerekmektedir. Bu başvuruda, bir suç işlendiğı veya işlenmek üzere olduğuna dair başvuru yapan görevlinin bunu haklı çıkarabilecek ayrıntıların; iletişimin dinleneceğı yere ilişkin spesifik belirlemelerin, iletişim türünün ve iletişimin ne kadar süreyle dinleneceğine dair bilginin bulunması gerekmektedir. Hakim, kararını vermek için ise, muhtemel / olası bir neden (**probable cause**) bulmalıdır.⁷²¹ Bu kavram, A.B.D. hukukunda muhtemel / olası nedeni ifade etmektedir. Türk hukukunda ise bu husus, başlangıç şüphesinden yoğun, olayın özelliklerinin dikkate alındığı ve somut bulgularla da desteklenmiş nitelikte bir muhtemel / olası nedeni ifade etmektedir. Ayrıca, mahkeme iletişimin dinlenmesine alternatif olabilecek tedbirlere başvurulduğunu ve bunların başarısızlıkla sonuçlandığını veya sonuçlanmak üzere olduğunu ya da bunlara başvurmanın tehlikeli olduğunu da inceleyecektir.⁷²² İletişimin dinlenmesi kararı 30 gün için verilir ve yenilenebilir.⁷²³ İletişimin dinlenmesi için hakim kararına başvurabilecek yetkili mercii, Başsavcı veya başkaca federal düzeyde yetkili bir görevli olmalıdır. Wiretap Act, ayrıca, bu denetimin uygulanabilmesi için belirli bir suç listesi de öngörmüştür.⁷²⁴

A.B.D. hukukunda telefon dinlemeler bakımından, “daraltma / **minimization**” denilen bir usulle; denetime ilişkin ilk defa verilen hakim kararında ve yenilemelerde, böyle bir karar olmasaydı denetime maruz kalmayacak olan iletişimlerin varlığı halinde, denetimin durdurulacağına dair bir hükmün olması kabul edilmiştir.⁷²⁵ Bu usule göre, örneğin, bir kişinin evindeki sabit telefonu yasadışı kumar ile ilgili bir olay nedeniyle dinleniyorsa; bu kişinin kız kardeşinin aynı hat üzerinden bir arkadaşıyla sinemaya gitmek üzere yaptığı konuşması olduğunda

⁷²⁰ The Wiretap Act, 18 USCS § 2511 (4/a).

⁷²¹ The Wiretap Act, 18 USCS § 2518 (1-4).

⁷²² Solove, Schwartz, **Privacy, Information, and Technology**, s. 143.

⁷²³ The Wiretap Act, 18 USCS § 2518 (5).

⁷²⁴ The Wiretap Act, 18 USCS § 2518 (7/a).

⁷²⁵ The Wiretap Act, 18 USCS § 2518 (5).

dinlemenin durdurulması gerekmektedir.⁷²⁶ Türk hukukunda bu usulün ne derece uygulanabileceği belirsizdir. Zira uygulamada telefon dinlemeleri bakımından dahi, canlı dinleme yerine, dinlemeyi kaydeden bir cihazla iletişimin denetlenmesinin yapıldığı yaygın olarak dile getirilmektedir.

b. Depolanmış İletişime Dair Kanun / The Stored Communications Act (SCA)

İletişim devam ederken yapılan müdahale, Wiretap Act ile korunurken; depolanmış iletişim kayıtlarının Stored Communications Act ile düzenlendiği görülmektedir. Burada elektronik depolama (**electronic storage**) söz konusudur. Buna göre, elektronik iletme bağlı telli veya elektronik iletişimin geçici depolanması, elektronik depolama olarak öngörülmüştür.⁷²⁷ SCA, aynı zamanda elektronik iletişimin servis sağlayıcıları tarafından internet hizmeti gibi modern iletişimin değişik formlarıyla birlikte, servis sağlayıcılarının, iletişimi veya abone kayıtlarını saklayabilme imkanlarını da göz önünde bulundurarak; bu tür iletişim içeriklerinin servis sağlayıcıları tarafından açıklanmasını da yasaklamaktadır.⁷²⁸ SCA'nın ihlali de, para veya hapis cezası ile cezalandırılmaktadır.⁷²⁹

SCA her yönüyle, hukukumuzdaki iletişimin denetlenmesi tedbirleriyle paralellik göstermemektedir. Bu yasal düzenleme çerçevesinde elde edilmek istenen iki tür bilgi ve böylece tedbir bulunmaktadır: depolanmış iletişim (içeriği) ve elektronik hizmeti kullanan kişinin adresi ve telefon numarası gibi iletişimin içeriğiyle ilgili olmayan bilginin elde edilmesi. Türk hukukundaki iletişimin kaydedilmesi veya tespiti tedbirleriyle paralellik kurulması akla gelebilir. Fakat burada aslında, kolluk görevlisinin elektronik hizmet sağlayıcısından isteyeceği ilk bilgi türü olan depolanmış iletişim bakımından, devam eden bir iletişim olmadığı ve böylece iletişimin denetlenmesi ve ayrıca bu denetim türlerinden biri olan iletişimin

⁷²⁶ Solove, Schwartz, **Privacy, Information, and Technology**, s. 143.

⁷²⁷ The Stored Communications Act, 18 USCS § 2510 (17/a).

⁷²⁸ The Stored Communications Act, 18 USCS § 2702 (a).

⁷²⁹ The Stored Communications Act, 18 USCS § 2701 (b).

kaydedilmesi bulunmamaktadır.⁷³⁰ Elde edilmek istenen ikinci bilgi türü olan kullanıcıya (örneğin internet hizmetini kullanan kişiye) ait adres, telefon numarası gibi bilgiler ise, iletişimin içeriğine ait değildir. Bu yönüyle bu bilgilerin denetimi bakımından, iletişimin içeriğine müdahaleyi öngörmeyen iletişimin tespitiyle paralellik kurulabileceği düşünülebilir.

Eğer kullanıcıya ait 180 veya daha az gündür saklanmış, iletişimin içeriğine dair bir bilgi söz konusu ise, kuvvetli şüphenin aranması ve hakim kararının temin edilmesi gereklidir.⁷³¹ 180 günden fazla saklanmış bilgi için, abone önceden haberdar edilir ve yetkili merciin yazılı emri yeterli olabilecektir. Fakat bu durumda abone önceden haberdar edilmezse, hakim kararı aranacaktır. İletişimin içeriği olmadan, ilgilinin adresi ve telefon numarası gibi bilgilerin elde edilmesi için de yetkili merciin yazılı emri; eğer bu bilgiler açıklanacaksa hakim kararı gerekmektedir.⁷³²

c. Teknik Bilgileri İçeren Kayıtlara Dair Kanun / The Pen Register Act

A.B.D. hukukunda hakim kararı olmadan, telle yapılan iletişimden veya elektronik iletişimden edinilen iletişim bilgilerinin kaydedilmesine yarayan araç (**pen register**) ve bu iletişim sistemi içerisinde sinyal bilgilerinin izlenilmesine yarayan araç (**trap and trace**) kullanılması yasaklanmıştır. Özellikle telefonla yapılan görüşmeler açısından, aranan telefon numaralarının elde edilmesi ilk akla gelen örnek olsa da, the Pen Register Act'in, **pen register** kavramını daha geniş tanımladığı görülür. Buna göre, tel ile yapılan iletişim veya elektronik iletişim yoluyla aktarılan; aramaya, arama güzergahına, aranan numaraya ve sinyal bilgilerine dair iletişim bilgilerini

⁷³⁰ TCK'nın bilgisayarlar, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma ile paralellik kurulması düşünülebilir. Fakat A.B.D. hukukundaki SCA'nın düzenlediği durumda, bilgisayardaki mevcut veriye elkoyma değil, elektronik hizmet sağlayıcıdan saklanmış iletişim bilgileri istenmektedir. Bu nedenle, bu yönüyle de farklı olduğu söylenebilir.

⁷³¹ The Stored Communications Act, 18 USCS § 2703 (a).

⁷³² The Stored Communications Act, 18 USCS § 2703 (c).

kaydetmeye veya çözmeye yarayan araç, **pen register** olarak kabul edilmektedir.⁷³³ Kaydedilen bilgi, iletişimin içeriğine dair bir bilgi teşkil etmemektedir.⁷³⁴ **Pen register** aracılığıyla iletişim bilgilerini kaydetmenin, örneğin Wiretap Act bağlamında dinlenen iletişimin içeriğinin de kaydedilmesi tedbiriyle arasındaki en önemli farkı burada ortaya çıkmaktadır.

Bu durumda bir kişinin aradığı telefon numaralarını kaydetmeye yarayan araç **pen register**; bunun tersi, bir kişiyi arayan numaraları kaydetmeye yarayan araç da **trap and trace** olarak ifade edilebilir. Bu araçların kullanılabilmesi için, hakimden 60 günü geçmeyecek şekilde karar alınması gerekmektedir.⁷³⁵

Görülüyor ki, pen register ile iletişim bilgilerinin kaydedilmesi, Türk hukukunda iletişimin tespiti tedbirine yakın olarak görülebilir. Nitekim iletişimin tespiti, iletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemler olarak kabul edilmektedir.⁷³⁶ **Pen register** ve **trap and trace** araçlarıyla yapılan da, tam da bu noktada sadece telefon numaraları ile sınırlı kalmayan ve diğer bilgilerin de elde edilmesine yarayan işlemler olmakla birlikte; iletişimin içeriğinin elde edilmesini de kapsamamaktadır.

3. Yabancı İstihbarat Denetimi Kanunu / The Foreign Intelligence Surveillance Act (FISA)

FISA, A.B.D. içinde yabancı istihbarat toplamak için iletişimin denetlenmesinin kullanılabilmesi için standart ve ilkeleri belirleyen bir yasa olarak ortaya çıkmaktadır. FISA bu yönüyle ECPA'dan farklı bir hukuki rejimi düzenlemektedir denilebilir. ECPA, A.B.D. içinde iletişimin adli amaçlı denetimi açısından ilke ve

⁷³³ The Pen Register Act, 18 USCS § 3127 (3). Türk hukukunda da, bu yolla elde edilen bilgilere, kimi zaman, teknik bilgileri içeren kayıtlar denildiği de görülmektedir, Kunter/Yenisey/Nuhoğlu, **a.g.e.**, s. 45, 18. dipnot.

⁷³⁴ The Pen Register Act, 18 USCS § 3127 (3).

⁷³⁵ The Pen Register Act, 18 USCS § 3123 (c).

⁷³⁶ TİB Yönetmeliği, m. 3/i; İletişimin Denetlenmesi Yönetmeliği m. 4/f.

usulleri düzenlerken; FISA, öncelikle istihbarat toplayan birimler için düzenlenmiş, yabancı devletler ve A.B.D.'de bulunan yabancı devletlerin istihbarat birimleri hakkında genel istihbarat toplamaya dair kurallar içermektedir. ECPA ise, ulusal hukuk bağlamında A.B.D.'de bulunan kişilerle ilgili ceza soruşturma ve kovuşturmalara dair bilgi toplamaya dair usul ve esasları düzenlemeyi amaçlamaktadır.

Türk hukukunda iletişimin denetlenmesi ile paralellik kurulması gerekirse, ECPA, hukukumuzda adli amaçlı iletişimin denetlenmesini düzenleyen, CMK'daki hükümler gibi değerlendirilebilir. FISA ile ise, hukukumuzda iletişimin önleme amaçlı denetimini düzenleyen 5397 sayılı Kanun arasında tam olarak paralellik kurulması çok da mümkün görünmemektedir. Nitekim FISA, yabancı güçler veya bu güçlere ait istihbarat birimleri hakkında iletişimin denetlenmesine başvurmayı düzenlemektedir. Fakat bununla birlikte, genel ilkeler itibariyle, iletişimin önleme amaçlı denetimine dair mevzuat ile benzerlikler gösterdiği de söylenebilir. FISA bağlamında hakim kararı alabilmek için federal düzeyde özel yetkili mahkemeye başvurulması gerekmektedir.⁷³⁷ Adalet Bakanlığı, CIA⁷³⁸ veya başka istihbarat birimleri adına başvurusunu yapar. Üye sayısı 7'den 11'e yükseltlen Mahkeme,⁷³⁹ gizli oturumla kararını verir ve bu usuli işlemler çoğunlukla kamuya veya iletişimi denetlenen kişiye açıklanmaz.⁷⁴⁰

FISA bağlamında iletişimin denetlenmesinde, muhtemel / olası nedenin bulunması aranır. Burada aranan, iletişimi denetlenen tarafın ilgili faaliyeti gerçekleştirmesi bakımından muhtemel / olası nedenin olması değil; iletişimi denetlenen tarafın yabancı devlet veya temsilcisi olması bakımından makul nedenin olup olmadığıdır. Burada mutlaka cezai bir faaliyetle bağlantının gösterilmesi aranmamaktadır.⁷⁴¹ Fakat bir A.B.D. vatandaşının iletişimi denetleniyorsa, kişinin suç işleme ihtimalinin olduğuna dair muhtemel / olası nedenin bulunması zorunluluğu geçerlidir. 2001

⁷³⁷ 50 USCS § 1804 (a).

⁷³⁸ Central Intelligence Agency, USA, (Çevrimiçi) <https://www.cia.gov/>, 29 Ocak 2012.

⁷³⁹ 50 USCS § 1803 (a).

⁷⁴⁰ Solove, Schwartz, **Privacy, Information, and Technology**, s. 201.

⁷⁴¹ Solove, Schwartz, **Privacy, Information, and Technology**, s. 201.

tarihinde, mahkeme tarafından reddedilen hiçbir denetim izni başvurusu olmamış ve böylece 934 başvuru onaylanmıştır.⁷⁴² 2001 tarihli USA Patriot Act'in A.B.D.'deki terörle mücadele anlayışındaki değişikliklerle de paralel olarak,⁷⁴³ iletişimin denetlenmesine ilişkin koşulları da kolaylaştırmasıyla bu sayıda artışın olduğu ve 2002'de 1.228; 2003'de 4'ünün reddedildiği, 1.727 ve 2004 yılında da, 1.758 başvurunun yapıldığı görülmektedir. Böylece 2001 yılından itibaren yüzde 88'lik bir artışın olduğu ifade edilmektedir.⁷⁴⁴

Taraflarından birinin A.B.D. vatandaşı olduğu bir iletişim içeriği elde edilmeyecekse ve sadece yabancı devletlerden istihbarat elde etmek amacıyla iletişimin denetlenmesi için hakim kararına gerek olmamaktadır. Bu durumda, Devlet Başkanı'nın yetkilendirmesiyle Başsavcı'dan yazılı bir talep gerekmektedir.⁷⁴⁵

11 Eylül saldırısından sonra, özellikle yurtdışından gelen telefonların hakim kararı olmadan dinlenmesindeki artışa yönelik tepkilerden sonra, 1978 tarihli Yabancı İstihbarat Denetimi Hakkında Kanunda Değişiklik Yapan 2008 tarihli Kanun (Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 / FAA)⁷⁴⁶ ile FISA'da birçok değişiklik yapıldı. Örneğin, FAA, yabancı istihbarat bilgisi elde etmek için, hakkında A.B.D. dışında olduğuna dair makul bir inancın olduğu kişinin iletişiminin denetlenmesine izin vermektedir. Bu kişi A.B.D. vatandaşı olmamalıdır.⁷⁴⁷ Burada önemli olan iki husus, iletişimin denetlenmesinin esaslı nedeninin yabancı istihbarat toplamak olması ve iletişimi denetlenen esas kişinin de ülke dışında olması gerektiğidir.⁷⁴⁸ Nitekim hakkında bilgi toplanan esas kişinin de A.B.D. dışında bulunması gerekmektedir. FAA ile ayrıca birtakım yeni daraltma

⁷⁴² Office of Attorney General, 2001 Annual FISA Report to Congress, Aktaran Solove, Schwartz, **Privacy, Information, and Technology**, s. 201.

⁷⁴³ Clayton Northouse, "Providing Security and Protecting Liberty", **Protecting What Matters: Technology, Security, and Liberty since 9/11**, Ed. by. Clayton Northouse, Washington, D.C., Brookings Institution, 2006, s. 14-17.

⁷⁴⁴ Solove, Schwartz, **Privacy, Information, and Technology**, s. 201.

⁷⁴⁵ 50 USCS § 1802 (a, b).

⁷⁴⁶ Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 10 Temmuz 2008, 50 USCS § 1801.

⁷⁴⁷ 50 USCS § 1801, section 702 (a, b); 703.

⁷⁴⁸ A.B.D.'de bulunan biriyle, A.B.D. dışından birinin telefon konuşmasının dinlenmesi bu duruma örnek olarak gösterilebilir.

usulleri de öngörülmüştür. Buna göre, Adalet Bakanlığı'nın ve Ulusal İstihbarat Direktörü'nün denetim faaliyetinin, iletişimi denetlenmesi amaçlanan esas kişinin kim olması gerektiği ile ilgili daraltma usullerine dair kurallara uyulduğunu ve denetimin esaslı amacının yabancı istihbarat elde etmek olduğunu önceden onaylamaları gerekmektedir.⁷⁴⁹ Gerekli koşullar sağlanmadan yapılacak bir iletişimin denetlenmesi olduğuna veya Adalet Bakanlığı'nın ve Ulusal İstihbarat Direktörü'nün onayının gerekli şartları taşımadığına hakim tarafından karar verilirse, tedbir başlatılmaz; başlamışsa durdurulur ve Devletin zararı tazmin etmesi gerekir.⁷⁵⁰

II. TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN ÖNLEME AMAÇLI DENETLENMESİNİN KOŞULLARI VE UYGULANMASI

A. İletişimin Önleme Amaçlı Denetlenmesinin Koşulları

1. Genel Olarak

CMK'nın 135. maddesi bağlamında iletişimin adli amaçlı denetiminin koşulları, tedbirin türlerine göre değişebilirken; iletişimin önleme amaçlı denetimi açısından koşullar, tüm denetim tedbirleri için uygulanabilecek şekildedir. Örneğin, iletişimin tespiti ve mobil telefonun yerinin tespiti açısından katalog suç aranmamakta⁷⁵¹ ve mobil telefonun yerinin tespitinin sadece şüpheli veya sanığın yakalanabilmesi için uygulanabildiği görülmektedir.⁷⁵² Önleme amaçlı denetimin koşulları açısından ise uygulanacak tedbire göre suçlar arasında bir ayrımın bulunmadığı ifade edilebilir.

⁷⁴⁹ 50 USCS § 1801, section 702 (g).

⁷⁵⁰ 50 USCS § 1801, section 702 (i/3-b).

⁷⁵¹ CMK m. 135/6; Özbek ve diğerleri, **a.g.e.**, s. 402.

⁷⁵² CMK m. 135/4.

2. Tedbirin Uygulanacağı Kişiler

İletişimin önleme amaçlı denetlenmesi tedbirinde, tedbirin uygulanacağı kişiler açısından değil, önlenmesi amaçlanan suçlar açısından bir düzenlemenin getirildiği görülmektedir.⁷⁵³ Kaldı ki, CMK'nın 135. maddesi kapsamındaki adli amaçlı denetimde olduğu gibi, iletişimin denetimi için bir suç dolayısıyla başlamış bir soruşturma ve kovuşturma da bulunmadığından, ortada iletişimi denetlenecek bir şüpheli veya sanık da bulunmamaktadır. Ayrıca adli amaçlı denetim tedbirinde, bazen tedbirin niteliğinden kaynaklanan bazı engellemeler bulunabilmektedir. Örneğin, adli amaçlı denetimin yasama dokunulmazlığından yararlanan yasama üyeleri için kovuşturma aşamasında uygulanabilmesi için, kural olarak yasama dokunulmazlığının kalkması⁷⁵⁴ ve bunun için Meclis'in kararı gerekmektedir. Oysa önleme amaçlı denetimde böyle bir kovuşturma veya soruşturmaya da gerek olmadığından, buna benzer bir sürecin de yaşanmaması ve gerekli şartları sağlayarak neredeyse herkesin böyle bir denetime maruz kalabilmesi söz konusu olabilir. Aslında sadece bu açıdan bakıldığında dahi mevcut düzenleme, suçların önlenmesi amacıyla neredeyse suç işleme ihtimali olan herkesin iletişiminin denetlenebileceği değerlendirmesini mümkün kıldığından dolayı eleştirilebilir.

Kullanılan iletişim aracının kime ait olduğunun bir önemi bulunmamaktadır. Kaldı ki, adli amaçlı denetimde olduğu gibi, şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişiminin kayda alınamayacağına dair⁷⁵⁵ ya da şüpheli veya

⁷⁵³ 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 6. maddesi.

⁷⁵⁴ Yasama dokunulmazlığı ile ilgili ayrıntılı bilgi için bkz: Hüseyin Özcan, **Yasama Bağımsızlıkları**, Ankara, Seçkin, 2006, s. 179-193. Ayrıca bkz: 1982 Anayasası m. 83/2, 3. Tanör, Yüzbaşıoğlu, **a.g.e.**, s. 244-250.

⁷⁵⁵ CMK'nın 135. maddesinin ikinci fıkrasına göre, “şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda alınamaz. Kayda alma gerçekleşikten sonra bu durumun anlaşılmaması hâlinde, alınan kayıtlar derhâl yok edilir.” Madde ifadesinde sadece kayda alma kavramı kullanıldığından, burada iletişimin dinlenip dinlenemeyeceği tartışmalıdır. Kunter/Yenisey/Nuhoğlu, yasağın sadece kayda almaya ilişkin olduğunu ve bu nedenle tanıklıktan çekinebilecek bu kişilerle olan konuşmaların dinlenebileceğini ileri sürmektedir, Kunter/Yenisey/Nuhoğlu, **a.g.e.**, s. 43. Şahin de şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle olan iletişiminin dinlenebileceğini, tespit edilebileceğini ve sinyal bilgilerinin değerlendirilebileceğini kabul etmektedir, Şahin, **a.g.e.**, s. 270. Şen ise, tanıklıktan çekinebilecek olacak kişiler kendilerine ait telekomünikasyon araçlarıyla şüpheli veya sanıkla iletişim kuruyorlarsa, bu iletişimlerinin tespit ve dinleme işlemleri bakımından

sanıkla müdafii arasındaki iletişimin denetimine getirilen yasak⁷⁵⁶ önleme amaçlı denetim bakımından söz konusu değildir. Böylece müdafiiyle veya tanıklıktan çekinme hakkına sahip örneğin eşle de gerçekleşen iletişim önleme amaçlı denetlenebilecektir.⁷⁵⁷

3. İletişimin Önleme Amaçlı Denetlenmesi Tedbirinin Uygulanmasıyla Önlenmesi Amaçlanan Suçlar

a. Polis ve Jandarma Bakımından

2559 sayılı PYSK'nın ek 7. maddesi ve 2803 sayılı Jandarma Kanunu'nun ek 5. maddesi, casusluk suçları hariç, CMK'nın 250. maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla iletişimin denetlenebileceğini hükme bağlamıştır. Bu suçlar ise, TCK'da yer alan örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imal ve ticareti suçu veya suçtan kaynaklanan malvarlığı değerini aklama suçu, haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar ile ikinci kitap dördüncü kısmının dört, beş, altı ve yedinci bölümünde tanımlanan suçlar (305, 318, 319, 323, 324, 325 ve 332. maddeler hariç) olarak ifade edilebilir.

Hükümde geçen ilk suç, örgüt faaliyeti çerçevesinde işlenen uyuşturucu veya uyarıcı madde imal ve ticareti suçu olarak karşımıza çıkmaktadır. Görülüyor ki, kişisel olarak uyuşturucu imal veya ticaret suçu işlemesi öngörülen kişiyle ilgili olarak iletişimin önleme amaçlı denetlenmesine başvurulamayacaktır. Bu suçun örgüt faaliyeti çerçevesinde işlenmesi açısından, örgütün şiddete başvurarak bir faaliyet

sınırlandırılması gerektiğini; kendilerine ait olmayan telekomünikasyon araçlarıyla yaptıkları görüşmeler açısından ise durumun anlaşılmasından itibaren dinleme ve tespit işlemine son verilmesi gerektiğini belirtmektedir, Şen, a.g.e., s. 162.

⁷⁵⁶ CMK'nın 136. maddesi şüpheli veya sanığa yüklenen suç dolayısıyla müdafinin bürosu, konutu ve yerleşim yerindeki telekomünikasyon araçları hakkında, iletişimin dinlenmesi, tespiti ve kayda alınmasına dair 135. madde hükmünün uygulanamayacağını hükme bağlamaktadır.

⁷⁵⁷ Özbek ve diğerleri, a.g.e., s. 403.

göstermesi aranmamaktadır. Sahip olunan üye sayısı ile araç ve gereç bakımından örgütün yapısı TCK'da, amaç suçları işlemeye elverişli ve üye sayısının en az üç kişi olması ile nitelendirilmiştir.⁷⁵⁸ Burada suçlar açısından herhangi bir ayırım yapılmamış; herhangi bir suçun işlenmesi için örgüt kurulması ile suç işlemek amacıyla kurulmuş örgüte üye olunması⁷⁵⁹ ve örgütün yöneticisi olunması⁷⁶⁰ suç olarak kabul edilmiştir. Önlenmesi amaçlanan suç, örgüt faaliyeti çerçevesinde işlenen uyuşturucu veya uyarıcı madde imal ve ticareti suçudur.⁷⁶¹ Bu nedenle örneğin, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma suçu⁷⁶² bakımından iletişimin önleme amaçlı denetiminin uygulanmayacağı söylenebilir.

Haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar da, iletişimin denetlenmesiyle önlenmesi amaçlanan suçlar arasında yer almaktadır. Burada çıkar amaçlı suç örgütüne değinilmesi gerekmektedir. Çıkar amaçlı suç örgütü, mülga 4422 sayılı ÇASÖMK'da tanımlanmaktaydı. Buna göre, “doğrudan veya dolaylı biçimde bir kurumun, kuruluşun veya teşebbüsün yönetim ve denetimini ele geçirmek, kamu hizmetlerinde, basın ve yayın kuruluşları üzerinde, ihale, imtiyaz ve ruhsat işlemlerinde nüfuz ve denetim elde etmek, ekonomik faaliyetlerde kartel ve tröst yaratmak, madde ve eşyanın azalmasını ve darlığını, fiyatların düşmesini veya artmasını temin etmek, kendilerine veya başkalarına haksız çıkar sağlamak, seçimlerde oy elde etmek veya seçimleri engellemek maksadıyla zor veya tehdit uygulamak veya kişileri kendilerine tabi kılmaya zorlamak veya mensupları arasında her ne suretle olursa olsun açık veya gizli işbirliği yapmak suretiyle yıldırma veya korkutma veya sindirme gücünü kullanarak suç işlemek için” kurulan örgüt, çıkar amaçlı suç örgütü olarak nitelendirilmekteydi.⁷⁶³

⁷⁵⁸ 5237 sayılı 26/09/2004 tarihli Türk Ceza Kanunu'nun 220. maddesi, Resmi Gazete No. 25611, Resmi Gazete tarihi: 12/10/2004.

⁷⁵⁹ TCK m. 220/2.

⁷⁶⁰ TCK m. 220/5.

⁷⁶¹ Uyuşturucu veya uyarıcı madde imal ve ticareti suçu TCK'nın 188. maddesinde düzenlenmiştir.

⁷⁶² TCK'nın 190. maddesi uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma suçunu düzenlemektedir. Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma suçuyla ilgili ayrıntılı bilgi için bkz.: Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok, **Teorik ve Pratik Ceza Özel Hukuku**, 5. bs., Ankara, Seçkin, 2007, s. 614-618.

⁷⁶³ 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu'nun 1. maddesi.

Görülüyor ki, örgüt faaliyeti çerçevesinde işlenen uyuşturucu veya uyarıcı madde imal ve ticareti suçu bakımından örgütün şiddete başvurarak bir faaliyet göstermesi aranmazken; haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde işlenen suçların önlenmesi için iletişimin denetlenmesine karar verebilmek için, bu suçların cebir ve tehdit uygulanarak işlenmesi ihtimali bulunmalıdır.

Çıkar amaçlı suç örgütü, amaç bakımından TCK'nın 220. maddesinde söz edilen herhangi bir suç için kurulan örgütten farklılık arz etmektedir. Çıkar amaçlı suç örgütü, iştirak ilişkisinden de farklı olarak ele alınmalıdır. Nitekim gerek TCK'nın 220. maddesi gerek mülga 4422 sayılı ÇASÖMK'da örgütlü suçlar açısından, örgütü kuran, yöneten, üye olan ve adına suç işleyen şekilde birden fazla kişinin varlığı gerekmektedir. Bu bağlamda, işlenebilmesi için birden çok failin bulunmasını zorunlu kılan çok failli suçlardan biri olarak nitelendirilebilir.⁷⁶⁴ İştirak halinde işlenen suçlar açısından ise, yasal olarak ve niteliği gereği tek kişi tarafından işlenebilen bir suçun, aralarında yaptıkları anlaşma bağlamında birden fazla kişi tarafından işlenmesi söz konusudur.⁷⁶⁵

Önlenmesi amacıyla Polis veya Jandarma'nın iletişimin denetlenmesi işlemini gerçekleştirebileceği diğer suçlar ise, TCK'nın ikinci kitap dördüncü kısmının dört, beş, altı ve yedinci bölümünde tanımlanan suçlar (305, 318, 319, 323, 324, 325 ve 332 nci maddeler hariç) olarak hükme bağlanmıştır.⁷⁶⁶ Bunlar, devletin güvenliğine karşı işlenen suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, milli

⁷⁶⁴ Kayıhan İçel, A. Hakan Evik, **Ceza Hukuku Genel Hükümler 2. Kitap, Suçun Yapısal Unsurları ve Özel Görünüş Şekilleri**, 4. bs., İstanbul, Beta, 2007, s. 261; Mehmet Emin Artuk, Ahmet Gökçen, A. Caner Yenidünya, **Ceza Hukuku Genel Hükümler**, 5. bs. Ankara, Turhan, 2011, s. 625.

⁷⁶⁵ Bir fiilin iştirak halinde işlenmesi için, tek bir faille işlenebilen, nedensellik değeri taşıyan suç sayılan hareketlerin birden fazla fail tarafından yapılmış olması ve bu kişiler arasında iştirak iradesinin bulunması ve tüm suç ortakları açısından aynı olan suçun icra hareketlerine başlanmış olması aranmaktadır, Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 627; İçel, Evik, **a.g.e.**, s. 263.

⁷⁶⁶ 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi.

savunmaya karşı suçlar ve devlet sırlarına karşı suçlar ile casusluk suçları olarak belirtilebilir.⁷⁶⁷

Belirtilen suçlardan, iletişimin denetlenmesi işlemi açısından istisna tutulan suçlar bulunmaktadır. Bunlardan ilki, TCK'nın 305, 318, 319, 323, 324, 325 ve 332. maddelerinde düzenlenen suçlardır. Böylece temel milli yararlar karşı faaliyette bulunmak için yarar sağlama, halkı askerlikten soğutma, askerleri itaatsizliğe teşvik, savaşta yalan haber yayma, seferberlikle ilgili görevin ihmali, düşmandan ünvan ve benzeri payeler kabulü ve askeri yasak bölgelere girme, iletişimin önleme amaçlı denetlenmesine konu olmayacak suçlar olarak ortaya çıkmaktadır. Diğer istisnayı ise, casusluk suçlarının önlenmesi oluşturmaktadır. Bunlar ise, siyasal veya askeri casusluk,⁷⁶⁸ uluslararası casusluk,⁷⁶⁹ yasaklanan bilgilerin casusluk amacıyla temini,⁷⁷⁰ yasaklanan bilgileri siyasal veya askeri casusluk amacıyla açıklama⁷⁷¹ ve taksir sonucu casusluk fillerinin işlenmesi⁷⁷² olarak ifade edilebilir.

Polis ve jandarma tarafından iletişimin denetlenmesiyle önlenmesi amaçlanan suçlar açısından bir farklılık olmamakla birlikte, polis ve jandarmanın bu yetkilerini kullanabilecekleri görev alanı bakımından bir ayrımın mevcut olduğu söylenebilir. Nitekim jandarmanın genel olarak görev ve sorumluluk alanı, polisin görev sahası dışında olup, bu alanları il ve ilçe belediye hudutları haricinde kalan veya polis teşkilatı bulunmayan yerler oluşturmaktadır.⁷⁷³ Buna göre, polisin görev sahası

⁷⁶⁷ TCK m. 302-339.

⁷⁶⁸ Devletin güvenliği veya iç veya dış siyasal yararları bakımından, niteliği itibarıyla, gizli kalması gereken bilgileri, siyasal veya askerî casusluk amacıyla temin etme şeklinde ortaya çıkmaktadır, TCK m. 328.

⁷⁶⁹ Yabancı bir devletin güvenliği veya iç veya dış siyasal yararları bakımından niteliği itibarıyla gizli kalması gereken bilgileri, diğer bir yabancı devlet lehine siyasal veya askerî casusluk maksadıyla temin etme olarak ortaya çıkmaktadır, TCK m. 331.

⁷⁷⁰ Yetkili makamların kanun ve düzenleyici işlemlere göre açıklanmasını yasakladığı ve niteliği bakımından gizli kalması gereken bilgileri siyasal veya askerî casusluk amacıyla temin etme şeklinde görülmektedir, TCK m. 335.

⁷⁷¹ Yetkili makamların kanun ve düzenleyici işlemlere göre açıklanmasını yasakladığı ve niteliği bakımından gizli kalması gereken bilgileri, siyasal veya askerî casusluk amacıyla açıklama şeklinde ortaya çıkmaktadır, TCK m. 337.

⁷⁷² TCK m. 338.

⁷⁷³ 2803 sayılı 10/3/1983 tarihli Jandarma Teşkilat, Görev ve Yetkileri Kanunu m. 10/1, Resmi Gazete No. 17985, Resmi Gazete tarihi: 12/31983. Jandarma veya emniyet teşkilatı, kendi sorumluluk sahasında yetersiz kaldıkları veya kalacaklarının değerlendirilmesi halinde, mahalli mülki amirler

dışında ve polis teşkilatı olmayan yerlerde jandarmanın, iletişimin önleme amaçlı denetlenmesi yetkisini kullanabileceği söylenebilir. Nitekim TİB Yönetmeliği'nin 9. maddesinde 2007 yılında yapılan bir değişiklikle, 2803 sayılı Jandarma Kanunu'nun ek 5. maddesi bağlamında iletilen talepler ile verilen kararlar ve yazılı emirlerde sorumluluk alanına ilişkin bilgi ve/veya belgelere de yer verileceği hükme bağlanmıştır.⁷⁷⁴ Bu hükmün polis ile sorumluluk alanı çakışabilecek jandarma açısından taşıdığı önem, MİT'in ülke çapında faaliyet göstermesi nedeniyle⁷⁷⁵ görev ve sorumluluk alanına dair böyle bir sorunla bu şekilde karşılaşmayacağı da dikkate alınırsa açıkça görülebilir.

Dinlemeye konu olan iletişimi gerçekleştiren kişilerin bir kısmı polis, diğer kısmı jandarma bölgesinde faaliyet gösteriyor olabilir. Polisin görev ve sorumluluk alanında iletişimi dinlenen bir örgüt üyesinin, jandarma bölgesindeki örgüt üyesiyle gerçekleştirdiği iletişiminin de jandarma tarafından denetlenmesi açısından jandarmanın yetkisiz olduğu ileri sürülebilir.⁷⁷⁶ Bu nedenle, jandarma ve polisin görev ve sorumluluk alanının çakışması durumuna ilişkin açık bir yasal düzenlemenin bulunmasının yerinde olacağı düşünülebilir. Uygulamada aynı suç için hem Polis'in hem de tüm ülke genelinde yetkili MİT'in aynı olay için iletişimin denetlenmesi işlemini gerçekleştirebilmesi mümkün görülmektedir. Zira TİB açısından önemli olan iletişimi denetlemeyi talep eden ilgili birimin bunu gerçekleştirmeye yetkili olup olmadığıdır.

b. Milli İstihbarat Teşkilatı Bakımından

MİT, 2937 sayılı MİT Kanunu'nun 4. maddesinde sayılan görevlerin yerine getirilmesi amacıyla 1982 Anayasası'nın 2. maddesinde belirtilen temel niteliklere ve

tarafından birbirlerinin sorumluluk sahalarında geçici olarak görevlendirilebilirler, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu m. 10/3.

⁷⁷⁴ Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığı'nın Kuruluş, Görev ve Yetkileri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik, m. 6, Resmi Gazete No. 26572, Resmi Gazete tarihi: 4 Temmuz 2007.

⁷⁷⁵ 2937sayılı MİT Kanunu m. 4/a.

⁷⁷⁶ Taşkın, **a.g.e.**, s. 202, 203.

demokratik hukuk devletine yönelik ciddi bir tehlikenin bulunması durumunda iletişimin denetlenmesi işlemine başvuruabilecektir.⁷⁷⁷ Bu bağlamda belirlenen hususlardan ilki, MİT'in, MİT Kanunu'nun 4. maddesinde sayılan görevlerinin yerine getirilmesi amacıyla iletişimi denetleyebilmesidir. Bu görevler ise - Türkiye Cumhuriyeti'nin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilecek mevcut ve muhtemel faaliyetler hakkında milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak,

- Devletin milli güvenlik siyasetiyle ilgili planların hazırlanması ve yürütülmesinde,
- Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamak,
- kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için Milli Güvenlik Kurulu ve Başbakana tekliflerde bulunmak,
- kamu kurum ve kuruluşlarının istihbarat ve istihbarata karşı koyma faaliyetlerine teknik konularda müşavirlik yapmak ve koordinasyonun sağlanmasında yardımcı olmak,
- Genelkurmay Başkanlığınca Silahlı Kuvvetler için lüzum görülecek haber ve istihbaratı, yapılacak protokole göre Genelkurmay Başkanlığına ulaştırmak,
- Milli Güvenlik Kurulunda belirlenecek diğer görevleri yapmak ve istihbarata karşı koymaktır.⁷⁷⁸

MİT'in önleme amaçlı iletişimi denetleyebilmesi bakımından öngörülen diğer husus, 1982 Anayasası'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 böyle bir tedbire başvuruabilecektir.⁷⁷⁹

⁷⁷⁷ 2937sayılı MİT Kanunu'nun 6. maddesi.

⁷⁷⁸ 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 4. maddesi, Resmi Gazete No. 18210, Resmi Gazete tarih: 03/11/1983.

⁷⁷⁹ A.e..

4. İletişimin Önleme Amaçlı Denetlenmesi Tedbirinin Uygulanmasında Suç İşleme İhtimali

Önleme amaçlı iletişimin denetlenmesi açısından, 5397 sayılı Kanun'da ve ilgili düzenlemelerde, bir şüphe derecesine yer verilmediği görülmektedir. Böylece önleme amaçlı denetim, tedbirin uygulanacağı kişinin suçu işleme ihtimali açısından iletişimin adli amaçlı denetlenmesinden de ayrılmaktadır. Önleme amaçlı denetimde bir suç dolayısıyla yapılan soruşturma ve kovuşturma bulunmamakta ve bir şüpheden bahsedilememektedir. Adli amaçlı denetimde, bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı telekomünikasyon yoluyla yapılan iletişimin denetlenmesine imkan verecektir.⁷⁸⁰

Şu hususu belirtmemiz gerekir ki, burada da madde hükmünün uygulanabilmesi için aranan kuvvetli şüphe açısından tam bir açıklık bulunduğu söylenemez. Kısaca değinmek gerekirse, bir görüşe göre, özel yaşamın ve iletişimin gizliliği hakkını yakından ilgilendiren iletişimin adli amaçlı denetlenmesi tedbirine başvurulabilmesi açısından basit şüphe yeterli görülmemelidir ve kaldı ki, madde hükmüyle de şüphenin nitelikli bir yoğunluğa ulaşmış şekliyle kuvvetli şüphe olması beklenmektedir.⁷⁸¹ Diğer bir görüşe göre ise, aranan şüphe açısından, basit bir şüphenin yeterli olabilmesi ve fakat mülga 4422 sayılı ÇASÖMK'da ifade edildiği gibi,⁷⁸² somut, olaylara dayanan ve elle tutulur kuvvetli belirtilerin bulunması gerektiği şeklinde değerlendirilme yapılmalıdır.⁷⁸³ Bu doğrultuda, madde hükmünden basit şüpheden daha yoğun ve fakat yeterli şüphe derecesine ulaşma zorunluluğu olmayan şüphe derecesinin arandığı da ileri sürülmektedir. Burada da esas itibarıyla, genel yaşam deneyimleri veya kriminalistik tecrübelerin yeterli kabul edilmeyerek,

⁷⁸⁰ CMK m. 135/1.

⁷⁸¹ Şahin, **a.g.e.**, s. 265.

⁷⁸² 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu'nun 2. maddesinin 2. fıkrası, "iletişimin dinlenmesine veya tespitine ilişkin kararların, ancak kuvvetli belirtilerin varlığı halinde verilebileceğini" hükme bağlamaktaydı.

⁷⁸³ Bu bağlamda objektif olarak tespit edilmiş olayların yaşam tecrübesi ve kriminalistik uygulamalara dayanarak suç işlendiği kanaatini uyandırabilecek özellik taşımasının arandığı ifade edilmektedir. Böylece örneğin dedikodu, test edilmemiş tahminler kuvvetli belirti olarak görülmemiştir, Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 48, 49.

suçun işlendiğine yönelik somut olayların varlığının aranması gerektiği vurgulanmaktadır.⁷⁸⁴

Tüm bu (i) kuvvetli şüphe, (ii) kuvvetli belirtilere bağlı basit şüphe veya (iii) yeterli şüphe varlığının gerektiği değerlendirmelerinin yanı sıra, (iv) kuvvetli suç şüphesi sebeplerinin varlığının suçun işlendiğine dair değil, suçun şüpheli veya sanık tarafından işlendiğine dair kuvvetli suç şüphesi olarak anlaşılması gerektiği de ileri sürülmüştür.⁷⁸⁵ Bu bağlamda, kuvvetli delil ve emarelerin iletişimin denetlenmesine başvurulabilmesi için zorunlu şart olarak aranmasının da yerinde olmayacağı değerlendirilmiştir. Böyle bir şartın bu tedbirin uygulanmasını ve ulaşılmak istenen amaca ulaşılmasını zorlaştıracığı ve tedbire başvurulmasını anlamsız hale getireceği temel dayanak noktası olarak ifade edilmiştir. Böylece kuvvetli belirtinin aranması ve fakat zorunlu bir ön koşul olarak beklenmemesi kabul edilmektedir.⁷⁸⁶

Kanımızca CMK bağlamında iletişimin adli amaçlı denetlenmesine yönelik, tedbirin uygulanacağı şüphe derecesine dair bu değerlendirmelere kısaca değinmemizdeki yarar, iletişimin önleme amaçlı denetlenmesinin de adli amaçlı denetimde olduğu gibi, özel yaşamın gizliliği ve iletişimin gizliliği hakkına müdahaleyi yakından ilgilendirmesiyle bağlantılıdır. Aslında koşullar ve varılmak istenen amaç gibi hususlar açısından temel anlamda farklı olsalar da iki tedbir türünün de bu temel hak ve özgürlüklerle ilişkisi açıktır. İletişimin adli amaçlı denetlenmesi açısından, madde hükmünde yer alan kuvvetli şüphe sebeplerinin varlığı kavramına dair yapılan değerlendirmeler, bazı farklı unsurlara değinseler de, esas itibarıyla sadece söylenti veya duyuma dayalı bilgi veya haberleri dayanak alarak iletişimin denetlenmesi tedbirine başvurma bu özgürlükler açısından yaratacağı hukuka aykırı müdahaleyi vurgulamaktadırlar.

Benzer doğrultuda bir değerlendirme, henüz ortada işlenmiş veya belki işlenmesine teşebbüs edilmiş bir suç olmadan başvuru ile iletişimin önleme amaçlı denetlenmesi

⁷⁸⁴ Özbek ve diğerleri, **a.g.e.**, s. 402, 403; Öztürk ve diğerleri, **a.g.e.**, s. 380, 381.

⁷⁸⁵ Şen, **a.g.e.**, s. 101, 102.

⁷⁸⁶ Şen, **a.g.e.**, s. 102, 103.

açısından yapılabilir. Önleme amaçlı denetimde soruşturma veya kovuşturma evresinden bahsetmediğimiz gibi, bu denetime bu evrelerden önce ve hatta sonra başvurulabilmesi de söz konusu olduğu için şüpheli veya sanıktan da söz etmemekteyiz. Kaldı ki 5397 sayılı Kanun'da da bir şüphe derecesine rastlamamaktayız. Bu bağlamda önleme amaçlı denetim açısından, yeterli şüphe veya kuvvetli şüphe sebeplerinin aranmadığı belirtilebilir. Fakat bu yöndeki bir değerlendirme, bu tedbirin uygulanmasıyla özel yaşamın ve iletişimin gizliliği hakkının ihlali ve hukuk devleti ilkesi açısından yaratacağı etki de göz önünde bulundurulduğunda, tedbirin her durumda ve zamanda herkes için başvurulabileceği sonucuna da götürmemelidir. Nitekim 5397 sayılı Kanun bu eksikliği nedeniyle eleştirilebileceği gibi, gelen ciddi istihbari bilgi aktarımlarının olduğu ve bu nedenle ilgililerin denetlenmesine dair “muhtemel / olası bir neden yaratılan” durumlar için bu tedbire başvurulabileceği düşünülebilir. Örneğin, iletişimin denetlenmesine karar verebilmek için A.B.D. hukukunda muhtemel / olası neden⁷⁸⁷ aranmaktadır. Bu bağlamda, yetkililerin iletişimi denetleyebilmek için hakim kararına başvururken, şüphelerini haklı çıkarabilecek ayrıntıları da başvurularına eklemeleri beklenmektedir.⁷⁸⁸

Muhtemel / olası neden aranmasını ifade ederken; bir suç dolayısıyla soruşturma ve kovuşturmada olduğu gibi şüphe aranmasının gerekli olamayacağını göz önünde bulundurmaktayız. Nitekim ceza muhakemesinde şüphe delillerle tarif edilebilir⁷⁸⁹ fakat burada delil veya ceza muhakemesinde soruşturma ve kovuşturma evresinden söz etmemekteyiz. Böylece adli amaçlı denetimde olduğu gibi bir kuvvetli şüphe aranması zorunluluğundan da bahsetmemekteyiz. Nitekim A.B.D. hukukunda aranan muhtemel / olası neden kavramıyla da esas itibarıyla, suç işleme ihtimalinin makul bir şekilde değerlendirilmesi ileri sürülmektedir. Kavramın ilk ortaya atıldığında

⁷⁸⁷ Aguilar v. Texas, 378 U.S. 108, 114, 1964; State v. Hinchion 207 Neb. 478, 1980. Mevcut olaylar ve koşulların sunulması ve hakim in değerlendirmesi hassasiyetle korunmaya çalışılmaktadır. State v. Hinchion kararında Supreme Court of Nebraska, kolluk görevlilerinin telefon dinleme kararı için yaptıkları başvuruda ileri sürdükleri iddiaların suç işlenmesi ihtimali bakımından muhtemel neden oluşturup oluşturmadığını incelemiştir. Buna göre, kolluğun sadece isimli ihbara ve sadece duyuma dayalı bilgisi, dinleme kararı verilmesi için gerekli muhtemel nedeni oluşturmaya yetmeyecektir.

⁷⁸⁸ Solove, Schwartz, **Privacy, Information, and Technology**, s. 143.

⁷⁸⁹ Öztürk ve diğerleri, **a.g.e.**, s. 380.

anlaşıldığı gibi kesin ve somut güvenilir bilgi aranması anlayışından uzaklaşmıştır. İlk ortaya atıldığında, ilk kullanıldığı kararların ismiyle,⁷⁹⁰ Aguilar-Spinelli doktrini olarak anılan muhtemel / olası neden anlayışında, bilginin güvenilirliği açısından, sadece isimsiz ihbar veya duyum şeklinde değil de, ilk elden bu bilginin elde edilmiş olması aranmaktaydı.⁷⁹¹ Zamanla hakimın kararı için başvuruda bulunan yetkilinin mevcut koşullar çerçevesinde, bir suç işleme ihtimalinin olduğunu ortaya koyabilecek olaylar sunabilmesinin beklenebileceği ileri sürülmüştür.⁷⁹² Böylece önceki anlayıştaki gibi, kolluğun, bilgisinin güvenilir olduğunu ortaya koymasının aranması şeklinde değil; daha çok mevcut koşulları dikkate alan, makul değerlendirme kavramına odaklı, sadece keyfi tahminlere dayanmadan, hakimın koşulları makul değerlendirmesi beklenmektedir.⁷⁹³

A.B.D. hukukunda muhtemel / olası neden, en genel itibariyle, suç işleme ihtimalinin, işlenmeme ihtimalinden daha fazla olması şeklinde nitelendirilmektedir.⁷⁹⁴ Nitekim Amerikan Yüksek Mahkemesi, muhtemel / olası neden koşuluna dayanak oluşturacak bilginin, güvenilir olması beklense de; bu güvenilirliğin sadece masum bir kişinin suç işleme ihtimalini ortaya koyabilecek miktarda olması gerektiğini ifade etmiştir.⁷⁹⁵ Bir başka deyişle, önleme amaçlı denetim tedbirini ve bu tedbirin uygulanmasını anlamsız kılacak şekilde bir ihtimal yoğunluğu veya kuvvetli şüphe derecesinde bir yoğunluk aranmamakta; makul olarak mevcut koşullar altında bir tehlike veya suç işleme ihtimali aranmaktadır. Nitekim önleme amaçlı denetimin anlamına ters düşmeyecek şekilde ve fakat ortada

⁷⁹⁰ Aguilar v. Texas, 378 U.S. 108, 114, 1964; State v. Hinchion 207 Neb. 478, 1980.

⁷⁹¹ R. Trent Gaither, "The Aguilar-Spinelli Doctrine: In Requiem," *Houston Law Review*, C.XXI, Ekim 1984, s. 957-960; Michael A. Quinn, "Criminal Procedure," *Creighton Law Review*, C.XV, 1981, s. 236.

⁷⁹² Quinn, *a.g.m.*, s. 231-239; Gaither, *a.g.m.*, s. 960. Ayrıca bkz.: Brinegar v. United States, 338, U.S. 160, 1949; New Jersey v. T.L.O., 469, U.S. 325, 1985.

⁷⁹³ Wesley Macneil Oliver, "The Modern History of Probable Cause," *Tennessee Law Review*, C.LXXVIII, 2010-2011, s. 428; Jeffrey J. Rachlinski, Chris Guthrie, Andrew J. Wistrich, "Probable Cause, Probability, and Hindsight," *Journal of Empirical Legal Studies*, C.VIII, 72-98, Aralık 2011, s. 73; Hixson, *a.g.e.*, s. 214.

⁷⁹⁴ Joseph M. Livermore, "The Draper-Spinelli Problem," *Arizona Law Review*, C.XXI, 1979, 7. dipnot, s. 946; Marshall H. Silverberg, "Anonymus Tips, Corroboration, and Probable Cause: Reconciling the Spinelli/Draper Dichotomy in Illinois v. Gates," *American Criminal Law Review*, C.XX, 1982, s. 101.

⁷⁹⁵ Beck v. Ohio, 379 U.S. 89, 1964.

da henüz bir suç olmadığı ve kişinin özel yaşamının gizliliği hakkının korunması gerektiği bilinciyle bir muhtemel / olası neden değerlendirmesi beklenmelidir.

Kısacası, hukukumuz bakımından, yetkili kişilerin sadece tahmine dayalı istihbarat bilgilerini veya sadece duyumları değerlendirip tehlike olasılığı sonucuna vararak iletişimi önleme amaçlı denetlemeleri hukuka aykırı olarak değerlendirilmelidir.⁷⁹⁶ Ayrıca hukukumuz bakımından da, ilgili yasal mevzuat, herkes hakkında önleme amaçlı denetim kararı verilebilmesinin mümkün olduğu kaygısı yaratmayacak açıklıkta düzenlenmelidir.

5397 sayılı Kanun'un öngörmediği bir diğer ilke de, başka suretle suç işlenmesinin önlenmesinin mümkün olmaması durumunda tedbirin uygulanabilmesi ilkesidir. İletişimin adli amaçlı denetlenmesinde, başka suretle delil elde etme imkanının bulunmaması şeklinde karşımıza çıkan bu husus son çare prensibi olarak da değerlendirilebilir.⁷⁹⁷ Nitekim İletişimin Denetlenmesi Yönetmeliği bu ilkeyi, soruşturma veya kovuşturma sırasında diğer tedbirlere başvurulmuş olsa bile sonuç alınamayacağı konusunda bir beklentinin varlığına veya başka yöntemlerden biri veya birkaçının uygulanmasına rağmen delil elde edilememesi ve delillere ancak bu Yönetmelik'te düzenlenen tedbirlerle ulaşılabilecek olması şeklinde düzenlemiştir.⁷⁹⁸ Ölçülülük ilkesinin bir alt unsuru olan gereklilik ilkesinin gereği olarak, amacı gerçekleştirmeye elverişli aynı derecede etkili tedbirler varsa, bu tedbirlerden ilgili temel hak ve özgürlüğe en az müdahale edeninin uygulanması gerekmektedir.⁷⁹⁹

İletişimin adli amaçlı denetiminde diğer koruma tedbirlerinin uygulama imkanı bakımından yapılabilecek değerlendirme, önleme amaçlı denetimde de uygulama imkanı olabilecek diğer önleme amaçlı tedbirler göz önünde bulundurularak

⁷⁹⁶ Şen, a.g.e., s. 69; Kunter, Yenisey, Nuhoğlu, a.g.e., s. 49; Vatan, a.g.e., s. 122, 123.

⁷⁹⁷ CMK m. 135/1; Hakan Hakeri, Yener Ünver, **Ceza Muhakemesi Hukuku Temel Bilgiler**, 6. bs., Ankara, Adalet, 2012, s. 237; Kunter, Yenisey, Nuhoğlu, a.g.e., s. 49, 50.

⁷⁹⁸ İletişimin Denetlenmesi Yönetmeliği'nin 4/c maddesi.

⁷⁹⁹ Ceza hukukçularının bu ilkeyi oranlılık ilkesinin bir alt unsuru olarak ikincillik ilkesi şeklinde ifade ettiği görülebilir. Bu bağlamda ifade edilen arama, el koyma, tutuklama tedbirleri gibi diğer koruma tedbirleri göz önünde bulundurularak, daha az müdahale oluşturan diğer tedbirlere öncelik verilmesidir, Şahin, a.g.e., s. 265, 266; Öztürk ve diğerleri, a.g.e., s. 468.

yapılabilir. Örneğin, teknik araçla izleme gibi bir tedbire de başvurabilme imkanı bulunmakta ise, özel yaşamın gizliliği ve iletişimin gizliliğine yapacağı müdahalenin ağırlığı da dikkate bulundurularak, iletişimin denetlenmesi ve teknik araçla izleme tedbirinden, hakka en az müdahale edeni uygulanmalı ve başka yolla suç işlenmesi önlenebilecekse, iletişimin denetlenmesi tedbirine başvurulamayacağı benimsenmelidir. Sonuç alınamayacağına dair makul bir beklenti olmadan sadece başka bir tedbiri uygulamanın sonuca ulaşmayı zorlaştıracak olması düşüncesi, iletişimin denetlenmesi tedbirine başvurmak için yeterli görülmeyebilir.⁸⁰⁰

5. İletişimin Önleme Amaçlı Denetlenmesi Tedbirinin Talep Edilmesi ve Karar

2559 sayılı PVSK'nın ek 7. maddesi, 2803 sayılı Jandarma Kanunu'nun ek 5. maddesi ve 2937 sayılı MİT Kanunu'nun 6. maddesi, polis, jandarma ve istihbarat yetkilileri tarafından iletişimin önleme amaçlı denetlenmesine başvurulabilmesi için kural olarak hakim kararına ihtiyaç olduğunu hükme bağlamıştır. Aynı hükümler uyarınca yetkili ve görevli hakim ise, talepte bulunan kolluk biriminin veya başkaca birimin bulunduğu yer itibarıyla yetkili olan ve 5271 sayılı CMK'nın 250. maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemesinin üyesidir.

CMK'nın 250/1. maddesine göre kurulan ağır ceza mahkemesi üyelerinin kendi yargı çevreleriyle sınırlı olarak karar vermeleri gerekliliği Yargıtay tarafından da dile getirilmiştir. Buna göre, “2803 sayılı Kanun’un ek 5. maddesinin 2. fıkrası gereğince yetkili ve görevli hakim, talepte bulunan kolluk biriminin bulunduğu yer itibarıyla yetkili olan ve 5271 sayılı Kanun’un 250. maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemesinin üyesi olması dolayısıyla Ankara Onbirinci Ağır Ceza Mahkemesi’nin kendi yargı çevresi ile ilgili karar vermesi gerekirken, tüm Ülke çapını kapsayacak şekilde karar vermesinin mümkün olmadığı dikkate alınmaksızın,

⁸⁰⁰ İletişimin adli amaçlı denetlenmesi açısından bu sonuca varan görüş için ise bkz.: Öztürk ve diğerleri, **a.g.e.**, s. 466 vd.

itirazın kabulü yerine (...) şekilde karar verilmesinde isabet görülmediğine”⁸⁰¹ hükmedilmiştir. Yargıtay yasa koyucunun amacı açısından da, “amacı ne olursa olsun hiçbir kuruma demokratik bir hukuk devleti olan Türkiye Cumhuriyetinde yaşayan insanlar şüpheli görülerek Ülke genelini kapsayacak şekilde yetki verilemeyeceği, anılan kanunların ilgili maddeleri gereğince talepte bulunan kolluk birimlerinin bulundukları yerler itibarıyla yetkili olan ve 5271 sayılı CMK’nın 250. maddesinin 1. fıkrasına göre kurulan ağır ceza mahkemesi üyelerinin kendi yargı çevreleri ile ilgili karar vermeleri gerektiği, sınırsız bir yetki verilmesi suretiyle iletişimin tespit edilerek dinlenilmesine karar verilemeyeceğini” vurgulamış ve Ankara 11. Ağır Ceza Mahkemesi’nin kararını yetki yönünden bozmuştur.⁸⁰²

İletişimin önleme amaçlı denetlenmesine henüz bir suç veya suç teşebbüsü olmadan başvurulduğundan, bu tedbirin dayanağını oluşturacak hakim kararında yasal koşulların somut olaydaki varlığının değerlendirilmesi gerektiği ifade edilebilir. Kaldı ki, iletişimi denetlenecek kişilerin olayla ilgili bağlantılarına dair somut bilgilerin, talepte bulunması ve hakime sunulması aranmalıdır.⁸⁰³

A.B.D.’de iletişimin dinlenmesi bakımından uygulanan yasal düzenleme olan Tel le Yapılan İletişimin Dinlenmesine Dair Kanun (Wiretap Act)’a göre de, dinleme kararı verilebilmesi için hakim kararı gerekmektedir ve bu kararda da sadece tedbirin süresi ve kullanılan iletişim aracının türü gibi bilgiler değil, iletişimi denetlenen kişinin suçu işleyeceği iddiasına dair değerlendirme de beklenmektedir. Wiretap Act bakımından hakimden böyle bir talepte bulunmaya sadece Başsavcı gibi belirli kamu görevlileri yetkili kılınmıştır. Örneğin polis, böyle bir dinleme yetkisi talep etmeye yetkili kılınmamıştır.⁸⁰⁴ A.B.D.’de, yabancı istihbaratın A.B.D. ile ilgili bilgi edinmesini ve terörizmi önlemek nedeniyle, iletişimin istihbari amaçlı denetlenmesini düzenleyen FISA’da da, hakim kararı aranan bir koşul olarak karşımıza çıkmaktadır. Fakat FISA’yı bu noktada farklı kılan, iletişimi denetlenen

⁸⁰¹ E. 2008/874, K. 2008/7160, Yargıtay 9. Ceza Dairesi, 04/06/2008.

⁸⁰² A.e.

⁸⁰³ Şen, a.g.e., s. 79.

⁸⁰⁴ Ayrıca sadece öngörülen belirli suçlar için böyle bir tedbir talebinde bulunulabilecektir, The Wiretap Act, 18 USCS § 2516 - §2518.

kişinin bir suç işleyeceğine dair değil, yabancı (A.B.D. vatandaşı olmayan) veya bir yabancının temsilcisi olduğuna dair - mahkemenin basit şüpheden daha yoğun, bazı somut belirtilere dayanan nitelikte - bir muhtemel / olası neden belirlemesinin beklenmesidir. FISA bağlamında iletişimin denetlenebilmesi için izin istenen mahkeme, federal yargıçlardan oluşan özel bir mahkemeden oluşmaktadır.⁸⁰⁵ Sadece yabancılarının olduğu bir iletişimden istihbarat ediniliyorsa ve iletişimdeki taraflardan hiçbiri A.B.D. vatandaşı değilse FISA bağlamında hakim kararına gerek olmadan iletişimin denetlenmesi gerçekleştirilebilecektir. Bu durumda Başsavcı aracılığıyla Başkan, böyle bir tedbir için izin verebilecektir.⁸⁰⁶

Türk hukukunda polisin, jandarmanın ve milli istihbarat yetkililerinin iletişimi önleme amaçlı denetlemeleri açısından, gecikmesinde sakınca bulunan hallerde kanunen yetkili kılınmış kişilerin vereceği yazılı emirle iletişimin denetlenebileceği öngörülmüştür. Bu kişiler, polis açısından, Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanı; jandarma açısından, Jandarma Genel Komutanı veya istihbarat başkanı ve MİT açısından da MİT Müsteşarı veya yardımcısı olarak kabul edilmiştir.⁸⁰⁷

Gecikmesinde sakınca bulunan hal, TİB Yönetmeliği'nde "derhal işlem yapılmadığı takdirde suçun iz, eser, emare ve delillerinin kaybolması veya şüphelinin kaçması veya kimliğinin saptanamaması olasılığının ortaya çıkması hali" olarak

⁸⁰⁵ The Foreign Intelligence Surveillance Act, 50 USCS § 1803.

⁸⁰⁶ The Foreign Intelligence Surveillance Act, 50 USCS § 1801, § 1802/a.

⁸⁰⁷ 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 6. maddesi. Burada işaret edilebilecek diğer husus, kamu düzeni, güvenliği ve suç işlenmesinin önlenmesi ile ilgili olarak yetkili olan valilerin ve kaymakamların, böyle bir görevleri olsa da, iletişimin önleme amaçlı denetlenmesi bakımından gecikmesinde sakınca bulunması halinde iletişimin denetlenmesi için yazılı emir verme yetkisine sahip kılınmamış olmalarıdır. Nitekim 5442 sayılı İl İdaresi Kanunu, 11. maddesinde valinin il sınırları içinde bulunan genel ve özel bütün kolluk kuvvet ve teşkilatının amiri olduğunu ve suç işlenmesini önlemek, kamu düzen ve güvenliğini korumak için gereken tedbirleri alabileceğini düzenlemiştir. Aynı kanun 32. maddesinde de, kaymakamların, ilçe sınırları içinde bulunan genel ve özel kolluk kuvvet ve teşkilatının amiri olduğunu ve suç işlenmesini önlemek, kamu düzen ve güvenliğini korumak için gereken tedbirleri alabileceğini hükme bağlamıştır, 5442 sayılı, 10/6/1949 tarihli İl İdaresi Kanunu, Resmi Gazete No. 7236, Resmi Gazete tarihi: 18/06/1949.

düzenlenmiştir.⁸⁰⁸ Buna göre, hakimden karar almak için yeterli zamanın olmaması ve örneğin suçun iz, eser, emare ve delillerinin kaybolması olasılığının varlığı aranan unsurlardan bazılarıdır. Fakat burada dikkat çeken husus, suçun iz, eser, emare ve delilleri gibi unsurların da düzenlemede yer bulmasıdır. Zira iletişimin önleme amaçlı denetlenmesinde, ortada bir suç bulunmamaktadır ve aslında bir suçun işlendiği iddiası yerine, suç işlenebilme ihtimalinden bahsedilmektedir.⁸⁰⁹

Bu bağlamda, 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 ihtimalinin ortaya çıkması ve gerektiğinde hakimden karar almak için vakit bulunmaması halinin, kanunen yetkili kılınmış merciin vereceği yazılı emirle iletişimin denetlenmesini mümkün kılan gecikmede sakınca bulunan hal olarak kabul edilmesi düşünülebilir. Nitekim bu tanımlamanın benzeri, Adli ve Önleme Aramaları Yönetmeliği'nde önleme aramaları bakımından öngörülmüştür.⁸¹⁰

Gerek polis, gerek jandarma gerek MİT'in iletişimi denetlemesi açısından, gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmi dört saat içinde yetkili ve görevli hakimın onayına sunulacaktır. Bu durumda hakimın kararını en geç yirmi dört saat içinde vermesi öngörülmüştür.⁸¹¹ Hakimın onayına sunulmak üzere gönderilen onay talep yazılarına dair, TİB Yönetmeliği'nin herhangi bir hüküm

⁸⁰⁸ TİB Yönetmeliği m. 3/f, m. 4.

⁸⁰⁹ Şen, a.g.e., s. 68.

⁸¹⁰ Adli ve Önleme Aramaları Yönetmeliği, Resmi Gazete No. 25832, Resmi Gazete tarihi: 01/06/2005. Yönetmeliğin 4. maddesi, gecikmesinde sakınca bulunan hal kavramını - önleme aramaları bakımından - "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 silâh, patlayıcı madde veya eşyanın tespit edilememesi ihtimalinin ortaya çıkması ve gerektiğinde hakimden karar almak için vakit bulunmaması hali" olarak düzenlemiştir.

⁸¹¹ 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 6. maddesi.

benimsemediği görülebilir. Fakat CMK bağlamında iletişimin denetlenmesini ilgilendiren İletişimin Denetlenmesi Yönetmeliği'nde bu husus düzenlenmiştir.⁸¹²

Bu esaslardan yola çıkarak, hakimden onay talep edilmesinden itibaren izlenecek usul açısından şunlar düşünülebilir. Öncelikle CMK bağlamında iletişimin denetlenmesinde gecikmesinde sakınca bulunan halde hakkında hakimden onay talep edilen yazı, Cumhuriyet başsavcılığı tarafından verilecek iken; önleme amaçlı denetimde yetkili mercii⁸¹³ tarafından verilecektir. İletişimin Denetlenmesi Yönetmeliği, gönderilen talep yazısının, hakim tarafından saat belirtilerek havale yapılacağını hükme bağlamıştır.⁸¹⁴ Buna göre, “talep, istemin içeriği gösterilmeksizin, hakim havalesinde belirtilen saat de işlenmek suretiyle, bu iş için görevlendirilen ilgili zabıt katibi tarafından mahkemenin değişik iş defterine kaydedilir. Hakim tarafından havale saatinden itibaren 24 saat içerisinde karar verilir. Verilen karar, tutanakla Cumhuriyet başsavcılığına teslim edilir ve mahkeme kaleminde kalan suretinin gizli tutulması için ilgili hakim tarafından gerekli tedbir alınır.”⁸¹⁵ Bu bağlamda, önleme amaçlı denetim açısından da hakime havale edilen talep yazısının kaydedilmesi, havaladan belli bir süre sonra karar verilmesinin öngörülmesi gibi hususların düzenlenmesinin yerinde olacağı söylenebilir.

Hakimin yetkili mercii vereceği yazılı emri incelemesi, hukuki bir denetim şeklinde, gecikmesinde sakınca bulunan bir hal olup olmadığı, verilen kararın ilgili suçların önlenmesine ilişkin olup olmadığı ve sorumluluk alanına dair yükümlülüklerin yerine getirilip getirilmediği gibi hususların değerlendirilmesi

⁸¹² İletişimin Denetlenmesi Yönetmeliği m. 12/3.

⁸¹³ Bu mercii polis açısından, Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanı; jandarma açısından, Jandarma Genel Komutanı veya istihbarat başkanı ve MİT açısından da MİT Müsteşarı veya yardımcısı olarak düzenlenmiştir, 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 6. maddesi.

⁸¹⁴ İletişimin Denetlenmesi Yönetmeliği m. 5/4.

⁸¹⁵ İletişimin Denetlenmesi Yönetmeliği'nde ayrıca, bu kararların tedbir süresince değişik iş kartonuna takılmayacağını ve tedbirin sona erdiği öğrenildiğinde ilgili kartonuna ilave edileceği de düzenlenmiştir. Bu maddedeki tüm işlemler sırasında gizliliğe uyulacağı da hükme bağlanmıştır, İletişimin Denetlenmesi Yönetmeliği m. 5/4.

şeklinde görülebilir.⁸¹⁶ Nitekim TİB Yönetmeliği, Jandarmanın iletişimin denetlenmesi işlemini yerine getirmesi için 2803 sayılı Jandarma Kanunu uyarınca iletilen talepler ile verilen kararlar ve yazılı emirlerde, sorumluluk alanına dair bilgi ve belgelere yer verilmesine ilişkin bir düzenleme içermektedir.⁸¹⁷ Bu hüküm de sorumluluk alanına ilişkin bir değerlendirme yapılması gerekliliğini düşündüren örneklerden biri olarak görülebilir.

Gerek TİB Yönetmeliği'nde gerek İletişimin Denetlenmesi Yönetmeliği'nde gecikmesinde sakınca bulunan halde verilen yazılı emrin hakimın onayına sunulacağı belirtilmiş olsa da, burada hakimın sadece bir onay makamı pozisyonunda olmasının düşünülmemesi gerekir. Bununla birlikte, kanımızca, böyle bir durumda 24 saat içinde kararını vermesinin beklendiği buradaki hakimden, iletişimin hukuka aykırı denetlenmesi nedeniyle önüne gelen olayda kararın yetki, usul ve esas açısından değerlendirmesini yapacak hakimle aynı nitelikteki bir değerlendirme yapması beklenmekte midir sorusu konusunda da bir açıklık bulunmamaktadır. Nitekim bu konuda, hakimın sadece hukuka uygunluk değil, amaca uygunluk denetimi de yapabileceği ileri sürülmüştür.⁸¹⁸

Uygulamada tedbirin uygulanmasına dair hakim kararının ileriye veya geriye dönük olabileceği hususunda, tedbirin türüne göre bir ayırım olduğu söylenebilir. Buna göre, iletişimin tespiti tedbirine dair kararın geriye dönük olarak verildiği görülmektedir. Böylece bu tedbir dahilindeki bilgilerin bir başka anlatımla bir telefon numarasından kimlerin ne zaman arandığı, bu numaranın kimler tarafından arandığı ve ne kadar süreyle görüşüldüğü gibi bilgilerin geçmişe dönük olarak TİB tarafından ilgili birimlere aktarıldığı söylenebilir. Sinyal bilgilerinin değerlendirilmesi de bu şekilde görülebileceği gibi; iletişimin dinlenmesi tedbirinde ise karar ileriye dönük olarak verilmektedir.

⁸¹⁶ Şen, a.g.e., s. 73, 74.

⁸¹⁷ TİB Yönetmeliği m. 9.

⁸¹⁸ Öztürk ve diğerleri, a.g.e., s. 476.

a. Hakimin Kararının Veya Yazılı Emrin İçeriği Ve Bulunması Gereken Bilgiler

İletişimin önleme amaçlı denetlenmesine ilişkin hakim kararında ve yetkili merciler tarafından verilen yazılı emirlerde tedbirin türü, kapsamı ve süresi, tedbire başvurulmasını gerektiren nedenler ile yazılı emrin verildiği tarih ve saatin⁸¹⁹ belirtilmesi gerektiği hükme bağlanmıştır.⁸²⁰ Ayrıca daha önce de ifade edildiği üzere, 2803 sayılı Jandarma Kanunu bağlamında iletilen talepler ile verilen kararlar ve yazılı emirlerde, sorumluluk alanına ilişkin bilgi ve/veya belgelere de yer verilmesi beklenmektedir. Kararda veya yazılı emirde yer alması öngörülen bazı bilgilerden ise belirlenebilen bir tanesinin dahi bulunması yetecektir. Buna göre, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespiti imkan veren kodundan belirlenebilenler kararda veya yazılı emirde bulunacaktır.⁸²¹

Kanımızca ilgili kararda bu bilgilerden sadece “belirlenebilenler”in yer alması, özel yaşamın gizliliği ve iletişimin gizliliği hakkı açısından sorunlu ve hatta bu hakların hukuka aykırı ihlallerine neden olabilecek bir düzenleme olarak değerlendirilmelidir. Nitekim uygulamada da bu bilgilerden kararda veya yazılı emirde - sadece onun belirlenebildiğinden bahisle - en kolay elde edilebilecek olan telefon numarasının belirtilmesi, diğer şartlar da varsa, denetim faaliyetinin başlatılması için yeterli görülmektedir. Fakat adli amaçlı denetim açısından CMK’da olduğu ilgili bilgilerin “belirtileceği”nin⁸²² düzenlenmesi yerine, önleme amaçlı denetim açısından 5397 sayılı Kanun’da sadece ilgili bilgilerden “belirlenebilenler” kavramının kullanılması; yasallık kaydı açısından yerinde görülemez. Zira 1982 Anayasası’nda temel hak ve özgürlüklerin ancak yasayla sınırlanabileceği hükme bağlanmıştır. Özel yaşamın gizliliği ve iletişimin gizliliği hakkını sınırlayacak yasanın sahip olması gereken

⁸¹⁹ TİB Yönetmeliği’nin ilk halinde mevcut olmayan bu bilginin yer alması zorunluluğu, tıpkı özellikle Jandarma açısından önem taşıyan, sorumluluk alanına ilişkin bilgi ve/veya belgelere de yer verilmesi gerekliliği gibi Yönetmeliğe 2007 değişikliğiyle eklenmiştir.

⁸²⁰ TİB Yönetmeliği m. 9/1.

⁸²¹ TİB Yönetmeliği m. 9/1 (a).

⁸²² CMK’nın 135. maddesi’ne göre kararda, “yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespiti imkan veren kodu, tedbirin türü, kapsamı ve süresi belirtilir”.

nitelikleri de, AİHM anlayışını dikkate alarak, çalışmanın daha önceki bölümlerinde ifade ettik. Buna göre, yasallık kaydı olarak ifade edebileceğimiz bu ilkenin sağladığı güvencelerin zedelenmeden korunması, kişilerin temel hak ve özgürlüklerinin korunması açısından büyük önem taşımaktadır. Bu güvencelerin en önemlileri, temel hak ve özgürlüğü sınırlayacak yasanın herkes için geçerli kurallar koyarken, sınırlamanın objektifliğini de sağlaması ve keyfiliğe dayanak teşkil etmemesidir. Nitekim AİHM yaklaşımından da anlaşıldığı üzere, yasallık ilkesine dair sorun sadece yasal değil de idari bir düzenleme olduğunda ortaya çıkmamaktadır. Kimi durumlarda bir yasal düzenlemenin varlığına ve ulaşılabilirliğine rağmen, bu ilkeye aykırılık tartışılabilmekte; yasanın kalitesi değerlendirilebilmektedir.⁸²³ Bu bağlamda, ilgili yasanın açık, belirli ve kişinin belirli şartlar içinde davranışının yaratabileceği sonuçları makul bir şekilde öngörebilmesini sağlayacak şekilde olması gereklidir.⁸²⁴ Kısacası, temel hak ve özgürlüğü sınırlayacak yasanın, kamusal makamlara aşırı takdir yetkisi verebilecek belirsizlikte olmaması gerekmektedir.⁸²⁵

5397 sayılı Kanun'da düzenlendiği şekliyle, ilgili bilgilerden sadece "belirlenebilenler" in, diğer bir deyişle bu bilgilerden uygulamada en çok karşılaşıldığı şekliyle telefon numarasının bulunmasının dahi yetecek olması, yasallık ilkesiyle bağdaşmamaktadır. Kaldı ki, denetlenmesi, adli amaçlı denetime göre daha kolay şartlara bağlanan iletişimin önleme amaçlı denetimi açısından böyle bir düzenlemenin yapılması; özel yaşamın gizliliği hakkı açısından esaslı bir tehlike teşkil etmektedir. Yasadaki bu düzenlemenin, yeterli güvenceyi sağlayacak şekilde yeniden düzenlenmesi gerektiği söylenebilir.

İlgili hususların kararda veya yazılı emirde yer almasına hassasiyet gösterilmesinin önemi, iletişimin denetlenmesine imkan verecek karar veya emrin belirli şahıslar için değil genel olarak ve yer itibarıyla örneğin tüm ülkeyi veya geniş anlamda belirli yerleri kapsayacak şekilde düzenlenmesi ve iletişimin de bu şekilde temel hak ve

⁸²³ Case of Kopp v. Switzerland, para 62-75.

⁸²⁴ Case of Malone v. The United Kingdom, para 67, 68. Case of Khan v. The United Kingdom, para 27; Case of Malone v. The United Kingdom, para 68; Case of Rotaru v. Romania, para 47-63; Case of Kopp v. Switzerland, para 16. Ayrıca bkz.: Kil Kelly, *a.g.e.*, s. 44, 45.

⁸²⁵ Kaboğlu, *a.g.e.*, s. 90.

özgürlükleri zedeleyecek şekilde denetlenmesinin önüne geçilmesi zorunluluğundan kaynaklanmaktadır.

Hakimin kararında veya yazılı emirde zorunlu bilgilerin olmaması durumunda TİB Yönetmeliği'ne aykırı bir karar veya yazılı emir ile karşı karşıya kaldığımız söylenebilir. Bu bağlamda, 5397 sayılı Kanun, CMK bağlamında iletişimin denetlenmesinde olduğu gibi,⁸²⁶ karar veya yazılı emre itiraz hususunu açıkça içermemektedir. TİB Yönetmeliği'ne göre, aykırılığı tespit edilen taleplerin, eksikliklerinin giderilmesi için ilgili kuruma iadeleri söz konusu olacaktır. Buna göre, yerine getirilmeyecek talepler Polisin yapacağı iletişimin denetlenmesi işlemi açısından, Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanlığına,⁸²⁷ Jandarma açısından, Jandarma Genel Komutanlığı İstihbarat Başkanlığına⁸²⁸ ve MİT bakımından MİT Müsteşarlığına⁸²⁹ iade edilebilecektir. Kaldı ki, taleplerin TİB Yönetmeliği'ne ve diğer ilgili mevzuata uygun olup olmadığını incelemek ve gerektiğinde yetkili mercilere başvuruda bulunmak da TİB'in görevleri arasında sayılmıştır.⁸³⁰ Bu hususlar, TİB'in itiraz yetkisi kapsamında değerlendirilebilir.⁸³¹

CMK bağlamında gerçekleştirilecek iletişimin denetlenmesi bakımından, TİB'e belirli koşullarda hakim kararına itiraz yetkisi verilmiş olduğu ve fakat aynı şeyin önleme amaçlı denetim açısından TİB Yönetmeliği'nde düzenlenmemiş olduğu da belirtilmelidir. TİB'in bu tür durumlarda, özellikle hakim kararlarına itiraz hakkının olup olmadığının belirsiz olduğu ve bu nedenle nasıl hareket edeceğinin bazı koruma tedbirleri için varolan itiraz imkanı ile paralellik kurularak açıklanmaya çalışılması⁸³² göz önünde bulundurulması gereken bir değerlendirme olabilir. Burada uygulama da dikkate alınmalıdır. Zira uygulamada TİB, kendisine karar veya yazılı emir ulaştıktan

⁸²⁶ CMK'nun 135. maddesindeki hükümlere aykırı olarak verilen kararlar ile İletişimin Denetlenmesi Yönetmeliği'nde sayılan ve tanımlanan iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi işlemleri dışındaki talepleri içerdiği açıkça anlaşılan kararlara karşı Başkanlık da itiraz edebilecekler arasında sayılmıştır, İletişimin Denetlenmesi Yönetmeliği m. 10/1.

⁸²⁷ TİB Yönetmeliği m. 5/son.

⁸²⁸ TİB Yönetmeliği m. 6/son.

⁸²⁹ TİB Yönetmeliği m. 7/son.

⁸³⁰ TİB Yönetmeliği m. 17/c.

⁸³¹ Uygulamada, bu itirazın başlamış işlemi durdurmadığından bahisle, hukuka aykırılığın kısa zamanda yerine getirilmesinin istendiği belirtilmektedir.

⁸³² Taşkın, a.g.e., s. 215.

ve ilgili kanun ve diğer mevzuata uygunluk incelemesi yapıldıktan sonra itiraz edebilmektedir. Bu nedenle, kural olarak itiraz edilemeyecek olan mahkeme kararlarına,⁸³³ temel hak ve özgürlükler açısından önem taşıyan tutuklama gibi bir koruma tedbiri kararı söz konusu olduğunda itiraz edilebilmesi gibi,⁸³⁴ TİB'in de böyle bir itiraz hakkının açıkça yasal düzenlemede yer alması yerinde olabilir. Nitekim iletişimin önleme amaçlı denetlenmesinin özel yaşamın gizliliği ve iletişimin gizliliği hakkı açısından ifade ettiği önem, önleme tedbirinin niteliği ve henüz bir suç işlenmemiş olduğu bu değerlendirmenin başlıca nedenlerini oluşturmaktadır.⁸³⁵ Kaldı ki, unutulmamalıdır ki, önleme amaçlı iletişimin denetlenmesi açısından durumdan haberdar olmayan ilgilinin itiraz etmesi gibi bir husus da söz konusu olamayacaktır.

b. Tedbirin Süresi

İletişimin önleme amaçlı denetlenmesi kararlarının en fazla üç ay için verilebileceği ve bu sürelerin aynı usulle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabileceği kabul edilmiştir.⁸³⁶ Sürenin başlangıcı, daha doğrusu kararın verilmesinden itibaren en geç ne kadar sürede uygulamanın başlatılacağı hakkında açısından ise, 5397 sayılı Kanun ve TİB Yönetmeliği herhangi bir hüküm içermemektedir. Buna karşılık, İletişimin Denetlenmesi Yönetmeliği 5. maddesinde sürenin, kararın Başkanlığa ulaştığı andan itibaren başlayacağını; 12. maddesinde ise, dinleme veya mobil telefonun yerinin tespiti kararlarında sürenin, kararın TİB'de sisteme tanıtıldığı andan itibaren başlayacağını hükme bağladığı görülmektedir. İki hüküm arasındaki bu farklılık, CMK'da da süreye ilişkin bir düzenlemenin mevcut olmadığı da dikkate alınarak, tedbirin süresinin ne zaman başlayacağına dair değişik değerlendirmeler yapılmasına neden olmuştur. Genel itibariyle iletişimin adli amaçlı

⁸³³ CMK'nun 267. maddesi, hakim kararları ile kanunun gösterdiği hallerde, mahkeme kararlarına karşı itiraz yoluna gidilebileceğini hükme bağlamıştır.

⁸³⁴ Öztürk ve diğerleri, *a.g.e.*, s. 414; Kunter, Yenisey, Nuhoglu, *a.g.e.*, s. 202, 203; Şahin, *a.g.e.*, s. 224, 225. Ayrıca bkz.: CMK m. 101/5

⁸³⁵ Kunter, Yenisey, Nuhoglu, *a.g.e.*, s. 86, 87.

⁸³⁶ 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 6. maddesi; TİB Yönetmeliği m. 9/son.

denetimiyle ilgili olsalar da, bu deęerlendirmelerin, önleme amaçlı denetimde süre konusuyla da paralellik kurulabilecek olması nedeniyle incelenmeleri yerinde olabilir.

Tedbirin uygulanma süresinin kararın hakim tarafından verildięi andan itibaren başlaması gerektięi bu yaklaşımlardan ilki olarak deęerlendirilebilir. Bu görüşe göre, hakim tarafından kararın verildięi an açısından gerekli şartların varlığına dair bir deęerlendirme yapılmıştır. Bu nedenle sürenin daha sonra başlayacağını kabul etmek, keyfilige ve hatta yetkililer tarafından istenildięi an başlatılarak tedbirin kötüye kullanılmasına da neden olabilecektir.⁸³⁷ Dięer bir yaklaşım ise, İletişimin Denetlenmesi Yönetmelięi'nin 5. maddesinden yola çıkarak, sürenin, tedbir kararının TİB'e ulaştıęı andan itibaren başlaması gerektiğini vurgulamaktadır. Bu görüş, keyfilige mümkün kılabilceęi ve kararın TİB'e ge gönderilerek aynı kaygıların gerekleşmesine imkan verebileceęi nedeniyle eleştirilebilir. Son olarak da, İletişimin Denetlenmesi Yönetmelięi'nin 12. maddesini de dikkate alarak, kararın TİB'de sisteme tanıtıldıktan sonra sürenin başlaması gerektięi yönündeki görüşün ileri sürüldüğü görülebilir. Kararın TİB'e ulaşmasından ve TİB'de sisteme tanıtılmasından sonra sürenin başlaması gerektiğine dair yaklaşımların Danıştay'ın ilgili kararında deęerlendirildięi görülmektedir.⁸³⁸

İletişimin denetlenmesi tedbiri, Danıştay tarafından, dięer özelliklerinin yanı sıra Anayasa ile güvence altına alınan haberleşme özgürlüğünün kısıtlanması anlamına gelen olağanüstü bir tedbir olarak deęerlendirilmiştir. Karar, iletişimin adli amaçlı denetlenmesine dair ve İletişimin Denetlenmesi Yönetmelięi ile CMK bağlamında bir deęerlendirme yapmış olsa da, kanımızca iletişimin önleme amaçlı denetlenmesi açısından da, özellikle tedbirin temel hak ve özgürlüklere olan etkisi yönünden, dikkate alınmalıdır. Bu bağlamda, tedbirin uygulanma süresinin başlangı anının, kararın sisteme tanıtılma anı olarak belirlenmesinin, karar sisteme tanıtılmadıęı sürece tedbirin uygulamasının ertelenebileceęi anlamına da gelebileceęi ifade

⁸³⁷ Özbek ve dięerleri, **a.g.e.**, s. 408; Şen, **a.g.e.**, s. 135, 136; Öztürk ve dięerleri, **a.g.e.**, s. 469; Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 52.

⁸³⁸ E. 2007/2795, K.t. 14/10/2008, Danıştay 10. Dairesi; E. 2007/2795, K. 2010/1299, K.t. 22/02/2010, Danıştay 10. Dairesi.

edilmiştir. Danıştay, böyle bir uygulamanın ilgili yasal düzenlemeyle bağdaşmayacağını ve uygulamayı sınırsız olarak ertelenebilir kılan Yönetmelik kuralının da hukuka uyarlık göstermediğini belirtmiştir. Ayrıca tedbir kararının verilmesi ile uygulamaya geçilmesi arasında teknik olarak belirli bir zaman dilimine ihtiyaç var ise, bu süreyi önceden öngören ve uygulama başlangıç tarihinin tedbir kararında yer almasını sağlayan bir düzenleme yapılması zorunluluğunu vurgulamıştır.⁸³⁹

İlgilendirdiği temel hak ve özgürlüğün niteliği de dikkate alındığında, Danıştay'ın yaklaşımında da belirtildiği üzere, iletişimin önleme amaçlı denetimine dair uygulamanın yasal düzenlemelerle güvence altına alınmış bir tedbir olarak hükme bağlanması neredeyse zorunlu gözükmektedir. Kaldı ki, 5397 sayılı Kanun'da ve TİB Yönetmeliği'nde karar veya yazılı emrin uygulanmasına dair işlemin başlatıldığı ve bitirildiği tarih ile saatin bir tutanakla saptanacağı da hükme bağlanmıştır.⁸⁴⁰ Bu bağlamda, sadece işlemin fiilen başladığı tarih ve saatin tutanakla belirlenmesiyle yetinilmemelidir. Uygulamanın tutarlı ve bu tür güvenceleri de anlamlı kılacak şekilde yapılabilmesi için, işlemin başlayacağı sürenin ne zaman olacağının da açık bir şekilde gerek 5397 sayılı Kanun gerek TİB Yönetmeliği'nde düzenlenmesi yerinde bir çözüm olarak değerlendirilebilir.

Uygulamada TİB tarafından tedbirin başlangıç süresi, mahkeme kararın verildiği tarih olarak kabul edilmektedir. Genel itibariyle, kararların verildiği tarihte TİB'e ulaştırılmasının ve aynı tarihte de hukuka uygunluk incelemesinden sonra sisteme tanıtılmasının bu değerlendirmede etkisinin olduğu söylenebilir. Bazı durumlarda, mahkeme kararında da tedbirin başlangıç süresinin belirtildiği bilinmektedir. Bu nedenle kararda özel, ayrı bir süre öngörülmemişse, genel itibariyle kararın verildiği tarih tedbirin başlangıç süresi olarak esas alınmaktadır.

⁸³⁹ Danıştay'ın bu yaklaşımının, kararın TİB'e ulaşma anından itibaren sürenin başladığına dair kabulü de imkansız kıldığı ileri sürülmüştür, Kaymaz, *a.g.e.*, s. 324

⁸⁴⁰ 5397 sayılı Kanun m. 1-3; TİB Yönetmeliği m. 10/2.

A.B.D.'de, iletişimin denetlenmesi tedbirine ilişkin sürenin 30 gün olabileceği ve sürenin başlangıcının, kararın uygulanarak tedbir işleminin fiilen yerine getirilmesi olduğu hükme bağlanmıştır. Bu sürenin, kararın verilmesinden itibaren 10 günü geçemeyeceği de güvence altına alınmaktadır.⁸⁴¹ Bununla birlikte, tedbirin süresinin hakimın amaca ulaşmak için gerekli gördüğünden ve her halukarda 30 günden fazla olmayacak sürelerle uzatılabilmesinin de mümkün olduğu görülmektedir.⁸⁴²

Türk hukukunda da iletişimin önleme amaçlı denetlenmesine dair sürenin üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilmesi mümkündür.⁸⁴³ Bu bağlamda 3 aylık ilk tedbir süresiyle birlikte toplam 12 ay iletişimin denetlenmesi kararı verilebilecektir.⁸⁴⁴ Bu süre uzatmalarının aslında, tedbirin yenilenmesi kararı olarak nitelendirilmesi düşünülebilir.⁸⁴⁵ Nitekim böyle uzatma taleplerine karar verilmesinde, aynı usulün izleneceği gerek 5397 sayılı Kanun gerek TİB Yönetmeliği'nde hükme bağlanmıştır.⁸⁴⁶ Yenileme kararı olacağı için, ilk dinleme kararıyla ulaşılmak istenen amaca ulaşılamamış ve fakat ulaşmanın da halen mümkün olması gerekliliği düşünülebilir.⁸⁴⁷ Bu bağlamda, ilgili düzenlemeler çerçevesinde koşulların bulunup bulunmadığına yönelik yeni bir değerlendirmenin söz konusu olacağı söylenebilir.

Tedbirin yenilenmesi kararları ile ilk tedbir kararı arasında ve hatta adli amaçlı denetimdeki gibi sadece bir defa değil birden fazla kez uzatılabileceği için, tedbirin

⁸⁴¹ The Wiretap Act, 18 USCS §2518 (5).

⁸⁴² The Wiretap Act, 18 USCS §2518 (5).

⁸⁴³ Mahmutoglu, "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi," s. 416 vd. Ayrıca bkz: 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 6. maddesi; TİB Yönetmeliği m. 9/son.

⁸⁴⁴ Mahmutoglu, a.y. İletişimin adli amaçlı denetimi açısından, bu sürenin 3 aylık uzatma süresiyle birlikte toplam 6 ay olduğu görülmektedir, CMK m. 135/3. Ayrıca adli amaçlı iletişimin dinlenmesi veya kayda alınması sırasında şüphelinin başka bir iletişim aracını kullandığı belirlendiğinde verilecek yeni tedbir kararının, ilk tedbir kararındaki sürenin bitiş tarihini geçemeyeceği de kabul edilmiştir, İletişimin Denetlenmesi Yönetmeliği m. 7/6.

⁸⁴⁵ A.B.D. hukukunda, the Wiretap Act'de de, ilk tedbir kararının uzatılabileceği (extension) hükme bağlanmış olsa da, bu uzatmalar doktrin tarafından sonraki kararın verilmesine dair şartlar da göz önünde bulundurularak, yenilenebilir (renewed) olarak değerlendirilmektedir, Solove, Schwartz, **Privacy, Information, and Technology**, s. 143.

⁸⁴⁶ 5397 sayılı Kanun m. 1-3; TİB Yönetmeliği m. 9/son.

⁸⁴⁷ Kunter, Yenisey, Nuhoğlu, a.g.e., s. 53.

yenilenmesi kararları arasında kesinti olup olamayacağı açık değildir. Kaldı ki, İletişimin Denetlenmesi Yönetmeliği'nde olduğu gibi, örneğin dinlemenin kesintisiz uygulanacağı gibi bir husus da, iletişimin adli amaçlı dinlenmesi bakımından TİB Yönetmeliği'nde hükme bağlanmamıştır. Bu nedenle, iletişimin adli amaçlı denetlenmesinde, özellikle dinlenmesinde olduğu gibi, kesintinin kararın uygulanması sırasında mı yoksa ilk karar ile yenileme kararı arasında mı olduğu tartışmasını, önleme denetlemesi söz konusu olduğunda hüküm bağlamında yapmak çok da mümkün olmayabilir. Adli amaçlı denetim bağlamında yapılan bu tartışmalar genel itibariyle iki görüş etrafında toplanmıştır. Bir görüş, yenilenmiş tedbir süresinin, ilk tedbir süresinin bitmesinden hemen sonra başlaması gerektiğini ve arada kesinti olmaması gerektiğini ileri sürmektedir.⁸⁴⁸ Diğer görüş ise, tedbirin uygulanması sırasında bir kesinti olamayacağı şeklinde değerlendirilmesi gerektiği üzerinde durmaktadır.⁸⁴⁹

Kanımızca iletişimin önleme amaçlı denetiminde, birden fazla kez tedbirin yenilenmesi kararı verilebileceği de göz önünde bulundurulduğunda, esasen tedbir kararı ile yenileme kararı veya kararları arasında kesintinin olması mümkündür. Kaldı ki, iletişimin denetlenmesinin sürekli ve kesintisiz olması gibi bir zorunluluğun öngörülmediği de söylenebilir. Ancak uygulama genellikle ilk tedbir süresi bitmeden önce, tedbirin yenilenmesi için başvuru ve yenileme kararına dair sürenin de ilk tedbir süresinden hemen sonra başlaması şeklinde görülmektedir.

Unutulmamalıdır ki, iletişimin önleme amaçlı denetimi bakımından belirli durumlar için tedbir süresi müteaddit defalar uzatılabilir. Buna göre, terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi durumunda, 3 aydan fazla olmamak üzere müteaddit defalar tedbir süresinin uzatılması mümkün olabilecektir.⁸⁵⁰ Bu bağlamda, terörist faaliyetlerin önlenmesi bakımından, tedbirin uygulanma süresine dair bir üst sınır belirlenmediği söylenebilir. Ayrıca sadece MİT

⁸⁴⁸ Şen, **a.g.e.**, s. 139, 140; Öztürk ve diğerleri, **a.g.e.**, s. 472.

⁸⁴⁹ Kaymaz, **a.g.e.**, s. 327, 328.

⁸⁵⁰ 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 6. maddesi; TİB Yönetmeliği m. 9/son.

açısından geçerli olmak üzere, 2007 yılında 5651 sayılı Kanun’la yapılan değişiklikle, casusluk faaliyetlerinin tespiti çerçevesinde devam eden tehlikelere ilişkin olarak da, gerekli görüldüğünde aynı şekilde 3 aydan fazla olmamak üzere müteaddit defalar tedbirin yenilenebilmesi söz konusu olacaktır.⁸⁵¹

Tedbirin yenilenmesi kararı hakim tarafından verilecektir. Buna göre, gecikmesinde sakınca bulunan halde yazılı emir verebilen yetkili merciin böyle bir yenileme kararı vermesi düşünülemez. Nitekim tedbirin yenilenmesi niteliğinde bir süre uzatılması söz konusu olduğundan, gecikmesinde sakınca bulunan bir halden de söz edilemeyeceği ve bu yenileme kararının hakimden istenmesi gerektiği ifade edilebilir.⁸⁵²

B. İletişimin Önleme Amaçlı Denetlenmesi Tedbirinin Uygulanması

1. Tedbirin Yerine Getirilmesi

Telekomünikasyon yoluyla yapılan iletişimin denetlenmesinin, TİB tarafından yürütüleceği hükme bağlanmıştır. Nitekim hem PVSK ve Jandarma Kanunu hem de MİT Kanunu, iletişimin denetlenmesi işlemlerinin TİB tarafından yürütüleceğini benimsemektedir. Bu bağlamda, hakim tarafından verilen kararların ve yetkili merciin verdiği yazılı emirlerin uygulanması TİB tarafından yerine getirilecektir. Uygulamada hakim tarafından verilen iletişimin denetlenmesine dair karar TİB’e ulaştıktan sonra, TİB’teki görevliler tarafından bu kararın hukuka uygunluğu incelenmektedir. Burada esas itibarıyla, karar veya yazılı emirde bulunması gereken bilgilerin varlığı gibi, 5397 sayılı Kanun’da öngörülen usul ve esaslara uyulup uyulmadığına dair bir inceleme söz konusudur.

⁸⁵¹ MİT Kanunu’nun 6. maddesinin 4. fıkrasına 5651 sayılı Kanun’un 12/4 maddesiyle eklenen ibare, 04/05/2007 tarihli 5651 sayılı Kanun, Resmi Gazete No. 26530, Resmi Gazete Tarihi: 23/05/2007.

⁸⁵² Kunter, Yenisey, Nuhoglu, a.g.e., s. 52.

Uygulamada incelenen temel iki husus, tedbirin süresi ve önlenmesi amaçlanan suçlardan birine dair iletişimin denetlenmesi kararı verilmiş olup olmadığı şeklinde karşımıza çıkmaktadır. TİB ile denetimi gerçekleştirebilecek olan Polis, Jandarma ve MİT arasında ortak bir ara bağlantı bulunmaktadır. Bu nedenle, karar hukuka uygun ise ve TİB herhangi bir itirazda bulunmuyorsa, bu bağlantı yoluyla ilgili kolluk görevlilerine iletişim açılır ve onların sesi duyması sağlanır. İlgili kolluk görevlilerinin aidiyet numaraları bulunmaktadır.⁸⁵³ Bu nedenle de aslında tedbirin sonlandırılması da, daha sonra görüleceği gibi, TİB tarafından gerçekleştirilir.

2009 yılında TİB Yönetmeliği'nde yapılan değişiklikle, hakim kararları ve yazılı emirler ile bunların içeriğinin, Başkanlığın belirleyeceği şekilde elektronik ortamda ilgili kurumlar tarafından Başkanlığa gönderileceği kabul edilmiştir. Kararlar ve TİB Yönetmeliği'ne uygun olan yazılı emirler ise, ilgili kurum görevlilerince TİB'in koordine ve nezaretinde uygulanır.⁸⁵⁴ TİB'de Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve MİT'ten temsilciler bulunmaktadır⁸⁵⁵ ve fiilen denetimin ilgili kurum görevlilerince yapıldığı ifade edilebilir.⁸⁵⁶ Gecikmesinde sakınca bulunan hallerde yetkili mercii tarafından yazılı emir verilebileceğini daha önce belirtmiştik. Tedbirin uygulanabilmesi ve sürecin devam edebilmesi için, yirmi dört saat içinde yetkili ve görevli hakimın bu emri onaylaması gerekmektedir. Nitekim sürenin dolması veya hakim tarafından aksine karar verilmesi halinde, tedbirin derhal kaldırılacağı kabul edilmiştir. Tedbirin bu şekilde kaldırılması durumunda, dinlemenin içeriğine ilişkin kayıtların en geç on gün içinde yok edilmesi ve durumun bir tutanakla tespit olunarak; bu tutanağın da denetimde ibraz edilmek üzere saklanması öngörülmüştür.⁸⁵⁷

TİB'de sadece Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve MİT'in ilgili birimlerinden birer temsilci değil, aynı zamanda verilen görevleri yerine

⁸⁵³ “Dinleme Yapılmıyor”, Bilgi ve İletişim Teknolojileri Dünyası, (Çevrimiçi) <http://www.bitdunyasi.com/tr/?Sayfa=Detay&Id=1447>, 30 Ocak 2012.

⁸⁵⁴ TİB Yönetmeliği m. 10.

⁸⁵⁵ 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi.

⁸⁵⁶ Kunter, Yenisey, Nuhoglu, a.g.e., s. 39.

⁸⁵⁷ 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi.

getirmek üzere yeteri kadar da personel bulunmaktadır.⁸⁵⁸ TİB Yönetmeliği'nde yer alan işlemlerle ilgili olarak, Emniyet Genel Müdürlüğünün kendi birimlerindeki işlemlerine ilişkin denetimi sıralı kurum amirleri, Emniyet Genel Müdürlüğü ve İçişleri Bakanlığının teftiş elemanları tarafından; Jandarma Genel Komutanlığının kendi birimlerindeki işlemlerine ilişkin denetimi sıralı kurum amirleri, Jandarma Genel Komutanlığı ve İçişleri Bakanlığının teftiş elemanları tarafından yapılır. MİT Müsteşarlığının kendi birimlerindeki işlemlerine ilişkin denetiminin ise sıralı kurum amirleri, Başbakanlık teftiş elemanları tarafından yapılacağı kabul edilmiştir.⁸⁵⁹

Hakim kararları ile yazılı emirler hakkındaki gelişmeler ilgili kurum tarafından derhal Başkanlığa bildirilir. Bu husus, iletişimin adli amaçlı denetlenmesi durumunda da başka şekilde önem kazanabilir. Yapılan denetime dair soruşturma ve kovuşturma makamlarına bilgi verilmesi şeklinde kendini gösterebilir. Nitekim A.B.D.'de bu bağlamda denetimle ulaşılmak istenen amaca erişme ve devam eden denetimin gerekliliğine dair ilgili hakimın bilgilendirilmesinin istenebileceği öngörülmüştür.⁸⁶⁰

2. Gizlilik

Gizlilik iletişimin adli amaçlı denetlenmesinde olduğu gibi, önleme amaçlı denetiminde de benimsenen esaslı ilkelerden biri olarak karşımıza çıkmaktadır. Fakat kanımızca iletişimin denetlenmesinin her türü bakımından titizlikle güvence altına alınması gereken bu ilkeye dair düzenlemeler açısından, önleme amaçlı denetimi düzenleyen hükümler belirsizliğe daha fazla imkan verecek şekilde düzenlenmiştir. Öncelikle adli amaçlı denetimin gerçekleştirilmesi bakımından, CMK'da açıkça, alınan karar ve yapılan işlemlerin tedbir süresince gizli tutulacağı hükme bağlanmıştır.⁸⁶¹ 5397 sayılı Kanun ve bu bağlamda PYSK, Jandarma Kanunu ve MİT Kanunu da gizliliği güvence altına almakta ve fakat yürütülen faaliyetler sonucu elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik ilkesinin geçerli

⁸⁵⁸ 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi.

⁸⁵⁹ TİB Yönetmeliği m. 24.

⁸⁶⁰ The Wiretap Act, 18 USCS §2518 (6).

⁸⁶¹ CMK m. 135/5.

olduğunu hükme bağlamaktadırlar.⁸⁶² Bu nedenle, tedbirin uygulanması sırasında da gizliliğin geçerli olup olmayacağı açıkça düzenlenmemiş olmaktadır. Bu noktada, uygulanan tedbirin niteliği ve müdahale ettiği temel hak ve özgürlük de dikkate alındığında, tedbirin uygulanmasına dair işlemler sırasında gizlilik, iletişimin adli amaçlı denetiminde olduğu gibi önleme denetlemesinde de korunması gereken bir ilke olarak kabul edilmelidir.

İletişimin denetlenmesine dair işlemler ile elde edilen bilgi ve kayıtlar gizliliği korunması gereken hususlar olduğundan, bu ilkenin ayrı bir önem ve nitelikle kendini göstermesi gerekmektedir. Örneğin iletişimin adli amaçlı denetimi açısından, sadece şüpheli veya sanık değil, müdafii de tedbirden haberdar olmamalıdır. İletişimin denetlenmesi tedbiri söz konusu olduğunda gizliliğin herkese karşı olduğu kabul edilmelidir. Kolluk görevlilerinin elde ettikleri bilgiyi mülki amirlerle paylaşımları ise, emniyet ve asayişe dair bilgiyi mülki amirlere bildirme yükümlülüğü bağlamında, gizliliğin ihlali olarak görülmeyebilir.⁸⁶³ Gizliliğin ihlal edilmesi durumunda, TCK bağlamında, haberleşmenin gizliliğini ihlal,⁸⁶⁴ gizliliğin ihlali⁸⁶⁵ ve göreve ilişkin sırrın açıklanması⁸⁶⁶ hükümlerine dayanılarak cezai sorumluluğun söz konusu olması gerektiği de ileri sürülmüştür.⁸⁶⁷

C. Tedbire Son Verilmesi

İletişimin denetlenmesinin, öncelikle tedbir süresinin sona ermesiyle biteceği düşünülebilir. Nitekim iletişimin adli amaçlı denetlenmesine olduğu gibi, önleme amaçlı denetimine de belli süreler için karar verilebildiği göz önüne alındığında, tedbir için belirlenen sürenin dolmasıyla, tedbirin de sona ereceği kabul edilmelidir.

⁸⁶² 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu'nun 6. maddesi.

⁸⁶³ Emniyet ve Asayiş İşlerinde İl, İlçe ve Bucaklardaki Jandarma ve Emniyet Ödevlerinin Yapılması ve Yetkilerinin Kullanılması Suretini ve Aralarındaki Münasebetleri Gösterir Yönetmelik m. 4/a-2.

⁸⁶⁴ TCK m. 132.

⁸⁶⁵ TCK m. 285.

⁸⁶⁶ TCK m. 258.

⁸⁶⁷ Şen, a.g.e., s. 148.

Bunun dışında, iletişimin önleme amaçlı denetimi açısından,⁸⁶⁸ yazılı emir hakkında hakim tarafından aksine karar verilmesi ile yazılı emrin hakim tarafından 24 saat içinde onaylanmaması ve koşulların ortadan kalkması, tedbirin uygulanmasının sona ermesi olarak değerlendirilebilir.⁸⁶⁹ Tedbirin sona ermesi TİB tarafından gerçekleştirilmektedir.

İletişimin önleme amaçlı denetimi açısından gecikmesinde sakınca olan hallerde yetkili mercii yazılı emriyle telekomünikasyon yoluyla yapılan iletişimin denetlenmesi mümkündür.⁸⁷⁰ Bu durumda tedbirin uygulanmaya devam etmesi için yetkili ve görevli hakim en geç 24 saat içinde emri onaylaması gerekmektedir. Hakimin bu emri onaylamaması durumunda tedbir derhal kaldırılacak ve böylece uygulanmasına son verilmiş olacaktır. Bunun yanı sıra unutulmamalıdır ki, yazılı emrin yetkili mercii tarafından 24 saat içinde hakim onayına sunulması ve hakim de 24 saat içinde bu emri onaylaması gerekmektedir. Bu nedenle, gecikmesinde sakınca bulunan halde yetkili mercii yazılı emriyle iletişimin denetlenmesine başlanmış ve fakat 24 saat içinde hakim onayına sunulmamışsa veya sunulmuş ve hakim 24 saatlik karar verme sürecinde kararını vermemişse, tedbirin uygulanmasına son verilecektir.⁸⁷¹

Kısacası, yazılı emrin yerine getirilmesiyle iletişimin denetlenmesine başlanmışsa, gerekli süre içinde hakim onayının alınıp alınmadığı belirlenmeli ve alınmadığı durumda tedbirin derhal kaldırılması gerekmektedir. Uygulamada, TİB tarafından genellikle 48 saat iletişimin denetlenebilmesi için sisteme tanımlama yapıldığından, bu süre sonunda hakim onayı alınmamış ve TİB'e ulaştırılmamışsa, TİB tarafından iletişimin denetlenmesi işlemi sona erdirilmektedir.

⁸⁶⁸ İletişimin adli amaçlı denetlenmesi tedbirinin sona ermesi halleri, önleme amaçlı denetimden farklı olarak, şüpheli hakkında kovuşturmayaya yer olmadığına dair karar verilmesi, Cumhuriyet savcısının kararının hakim tarafından onaylanmaması ve koşulların ortadan kalkması olarak ortaya çıkmaktadır, CMK m. 137/1, 3.

⁸⁶⁹ TİB Yönetmeliği m. 11.

⁸⁷⁰ Bu mercii polis açısından, Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanı; jandarma açısından, Jandarma Genel Komutanı veya istihbarat başkanı ve MİT açısından da MİT Müsteşarı veya yardımcısıdır.

⁸⁷¹ 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 6. maddesi; TİB Yönetmeliği m. 11/2.

İletişimin önleme amaçlı denetlenmesinin uygulanmasına son verilmesine dair diğer husus, denetimin uygulanmasına ilişkin koşulların ortadan kalkması olarak ifade edilebilir. Nitekim 5397 sayılı Kanun'da ve TİB Yönetmeliği'nde "uygulanen tedbirin sona ermesi" kavramıyla, tedbirin sona ermesine ilişkin diğer nedenlerin kastedildiği düşünülebilir. Suç işleme ihtimali olduğu düşünülen kişinin ölmesi, önlenmesi amaçlanan suçun ilgili yasal düzenlemede suç olmaktan çıkarılması ve iletişimin denetlenmesi yerine başka bir yolun uygulanmasıyla beklenen sonuca ulaşma imkanının ortaya çıkması gibi hususlar tedbirin uygulanmasına ilişkin koşulların ortadan kalkmasına örnek olarak gösterilebilir.⁸⁷² Bunun dışında, önlenmeye çalışılan suç işlendikten sonra da, iletişimin önleme amaçlı denetimine son verilmesi gerekmektedir. Kaldı ki, böyle bir durumda önleme amaçlı denetime devam edilmesinin, hukuka aykırı bir denetim ve elde edilen bilginin de ceza yargılamasında değerlendirilememesi sonucunu doğuracağı söylenebilir.⁸⁷³

İletişimin denetlenmesine ilişkin koşulların ortadan kalkması hususunda, esas olarak, tedbire gerek kalmadığı durumlara vurgu yapıldığını düşünmekteyiz. Nitekim burada, iletişimin denetlenmesi tedbirinin uygulanmasına ilişkin bir süre belirlenmiş olmasına rağmen, süre dolmadan, bu işlemin uygulanmasına dair koşullardan birinin ortadan kalkması halinde tedbirin uygulanmasına son verilmesi söz konusudur. Bu bağlamda, tedbire artık gerek kalmadığı durumda, tedbire son verilmesi gerektiği düşünülebilir. Tedbire son verilmesi açısından, tedbire karar verilmesinde olduğu gibi hakimden ayrıca bir karar alınmasının aranmadığı görülmektedir.⁸⁷⁴ Kaldı ki, iletişimin adli amaçlı denetlenmesi açısından, iletişimin denetlenmesi tedbirine Cumhuriyet savcısı tarafından son verileceği ifade edilirken,⁸⁷⁵ önleme amaçlı denetim açısından böyle bir hükmün de düzenleme altına alınmadığı söylenebilir.

⁸⁷² Öztürk ve diğerleri, **a.g.e.**, s. 475; Taşkın, **a.g.e.**, s. 223.

⁸⁷³ Kaymaz, **a.g.e.**, s. 495.

⁸⁷⁴ Öztürk ve diğerleri, **a.g.e.**, s. 475; Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 60.

⁸⁷⁵ CMK m. 137/3.

D. Kayıtların Yok Edilmesi

Gerek 5397 sayılı Kanun gerek TİB Yönetmeliği iletişimin denetlenmesi tedbirine son verilmesi hususundan sonra kayıtların yok edilmesini düzenlemektedir.⁸⁷⁶ Bu bağlamda, yetkili mercii tarafından verilen yazılı emir hakkında hakim tarafından aksine karar verilmesi, tedbirin koşulların ortadan kalkması durumunda sona ermesi veya yazılı emir hakkında hakimden 24 saat içinde onay alınmaması nedeniyle iletişimin denetlenmesi uygulamasına son verilmesi durumunda kayıtların yok edilmesi açısından bir farklılık yaratılmadığı söylenebilir. Buna göre, dinlemenin içeriğine ilişkin kayıtların ilgili kurumların en üst amirinin ve bu kayıtların TİB’de tutuluyorsa TİB Başkanlığında denetimi altında en geç on gün içinde yok edileceği kabul edilmektedir. Kayıtların, bu kayıtları tutan ilgili kurum tarafından yok edileceği anlaşılmaktadır.⁸⁷⁷

Uygulanan tedbirin sona ermesi halinde kayıtların yok edilmesine ilişkin usulü 5397 sayılı Kanun ve TİB Yönetmeliği, dinlemenin içeriğine ilişkin kayıtlar kavramı üzerinden yapmaktadır. Kanımızca bu kanun ve yönetmeliğin karar veya yazılı emrin uygulanması ve kayıtların yok edilmesi hususlarını, iletişimin denetlenmesi türleri bakımından bir ayrım yapmayarak hükme bağladığı da göz önünde bulundurulduğunda, böyle bir düzenleme belirsizlik yaratmaktadır. Nitekim iletişimin dinlenmesi bu bağlamda uygulanacak denetleme türlerinden sadece biridir. Fakat düzenleme, yok edilecek kayıtların sadece iletişimin dinlenmesine mi yoksa tüm denetim türlerine mi ilişkin kayıtlar olduğu konusunda açık değildir.

Kayıtların yok edilmesi usulünün, tedbirin sona ermesinden sonra yer alması ve tedbirin sona ermesi bakımından da denetim türleri arasında bir ayrım yapılmadığı dikkate alınırsa, kanımızca, burada da sadece iletişimin dinlenmesine ilişkin kayıtların yok edilmesinin hükme bağlandığı sonucuna açıkça varılamamaktadır.

⁸⁷⁶ 5397 sayılı Kanun m. 1-3; 2559 sayılı Polis Vazife ve Salahiyet Kanunu’nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu’nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu’nun 6. maddesi; TİB Yönetmeliği m. 11/3.

⁸⁷⁷ İletişimin adli amaçlı denetiminde, tespit veya dinlemeye ilişkin kayıtların Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edileceğinin düzenlendiği görülmektedir, CMK m. 137/3; İletişimin Denetlenmesi Yönetmeliği m. 13.

Fakat uygulamanın, sadece dinlemeye ilişkin kayıtları yok eden bir yaklaşımı olduğu da söylenebilir. Örneğin iletişimin tespitine dair kayıtların ilgili kurumda veya TİB’de belli bir süre saklanacağına dair bir düzenlemeyle karşılaşmamaktayız. Fakat iletişimin dinlenmesine ilişkin kayıtlar, tedbirin sona ermesinden sonra yok edilmesine rağmen; iletişimin tespitine dair kayıtlar TİB’de tutulmaktadır. Kişinin telefon görüşmesini nerede yaptığına dair anlık yer bilgisi gibi sinyal bilgilerine dair kayıtlar da uygulamada, iletişimin tespiti gibi değerlendirilmekte ve kayıtlar tutulmaktadır. İletişimin adli amaçlı denetimi bakımından ise, İletişimin Denetlenmesi Yönetmeliği’nde, iletişimin tespitine yönelik verilerin ceza muhakemesinde kullanılmak üzere TCK’da belirlenen dava zaman aşımı hükümleri dikkate alınmak suretiyle Başkanlıkça arşivleneceğinin hükme bağlandığı görülmektedir.⁸⁷⁸

Uygulanan tedbire ilişkin kayıtların ilgili kurumlarda ve TİB’de tutulduğu söylenebilir.⁸⁷⁹ Bu ilgili kurumun üst amiri ve TİB’de tutulmuşsa, TİB Başkanı’nın da denetimi altında kayıtlar yok edildikten sonra durum, denetimlerde sunulmak üzere saklanacak olan bir tutanakla tespit olunacaktır.⁸⁸⁰

İletişimin denetlenmesi tedbirinin uygulanmasıyla elde edilen kayıtların yok edilmesine ilişkin açık yasal düzenlemelerin yapılması yerinde olacaktır. Nitekim birtakım belirsizliklerin varlığına rağmen, yok edilmesi gereken kayıtların tutulması, gereğinden fazla tutulması ve böylece amaç dışı kullanımı gibi durumlar, hem iletişimin denetlenmesi hem de bu süreç açısından özel yaşamın gizliliği ile kişisel verilerin korunması hakkının özünü etkileyebilecek sonuçlar yaratabilecektir. AİHM’nin de genel olarak kayıtların yok edilmesine ve özellikle de tedbirin uygulanmasına dair şartların ortadan kalkması durumunda kayıtların yok edilmesine

⁸⁷⁸ İletişimin Denetlenmesi Yönetmeliği m. 9/3.

⁸⁷⁹ TİB Yönetmeliği’nin 11. maddesinin ilk hali “dinlemenin içeriğine ilişkin kayıtların Başkanın ve ilgili kurumların en üst amirinin denetimi altında en geç on gün içinde yok edilir” şeklinde düzenlenmişti, 10/11/2005 tarihli 25989 numaralı Resmi Gazete’de yayımlanan TİB Yönetmeliği.

⁸⁸⁰ 2559 sayılı Polis Vazife ve Salahiyet Kanunu’nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu’nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu’nun 6. maddesi; TİB Yönetmeliği m. 11/3.

dair yasal düzenlemelerin olması gerektiğini vurguladığı görülmektedir.⁸⁸¹ Kaldı ki, yetkili makamların bu işlemi gerçekleştirmelerine ilişkin olarak yetkilerini kullanmalarına yönelik mevzuatın, amaç ve kapsamının makul bir açıklıkta düzenlenmesi gerektiğini; böyle bir yasal güvencenin olmamasının hem AİHS'nin 8. maddesini hem de demokratik bir devlette hukukun üstünlüğünü ihlal ettiği kabul edilmiştir.⁸⁸²

III. TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN ÖNLEME AMAÇLI DENETLENMESİ SONUCU ELDE EDİLEN VERİLERİN NİTELİĞİ ve KULLANIMI

Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sonucu elde edilen verilerin niteliği, iletişimin adli ve önleme amaçlı denetlenmesi arasındaki en temel farklılıklardan biri olarak kendini gösterir. İletişimin adli amaçlı denetimi sonucu elde edilen bilgiler delil⁸⁸³ niteliği taşırken; önleme amaçlı denetlenmesi sonucu elde edilen bilgiler delil olarak kullanılamaz.⁸⁸⁴ Kaldı ki, kısaca değinmek gerekirse, adli amaçlı denetim sonucu elde edilen delilin ispat değeri ve tek başına mahkumiyete esas teşkil edip etmediği konusunda da genel itibariyle farklı iki görüşün olduğu söylenebilir. Öncelikle şunu belirtmeliyiz ki, elde edilen delillerin genel itibariyle belirti delili sayılması kabul edilmektedir. Burada da belirti delilinin olayın dolaylı olarak ispatına yarayan niteliğinden yola çıkılarak; tek başına ispat kuvvetinin olmadığı ve somut ve yan delillerle desteklenmesi gerektiği ifade edilmektedir.⁸⁸⁵

⁸⁸¹ Case of Kruslin v. France, para 35, 36; Case of Huvig v. France, para 34, 35.

⁸⁸² Case of Kruslin v. France, para 35, 36; Case of Huvig v. France, para 34, 35.

⁸⁸³ Delil genel itibariyle hukuk düzeninin kabul ettiği, ispata yarayan araç olarak ifade edilebilir. İspat ise “filin fail tarafından işlendiği veya işlenmediği konusunda hukuk düzenince kabul edilen araçlarla, yargılama makamının tam bir kanaate ulaşmasını sağlama işi olarak nitelendirilebilir”, Öztürk ve diğerleri, **a.g.e.**, s. 351 vd.; Özbek ve diğerleri, **a.g.e.**, s. 637 vd.

⁸⁸⁴ Şahin, **a.g.e.**, s. 270; Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 61; Özbek ve diğerleri, **a.g.e.**, s. 181, 183.

⁸⁸⁵ Özbek ve diğerleri, **a.g.e.**, s. 617; Öztürk ve diğerleri, **a.g.e.**, s. 353 vd.; Şen, **a.g.e.**, s. 165-171. Elde edilen delilin somut ve yan delillerle desteklenerek mahkumiyete esas teşkil edecek olmasının önemi Şen tarafından şöyle bir örnekle ifade edilmiştir: Bir telefon dinlemesinde fail suçunu ikrar etmiş ve kasten insan öldürme suçunda ceset ve silaha ulaşılmışsa somut delillerle desteklendiği kabul edilebilir ve cezalandırmak için yeterli görülebilir. Fakat ortada maddi delil olmadan örneğin ihaleye fesat karıştırma beyanına dayanan sadece konuşma kayıtları söz konusu ise destekleyici, somut delillerin aranması gerekmektedir, Şen, **a.g.e.**, s. 169, 170.

Bu görüşün Anayasa Mahkemesi'nin ses kayıtlarının tek başına delil olarak değerlendirilemeyeceğine dair kararıyla, birebir aynı yönde olmasa da, paralellik gösterdiği söylenebilir. Anayasa Mahkemesi ilgili kararında, iletişimin dinlenmesi ve konuşulanların kaydedilmesi değil; birtakım toplantılarda gizlice oluşturulan ses bantlarından bahsetmektedir. Mahkeme burada, başkaca pekiştirici kanıtlar bulunmadan sadece ses bantlarının ispat değeri olmadığını ve böylece yapılan bir suç isnadının hukuk devletinde yerinde olmadığını hükme bağlamıştır.⁸⁸⁶ Mahkeme'ye göre, "ses alma alanındaki ilerleme ve gelişmeler bugün o evrededir ki bir sesin belirli bir kişiye ilişkin bulunduğu hala parmak izlerinde olduğu gibi kuşkusuzca ve kesinlikle saptanamamasına karşılık birtakım montaj yollarıyla ve gerekirse ses taklit etmede usta kişilerin yardımlarından da yararlanılarak bantlar istenildiği gibi doldurulabilmektedir. Bir toplantıda hazır bulunanlar, zamanında ve usulünce tutanaklarla saptanarak o toplantıya ilişkin bulunduğu ileri sürülen ses bantlarına böylece destek ve güç kazandırılmadıkça bant çevirilerine hukuk yönünden tam bir güvenle bağlanıp dayanılamayacağı ortadadır. Öte yandan MİT ajanının toplantılara katılması halinde bunun fezlekele açıkça gösterilmesi yolu tutulduğuna göre yalnız ses bandından söz edilince o toplantıda ajanın bulunmadığı sonucu çıkmaktadır. Ankara'da Osman Köksal'ın da katılmasıyla Cemal Reşit Eyüboğlu'nun evinde beş kez, (İ)lhami Soysal'ın bürosunda üç kez ve Doğan Avcıoğlu'nun bürosunda bir kez yapıldığı ileri sürülen dokuz toplantıda MİT Elemanı'nın yer aldığı belirtilmediğine göre bu ev ve bürolarda daha önceden yerleştirilen ses alma araçları bulunduğu izlenimi uyanmaktadır. Buralara araçların kimlerce, ne vakit, nasıl yerleştirildiği, nasıl uzun bir zaman korunup çalıştırılabildiği, konuşanların kimliklerinin ve banda çekilmiş seslerle ilişkilerinin ne yolla saptandığı bilinmediği için bu durum ses bantlarının isnada ciddilik verme gücünü daha da gölgelemektedir. (...) Yukarıdan beri açıklananlarla varılan sonuç şudur: Başkaca inandırıcı ve pekiştirici kanıtlar bulunmadıkça yalnızca ses bantlarının ve gizli ajan raporlarının, bir yurttaşta yapılan "Türkiye Cumhuriyeti Anayasasını teğyir ve tebdile ve bu yasa ile kurulmuş Türkiye Büyük Millet Meclisini iskata veya görevini yapmaktan men'e cebren teşebbüs

⁸⁸⁶ E. 1971/41, K. 1971/67, K.t. 17/08/1971.

gayesiyle gizlice ittifak kurmak" gibi çok ağır bir isnada yasama dokunulmazlığının kaldırılması yönünden ciddilik kazandırabilmesi bir hukuk (d)evletinde düşünülemez.”⁸⁸⁷ Telefon görüşmeleri kayıtlarına dair ise Yargıtay, elde edilen bilginin tek başına, somut delillere ulaşılmadan mahkumiyete esas teşkil etmeyeceğini ifade etmiştir.⁸⁸⁸

Bunun dışında, iletişimin denetlenmesinden elde edilen kayıt üzerinde tahrifat olup olmadığına ve denetimin türüne göre bir değerlendirme yapılması gerektiğini dile getiren görüşler de bulunmaktadır.⁸⁸⁹ Bu bağlamda, hukuka uygun olarak elde edilmiş, üzerinde değişiklik yapılmamış⁸⁹⁰ ve yine usulüne uygun olarak korunmuş kayıtlar delil olarak kabul edilebilir.⁸⁹¹ Bunun dışında denetimin türü açısından ayırım yapan görüş de bulunmaktadır. Buna göre, iletişimin tespiti sonucu elde edilen bilginin belirti, iletişimin dinlenmesinde iletişimi dinleyen görevlinin tanık olarak kabul edilmesi gerekmektedir. İletişimin kaydı sonucu elde edilen bilginin belirti olarak keşif yöntemi ile duruşmada ortaya konulması ve sinyal bilgilerinin değerlendirilmesi sonucu elde edilen bilginin ise dolaylı ispat aracı olarak kullanılması da bu görüş çerçevesinde ileri sürülmektedir.⁸⁹²

Şu ana kadar iletişimin adli amaçlı denetlenmesi sonucu elde edilen bilginin delil niteliği ve her şeyden önce mahkumiyete esas teşkil edip edemeyeceği değerlendirmelerine şu farkındalıkla değinmeye çalıştık: İletişimin önleme amaçlı denetlenmesinde bir soruşturma ve kovuşturmadan bahsetmemekteyiz. Kaldı ki, 5397 sayılı Kanun gerek Polis gerek Jandarma ve gerekse MİT bakımından yürütülen faaliyetler çerçevesinde elde edilen kayıtların, yasada belirtilen amaçlar dışında

⁸⁸⁷ E. 1971/41, K. 1971/67, K.t. 17/08/1971.

⁸⁸⁸ Yargıtay bu kararında, “sanıkların üzerine atılı suç işlediklerine dair, savunmalarının aksine, içeriği maddi bulgularla desteklenemeyen telefon görüşmelerine dayalı iletişim kayıtları dışında cezalandırılmalarına yeter kesin ve inandırıcı delil elde edilemediği, sanıkların üzerlerinde ve evlerinde yapılan aramalarda herhangi bir suç unsuruna rastlanmadığı gözetilmeden, atılı suçtan beraatları yerine yazılı şekilde kabul edilerek ceza tayin edilmesi”ni bozmuştur, E. 2008/13862, K. 2009/479, K.t. 22.01.2009.

⁸⁸⁹ Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 61, 62.

⁸⁹⁰ Üzerinde değişiklik yapılmış kayıt esas itibariyle hukuka aykırı delil olarak da kabul edilebilecektir, Şen, **a.g.e.**, s. 170.

⁸⁹¹ Öztürk ve diğerleri, **a.g.e.**, s. 353 vd.

⁸⁹² Kunter, Yenisey, Nuhoglu, **a.g.e.**, s. 61.

kullanılamayacağını hükme bağlamaktadır. Bu bakımından, iletişimin önleme amaçlı denetlenmesi sonucu elde edilen bilginin suç işlenmesinin önlenmesi amacıyla kullanılması gerektiği kabul edilmeli ve böyle bir bilginin bir soruşturma veya kovuşturmada doğrudan kullanılması yerinde görülmemelidir. Böyle bir bilgi, adli amaçlı denetim sonucu elde edilen delilden bu yönleriyle farkı olsa da, yapılan değerlendirmelerle bazı temel hususlarda paralellikler kurulabilir.

Öncelikle iletişimin önleme amaçlı denetimi sonucu elde edilen bilginin açıkça, öngörülen suçların işlenmesinin önlenmesinden başka amaçla kullanılamayacak olmasının delil olarak kullanılmamayı da kapsadığı ifade edilebilir. Bu tür bilgilerin delile götüren bilgi olarak nitelendirilebileceği de ileri sürülmüştür.⁸⁹³ Kaldı ki, iletişimin önleme amaçlı denetlenmesi sırasında, kişinin bir başka suçu örneğin bir kişiyi öldürdüğü dinlenilir ve kaydedilirse de iletişimi denetleyen görevlinin ne yapacağı konusunda bir açıklık bulunmamaktadır. Adli amaçlı denetim açısından, böyle bir durumun ikrar sayılacağı ve fakat ikrarın da delillere ilişkin diğer belirlemelerde olduğu gibi, somut ve yan delillerle desteklenerek kanıtlanmasının aranması gerektiği ifade edilmektedir.⁸⁹⁴ Başka bir ifadeyle, böyle bir bilginin mahkeme dışı ikrar olarak nitelendirilerek, mahkumiyete esas teşkil etmek için maddi ve yan delillerle doğrulanması gerektiği kabul edilmektedir.⁸⁹⁵ Önleme amaçlı denetim bakımından da böyle bir bilginin ne şekilde kullanılıp kullanılamayacağı değerlendirilebilir. Bu bilginin hiç kullanılmamasının iletişimi denetleyen yetkili kişinin TCK bağlamında sorumluluğunun doğmasına neden olacağı dahi düşünülebilir. Nitekim TCK'nın işlenmekte olan bir suçu bildirmeyen bir kişiye veya kamu adına soruşturma ve kovuşturmayı gerektiren bir suçun işlendiğini göreviyle bağlantılı olarak öğrenip de yetkili makamlara bildirmeyen kamu görevlisine dair düzenlemesi bu bağlamda değerlendirilebilir.⁸⁹⁶

⁸⁹³ Taşkın, *a.g.e.*, s. 227-229.

⁸⁹⁴ Böyle bir telefon dinlemesinde suç ikrar edilmiş ve kasten insan öldürme suçunda ceset ve silaha ulaşılmışsa somut delillerle desteklendiği kabul edilebilir ve cezalandırmak için yeterli görülebilir denmiştir, Şen, *a.g.e.*, s. 170.

⁸⁹⁵ Kayseri 2. Ağır Ceza Mahkemesi'nin 16.03.2007 tarih, E. 2006/290, K. 2007/85 numaralı kararı, aktaran, Şen, *a.g.e.*, s. 172.

⁸⁹⁶ TCK'nın 279. maddesine göre, kamu adına soruşturma ve kovuşturmayı gerektiren bir suçun işlendiğini göreviyle bağlantılı olarak öğrenip de yetkili makamlara bildirimde bulunmayı ihmal eden veya bu hususta gecikme gösteren kamu görevlisi, altı aydan iki yıla kadar hapis cezası ile

Tüm bunlar göz önünde bulundurulduğunda, iletişimin önleme amaçlı denetimi sonucu elde edilen bilginin, hükme esas teşkil etmeyecek olmakla birlikte, soruşturma ve kovuşturma aşamaları açısından şüphe (ve hatta basit/başlangıç şüphesi)⁸⁹⁷ kavramının oluşmasında ve böylece belirli koruma tedbirlerinin uygulanabilmesinde kullanılabileceği düşünülebilir. Bu konuda önleme amaçlı denetim sonucu elde edilen bilginin, arama gibi makul şüphenin arandığı koruma tedbirlerinin uygulanmasına imkan tanınması örnek olarak düşünülebilir. Nitekim “şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerlerin, yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa aranabileceği” düzenlenmiştir, CMK m. 116/1. Görülüyor ki, aranan makul şüphe, suçun işlendiğine dair değildir; aranacak yerlerde, yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa tedbirin uygulanması öngörülmektedir. Diğer bir değerlendirmeyle ve bir adım daha ileri giderek, somut ve maddi delillerle desteklenerek, CMK bağlamında iletişimin denetlenmesine başvurabilmek için aranan, suç işlendiğine yönelik kuvvetli şüphe sebeplerinin bulunmasına dair şartın gerçekleşmesinde kullanılabileceği de ifade edilmektedir.⁸⁹⁸ Fakat kanımızca bu şekilde, hukukumuzda yeterli açıklıkta ve ayrıntılı olarak düzenlenmemiş olan iletişimin önleme amaçlı denetimi, adli amaçlı denetime geçiş için bir araç olarak kullanılma tehlikesi yaratabilir. Nitekim önleme amaçlı denetim sonucu elde edilen bilgiye dair yapılacak değerlendirmeler, elde edilen bilginin delil olarak kullanılamayacağı ve yargılamada hükme esas teşkil etmeyeceği hususuna aykırılık teşkil etmemelidir. Kaldı ki, bu denetim türünün istisnai olduğu ve özel yaşamın gizliliği ve haberleşme özgürlüğü ile yakın ilişkisi dikkate alınarak da bu esasları göz önünde bulunduracak bir yasal düzenleme gerekliliğinden de söz edilebilir.

cezalandırılır. Suçun, adli kolluk görevini yapan kişi tarafından işlenmesi halinde, yukarıdaki fıkraya göre verilecek ceza yarı oranında artırılır.”

⁸⁹⁷ Öztürk, basit şüpheyi/başlangıç şüphesini, “dayandığı deliller basit, yetersiz ve/veya sayıca az olan şüphedir. Soruşturmaya başlanabilmesi için, belli ve yaşanmış somut olayların, en azından belirti şeklinde ortada bulunan delillerin belli bir suçun işlendiği yolunda bir şüphe ortaya koyması şarttır. Belirli olaylara ve belirti şeklindeki delillere dayanmayan ve sadece tahminden ibaret bulunan şüphe soruşturmaya başlanabilmesi için yeterli değildir; yeterli sayılırsa keyfiliğin önlenmesi mümkün olmaz.” şeklinde açıklamaktadır, Öztürk ve diğerleri, **a.g.e.**, s. 380.

⁸⁹⁸ Şen, bu yönde ayrıca, elde edilen kayıtların ceza soruşturmasına dayanak teşkil edebileceği konusunda bir tereddütün bulunmadığını dile getirmektedir, Şen, **a.g.e.**, s. 75.

IV. HUKUKA AYKIRI OLARAK TELEKOMÜNİKASYON YOLUYLA YAPILAN İLETİŞİMİN ÖNLEME AMAÇLI DENETLENMESİ VE YAPTIRIMI

A. Hukuka Aykırılık

Telekomünikasyon yoluyla yapılan iletişimin, 5397 sayılı Kanun çerçevesinde düzenlenen koşulları taşımayan şekilde denetlenmesinin hukuka aykırı sayılacağı ifade edilebilir. Kaldı ki, sadece dinlemeler kavramı kullanılmış olsa da, 5397 sayılı Kanun Polis, Jandarma ve MİT için geçerli olacak şekilde, belirlenen usul ve esaslara aykırı dinlemelerin hukuken geçerli sayılmayacağını hükme bağlamaktadır. İletişimin önleme amaçlı denetlenmesinin hukuka aykırı gerçekleştirilmesi sonucu elde edilen bilgiyle, örneğin kuvvetli suç şüphesi yarattığı iddiasıyla iletişimin adli amaçlı denetlenmesi gibi bir tedbire karar verilmemesi gerektiği söylenebilir. İletişimin denetlenmesinde hukuka aykırılık tartışmasını belirsiz kılan hususlar genel itibarıyla iki açıdan incelenebilir: Birincisi, hakkında iletişimin denetlenmesi kararı bulunmayan üçüncü kişiler arasında gerçekleşen iletişimin denetlenmesi; diğeri de, iletişimin denetlenmesi sırasında ve fakat önlenmesi amaçlanan suçla değil de, başka bir suçla ilgili olarak bilgi edinilmesi.

İlk olarak, hakkında iletişimin denetlenmesi kararı bulunmayan üçüncü kişiler arasında gerçekleşen iletişimin denetlenmesi ile ilgili olarak özellikle iletişimin dinlenmesi açısından, dinlemeye konu olan telefonun ilgili kişi dışında başka bir kişi adına kayıtlı olması ve böylece haklarında dinleme kararı olmayan üçüncü kişilerin dinlenmesi ihtimali düşünülebilir. Böyle bir durumda, 5397 sayılı Kanun'un tedbirin uygulanabilmesi için öngördüğü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespiti imkan veren kodundan belirlenebilenlerin hakim kararında veya yazılı emirde yer alması gerekliliği hatırlanmalıdır. Nitekim ilgili kişi hakkında telefon numarası belirtilerek iletişimin denetlenmesi kararı verilmiş olmasına rağmen, bu telefonu kullanan ve hakkında iletişimin denetlenmesi kararı bulunmayan üçüncü kişinin

yaptığı konuşmanın dinlenmesi ve/veya kaydedilmesi hukuka aykırı kabul edilmelidir.⁸⁹⁹

Diğer hukuka aykırılık tartışması olan denetim sonucu önlenmesi amaçlanan suçla değil de, başka bir suçla ilgili olan bilgi edinilmesi açısından ise, elde edilen bilginin niteliği ve iletişimin denetlenmesine devam edilip edilmemesi gerektiği değerlendirilebilir. Bu şekilde adeta tesadüfen elde edilen bilgi, önlenmesi amaçlanan suçlardan biriyle ilgili ise, önleme amaçlı denetime devam edebilmek için ayrı bir hakim kararına ihtiyaç olduğu kabul edilmelidir. Bu ihtimali bir adım daha ileri götürerek, iletişimin önleme amaçlı denetimine başlayıp, belirli bilgiler edinildikten sonra adli amaçlı denetim yapılabilmesine dayanak teşkil edecek koşullar oluşmadan adli amaçlı denetime geçiş yapılmasının da hukuka uygun görülmemesi gerektiği söylenebilir.⁹⁰⁰ Aksi takdirde, temel hak ve özgürlüğü sınırlayan ve son çare olarak uygulanması gereken böyle bir tedbirin, kişiler için hukuki güvenceyi zedeleyecek şekilde kullanılmasına olanak tanınmış olur. Ayrıca adli amaçlı denetime nazaran daha hafif koşulları öngören önleme amaçlı denetimin hukuka aykırı kullanımına açık olarak imkan verilmiş olur.

CMK’da, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ve ancak 135. maddede belirtilen suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilmesi durumunda bu delilin muhafaza altına alınacağını ve durumun Cumhuriyet

⁸⁹⁹ Yargıtay’ın bu konuda ilgili bir kararı bulunmaktadır. Bu kararda Yüksek Mahkeme, hakkında iletişimin dinlenmesi kararı olmayan üçüncü kişilerin iletişiminin dinlendiği belirlemesini yapmakta ve fakat bu durumun hukuka aykırılığına açıkça değinmemiştir. Kararda genel itibarıyla, böyle bir iletişimin dinlenmesi sonucu tesadüfen elde edildiği kabul edilen suç kanıtının değerlendirilebilmesi incelenmiştir. Yargıtay’a göre, “dosyada kanıt olarak kabul edilen 22.03.2004 tarihli konuşmanın tutanakları incelendiğinde, bu görüşmenin haklarında dinleme kararı bulunmayan üçüncü kişiler arasında geçtiği açıktır. Bu konuşmada tesadüfen elde edildiği kabul edilen suç kanıtının değerlendirilebilmesi için 4422 sayılı Yasada herhangi bir hüküm yer almadığı gözetildiğinde, bu konuşma tutanağı yasa dışı elde edilmiş kanıt niteliğindedir. Kaldı ki, 5271 sayılı CMY’nın 138. maddesine göre de bu tutanağa yasal bir kanıt değeri verilmesi olanaksızdır. Zira, tesadüfen elde edilen bu kanıt, görevde yetkiyi kötüye kullanma suçu ile ilgili olup, bu suç 135. maddede sayılan katalog suçlar arasında yer almadığından, yasa dışı elde edilmiş kanıt niteliğindedir. Yasa dışı elde edilen bir kanıtın ise soruşturma ve kovuşturma aşamalarında kullanılmasına olanak bulunmamaktadır.” Ceza Genel Kurulu, E. 2006/4.MD-122, K. 2006/162.

⁹⁰⁰ Şen, a.g.e., s. 76, 77.

Savcılığına bildirileceğinin düzenlendiği görülmektedir.⁹⁰¹ Tesadüfen elde edilen deliller başlıklı böyle bir düzenleme ile önleme amaçlı denetim sırasında adeta tesadüfen elde edilebilecek bilgiler arasında tam bir benzerlik veya paralellik kurmamaktayız. Her şeyden önce, önleme amaçlı denetim sonucu elde edilen bilginin delil niteliğinde kabul edilemeyeceği açıktır. Fakat iletişimin önleme amaçlı denetlenmesi açısından da, denetim sırasında önlenmesi amaçlanan suç dışında bir suç ile ilgili bilgi edinilmesi durumunda ne olacağına dair bir düzenleme yapılması gerektiğini düşünmekteyiz.

İletişimin belli bir suçun önlenmesi amaçlı denetimi sırasında, elde edinilen bilgi 5397 sayılı Kanun kapsamında bir suça ilişkin ise, iletişime devam edilmeden ayrı bir hakim kararının aranması düşünülebilir. Bu şekilde elde edilen bilginin, önleme amaçlı denetimle önlenmesi amaçlanan suçlardan biri ile ilgili olmasa da, kanımızca yine delil olarak değil, fakat bir soruşturma için basit/başlangıç şüphesi⁹⁰² olarak kullanılabilmesinin mümkün olduğu düşünülebilir.

B. Tazminat

1. Genel Olarak

İletişimin önleme amaçlı denetimi, uygulanması için hakim kararını gerektiren; suçun önlenmesine ilişkin idari bir faaliyet olarak karşımıza çıkmaktadır. Bu yönüyle, idare hukuku hükümlerine tabi bir sorumluluk anlayışından söz edebiliriz.⁹⁰³ Nitekim 1982 Anayasası'nın kişinin, resmi görevliler tarafından

⁹⁰¹ CMK m. 138/2.

⁹⁰² Öztürk ve diğerleri, *a.g.e.*, s. 486 vd.

⁹⁰³ Ceza hukuku ve ceza yargılaması açısından da, önleyici kolluk faaliyeti ve hazırlık hareketi, icra hareketi ayrımına bu bağlamda değinilebilir. Şen'e göre, suçun icra hareketleri başlamadan, daha hazırlık hareketleri aşamasında adli kolluk değil, idari kolluk yetkili olacak ve önleyici kolluk olarak faaliyette bulunabilecektir. Hazırlık hareketleri ile icra hareketleri arasındaki ayrımı yapmak, fail için ceza sorumluluğunun hangi anda başladığını belirlemek bakımından önemlidir. Failin hareketi suçun hazırlık hareketi ise, bu hareketten dolayı ceza sorumluluğu doğmayacak, fakat hareket suçun icra hareketlerinden sayılmakta ise, bu hareket sebebiyle failin en azından suça teşebbüs ettiğinden bahisle ceza sorumluluğu gündeme gelecektir.", Şen, *a.g.e.*, 15. dn., s. 68.

gerçekleştirilen haksız işlemler sonucu uğradığı zararın, kanuna göre, Devletçe tazmin edileceğini ve Devletin sorumlu olan ilgili görevliye rücu hakkının saklı olduğunu öngören 40/3. maddesi bu bağlamda düşünülebilir. Bunun yanı sıra, yine 1982 Anayasası'nın idarenin kendi eylem ve işlemlerinden doğan zararı ödemekle yükümlü olduğunu hükme bağlayan 125/7. maddesi ve memurlar ve diğer kamu görevlilerinin yetkilerini kullanırken işledikleri kusurlardan doğan tazminat davalarının, kendilerine rücu edilmek kaydıyla ve kanunun gösterdiği şekil ve şartlara uygun olarak idare aleyhine açılabilceğini güvence altına alan 129/5. maddesine göre de idarenin sorumluluğu göz önünde bulundurulabilir. Denetim kararını veren hakimın kararının yargısal bir faaliyet olduğu dikkate alındığında hakimın sorumluluğu açısından, Hukuk Muhakemeleri Kanunu (HMK)'nın hakimlerin sorumluluğunu düzenleyen 46 vd. maddelerinin göz önünde bulundurulması gerektiği söylenebilir.⁹⁰⁴ Gecikmesinde sakınca bulunan halde, yetkili merciin verdiği yazılı emrin ise, idarenin kamu gücü ayrıcalıklarıyla gerçekleştirdiği bir idari faaliyet olduğu ve idari sorumluluğu doğurduğu ifade edilebilir. Nitekim idari sorumluluk, idarenin kamu hukukuna tabi bir faaliyeti sonucu ortaya çıkan bir sorumluluk olarak nitelendirilebilir. Böyle bir sorumluluğun varlığı halinde, idarenin kişilere verdiği zarar idari yargıda ve kamu hukuku kurallarına göre tazmin edilir.⁹⁰⁵

2. İdarenin ve Kamu Görevlilerinin Sorumluluğu

Telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetiminde idarenin sorumluluğu açısından, kural olarak kusura dayanan bir sorumluluktan söz ettiğimiz dikkate alınır, üç sorumluluk halini değerlendirebiliriz: (i) salt kişisel kusur halleri,⁹⁰⁶ (ii) hizmetle ilişkisi kesilemeyen kişisel kusur halleri⁹⁰⁷ ve (iii) hizmet

⁹⁰⁴ 12/01/2011 tarihli, 6100 sayılı Hukuk Muhakemeleri Kanunu, Resmi Gazete No. 27836, Resmi Gazete tarihi: 04/02/2011. HMK'nın 46. maddesinin ilk fıkrası, hakimlerin yargılama faaliyetlerinden dolayı belirli sebeplere dayanılarak Devlet aleyhine tazminat davası açılabilceğini hükme bağlamaktadır.

⁹⁰⁵ İl Han Özay, *Günüşiğinde Yönetim*, İstanbul, Alfa, 2002, s. 731-740, 758-762, 762-764; Kemal Gözler, Gürsel Kaplan, *İdare Hukuku Dersleri*, 11. baskıdan tıpkı ek baskı, Bursa, Ekim, 2011, s. 745, 746.

⁹⁰⁶ Özay, a.g.e., s. 762, 763.

kusurunun bulunduğu haller.⁹⁰⁸ Kişisel kusur genel itibariyle kamu görevlilerinin ifasından ayrılabilir nitelikte olan kusurlardır. Kişisel kusur da kendi içinde üç şekilde görülebilir. Buna göre, kişisel kusur halleri hizmetle hiçbir bağlantısı olmayan, görevin tamamen dışındaki kusurlar; görevin içinde işlenmekle birlikte, ağır nitelikteki kusurlar; görevin ifası dışında ve fakat görev dolayısıyla, görevden tamamen kopuk olmayan kusurlar olarak sayılabilir.⁹⁰⁹

İletişimin önleme amaçlı denetlenmesi bakımından, görevlinin görevinin dışında, kendi sağladığı birtakım araçlarla iletişimin denetlenmesini gerçekleştirmesi örneği düşünülebilir. Bu şekildeki salt kişisel kusur halinde, idarenin değil; genel hükümler bağlamında görevlinin sorumluluğu söz konusu olabilecektir. Konumuz bakımından kişisel kusura ilişkin bu ayrım bağlamında asıl üzerinde durduğumuz diğer kişisel kusur hali ise, görevin ifası dışında ve fakat görev dolayısıyla, görevden tamamen kopuk olmayan - hizmet ve şahsi kusurun birleşmesi olarak ortaya çıkan - kusur halidir.⁹¹⁰ Burada, kamu görevlisinin görevinin icrası ile ilgili olarak düzenlemelerde belirlenen görev ve yetki alanını aşarak ve idarenin kendine verdiği araçlar sayesinde gerçekleştirdiği kusurlu davranışı bulunmaktadır. Bu durumda kural olarak, hem idarenin hem de kamu görevlisinin zarardan sorumlu olacağı düşünülebilir.⁹¹¹

İletişimin önleme amaçlı denetimi açısından diğer kusur hali ise, hizmet kusuru olarak nitelendirilebilir. Hizmet kusurunda kamu görevlisinin kusurlu davranışı, hizmetten ayrılmaz niteliktedir.⁹¹² İletişimin önleme amaçlı denetlenmesi açısından, hakim kararı mevcut olsa da, ülkede yaşayan bütün insanların suç işleme ihtimalinin

⁹⁰⁷ Özay, a.g.e., s. 758-762.

⁹⁰⁸ Özay, a.g.e., s. 753-758; Gözler, Kaplan, a.g.e., s. 753, 754.

⁹⁰⁹ Gözler, Kaplan, a.g.e., s. 754, 755.

⁹¹⁰ 1602 sayılı Askeri Yüksek İdare Mahkemesi Kanunu - 2568 sayılı Kanun'la 1981 yılında değişmiş - 24. maddesinde hizmet ve şahsi kusurun birleşmesi başlıklı bir düzenlemeye yer vermiştir. 1602 sayılı 04/07/1972 tarihli Askeri Yüksek İdare Mahkemesi Kanunu, Resmi Gazete No. 14251, Resmi Gazete tarihi: 20/07/1972.

⁹¹¹ Özay, a.g.e., s. 758-762; Gözler, Kaplan, a.g.e., s. 755.

⁹¹² Özay, a.g.e., s. 731-735; Gözler, Kaplan, a.g.e., s. 753, 754.

varolduğundan yola çıkarak, ülke genelini kapsayacak şekilde yetki verilmesinin hizmet kusurunun işlendiği bir hal olarak kabul edilebilmesi mümkündür.⁹¹³

Hakim kararı veya gecikmesinde sakınca bulunan halde yetkili merciin yazılı emri olmadan gerçekleştirilecek iletişimin denetlenmesi söz konusu olduğunda, ilgili görevlinin kişisel kusurundan söz edilebileceği açıktır. Fakat Türk hukuku bakımından, görevlinin kişisel kusurunun bulunması durumunda idare de, hizmet kusurlu olarak kabul edilmektedir. Kaldı ki, 1982 Anayasası'nın 129. maddesi ve 657 sayılı Devlet Memurları Kanunu'nun 13. maddesi de dikkate alındığında, zarar görene karşı idarenin sorumluluğu esası oluşturmaktadır.⁹¹⁴ Aslında bu şekilde, hizmet ve kişisel kusurun birleşmesi dahi değil; idarenin tek başına sorumluluğunun öngörüldüğü söylenebilir.⁹¹⁵

3. Ceza Hukuku Açısından Sorumluluk

Hukuka aykırı olarak gerçekleştirilen iletişimin denetlenmesi açısından, ilgili görevlilerin suç teşkil eden davranışları dolayısıyla ceza sorumluluğu söz konusu olabilecektir. Nitekim iletişimin denetlenmesi açısından öngörülen usul ve esaslara aykırılık sadece hakimın kararı alınmadan veya gecikmesinde sakınca bulunan halde yetkili mercinin yazılı emri olmadan gerçekleştirilen iletişimin denetlenmesi durumunda ortaya çıkmamaktadır. Diğer ilke ve esasların da böyle bir hukuka aykırılık yaratabileceği açıktır. Örneğin, iletişimin denetlenmesi sonucu elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik ilkesine uyulmayarak; bunların açıklanması da hukuka aykırılık olarak kabul edilmelidir. Bunun yanı sıra,

⁹¹³ Yargıtay'ın E. 2008/874, K. 2008/7160, K.t. 04/06/200, ülke genelini kapsayacak şekilde iletişimin denetlenmesi yetkisi verilmek suretiyle iletişimin denetlenmesine dair kararı bu bağlamda değerlendirilebilir.

⁹¹⁴ 1982 Anayasası'nın 129. maddesi, memurlar ve diğer kamu görevlilerinin yetkilerini kullanırken işledikleri kusurlardan doğan tazminat davalarının, kendilerine rücu edilmek kaydıyla ve kanunun gösterdiği şekil ve şartlara uygun olarak, ancak idare aleyhine açılabilmesini kabul etmiştir. 657 sayılı Devlet Memurları Kanunu'nun 13. maddesi ise, kişilerin kamu hukukuna tabi görevlerle ilgili olarak uğradıkları zararlardan dolayı bu görevleri yerine getiren personel aleyhine değil, ilgili kurum aleyhine dava açabileceklerini düzenlemektedir. 657 sayılı 14/07/1965 tarihli Devlet Memurları Kanunu, Resmi Gazete No. 12056, Resmi Gazete tarihi: 23/07/1965.

⁹¹⁵ 1982 Anayasası'nın 129/5. maddesi ve 129/657 sayılı Devlet Memurları Kanunu'nun 13/2. maddesi.

iletişimin denetlenmesine dair sürenin bitmesine rağmen, denetime devam edilmesinin de aynı şekilde ilgili görevliler açısından cezai sorumluluk yaratacağı düşünülebilir.⁹¹⁶

5397 sayılı Kanun, iletişimin önleme amaçlı denetimi çerçevesinde elde edilen kayıtların suçun önlenmesi amacı dışında kullanılmasında ve elde edilen bilgi ve kayıtların saklanması ve korunmasında görev sırasında veya görevden dolayı gizlilik ilkesine uymayan yetkililer açısından, Cumhuriyet savcılarınca doğrudan soruşturma yapılacağını kabul etmektedir. TCK'da, haberleşmenin gizliliğini ihlal;⁹¹⁷ özel hayatın gizliliğini ihlal;⁹¹⁸ kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleme veya bunları bir ses alma cihazıyla kaydetme⁹¹⁹ ve kişisel verilerin kaydedilmesi⁹²⁰ yaptırıma bağlanmıştır. TCK'nın 137. maddesi ise, bu suçların kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılarak işlenmesi durumunda cezanın yarı oranında artırılacağını öngörmektedir. Burada şu belirtilmelidir ki, TCK'nın 133. maddesiyle düzenlenen konuşmaların gizlice dinlenmesi ve kayda alınmasının, telekomünikasyon yoluyla yapılan iletişim yerine, genel itibarıyla sözlü iletişim veya karşılıklı konuşmanın denetlenmesi şeklinde değerlendirilmesi beklenmektedir.⁹²¹

⁹¹⁶ Hakeri, Ünver, a.g.e., s. 248, 249; Şen, a.g.e., s. 192, 193.

⁹¹⁷ TCK m. 132. maddesine göre, “kişiler arasındaki haberleşmenin gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu gizlilik ihlâli haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur.”

⁹¹⁸ TCK'nın 134. maddesi, “kişilerin özel hayatının gizliliğini ihlal eden kimsenin, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılacağını” hükme bağladığı gibi; “gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlâl edilmesi halinde, cezanın alt sınırının bir yıldan az olamayacağını” da düzenlemektedir.

⁹¹⁹ Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, TCK'nın 133. maddesine göre, iki aydan altı aya kadar hapis cezası ile cezalandırılacaktır.

⁹²⁰ TCK m. 135. maddesi sadece kişisel verilerin hukuka aykırı olarak kaydedilmesini cezalandırmamış; aynı zamanda hassas verilere ilişkin de bir düzenleme öngörmüştür. Buna göre, “kişilerin siyasi, felsefi veya dini görüşlerine; ırkî kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.”

⁹²¹ Karşılıklı yapılan konuşmaların - A.B.D. hukukunda ifade edildiği şekliyle, oral communications - gizlice kayıt edilmesi sorunu ile ilgili ayrıntılı bilgi için bkz.: Kunter, Yenisey, Nuhoglu, a.g.e., s. 65, 66.

Telekomünikasyon yoluyla yapılan iletişimin denetlenmesinde öngörülen ve 5397 sayılı Kanun'da da güvence altına alınan gizlilik ilkesi bakımından TCK'nın göreve ilişkin sırrın açıklanmasına dair 258. maddesi de dikkate alınabilir. Elde edilen bilgi ve kayıtların özellikle saklanması ve korunmasında uyulması gereken bu ilkeye aykırılık, yetkili görevlinin sorumluluğuna yol açabilecektir.⁹²²

4. İdari Denetim

İletişimin önleme amaçlı denetlenmesi bağlamında taleplerin TİB Yönetmeliği'ne ve diğer ilgili düzenlemelere uygun olup olmadığını incelemek ve gerektiğinde yetkili mercilere başvuruda bulunmak, TİB'in görevleri arasında bulunmaktadır.⁹²³ Polis, Jandarma ve MİT'in, bir başka anlatımla iletişimin denetlenmesini gerçekleştiren birimlerin işlemlerine ilişkin denetim yetkisi TİB'de değildir. Zira Emniyet Genel Müdürlüğü'nün TİB Yönetmeliği'nde yer alan faaliyetlerle alakalı kendi birimlerindeki işlemlerine ilişkin denetimi, sıralı kurum amirleri, Emniyet Genel Müdürlüğü ve İçişleri Bakanlığının teftiş elemanları; Jandarma Genel Komutanlığının bu tür işlemlerine ilişkin denetimi, sıralı kurum amirleri, Jandarma Genel Komutanlığı ve İçişleri Bakanlığının teftiş elemanları; MİT Müsteşarlığının bu işlemlerine ilişkin denetimi ise, sıralı kurum amirleri, Başbakanlık teftiş elemanları tarafından yapılacaktır.⁹²⁴ TİB'in, TİB Yönetmeliği'nde düzenlenen faaliyetlerle ilgili denetiminin, Başbakanın özel olarak yetkilendireceği kişi veya komisyon tarafından yapılacağına dair düzenlemenin 2009 yılında kaldırıldığı⁹²⁵ ve fakat denetime dair yukarıda belirtilen kurum amirlerinin denetim yetkisinin korunduğu görülmektedir. Uygulamada da TİB'in, sistemi ilgili kolluk birimlerine açtıktan

⁹²² "Görevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği ve gizli kalması gereken belgeleri, kararları ve emirleri ve diğer tebligatı açıklayan veya yayımlayan veya ne suretle olursa olsun başkalarının bilgi edinmesini kolaylaştıran kamu görevlisine, bir yıldan dört yıla kadar hapis cezası verilebileceği" TCK'nın 258/1. maddesinde güvence altına alınmıştır.

⁹²³ TİB Yönetmeliği m. 17/c. Bu bağlamda, TİB Yönetmeliği'nin 5/son, 6/son ve 7/son maddeleri de göz önünde bulundurulabilir.

⁹²⁴ TİB Yönetmeliği m. 24.

⁹²⁵ TİB Yönetmeliği'nde 2009 yılında yapılan değişiklik için bkz.: 7/8/2009 tarihli, 27312 numaralı Resmi Gazete.

sonra, denetimin yapıldığı sürede ilgili bu birimleri denetleme gibi bir faaliyeti olmamaktadır.

Genel olarak iletişimin hukuka aykırı denetlenmesine dair düzenleme eksikliği ve özel olarak da önleme amaçlı denetimin Türk hukuku bakımından kolay sağlanabilecek koşullarla özel yaşamın ve iletişimin gizliliği hakkına ağır bir müdahale yaratabileceği dikkate alındığında, TİB Yönetmeliği ve ilgili mevzuat çerçevesindeki faaliyetlerin, bağımsız ve tedbirin niteliğiyle bağdaşır yetkilere sahip kişi veya kişilerce yapılmasının sağlanması gerektiği açıktır. Nitekim telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesi, uygulanması açısından belirli ilkelerin sadece düzenlenmesini değil, özenle uyulmasını da zorunlu kılan bir tedbir türüdür.

SONUÇ

Özel yaşamın gizliliği hakkı, genel itibariyle kişilerin, kendilerine ait bilgiyi ne zaman, ne şekilde ve hangi kapsamda başkalarıyla paylaşacaklarını belirleyebilmelerine ilişkin taleplerinin korunması olarak ortaya çıkmaktadır. Bu hakkın korunmasıyla asıl çaba sarfedilen ise, hakkın koruduğu - kişisel bağımsızlık, duygusal çözülme, sınırlı ve korunaklı iletişim ile kişisel karar alabilme serbestliği - değerlerin güvence altına alınmasıdır. Özel yaşamın gizliliğine iletişimin denetlenmesi yoluyla yapılan müdahalelerin hakkın hukuka aykırı sınırlanması sonucunu doğurmamasına, hakkın koruduğu bu değerler veya işlevler göz önünde bulundurularak özen gösterilmelidir. Önleme amaçlı denetim de, iletişimin adli amaçlı denetimi gibi gizli gerçekleştirilmektedir. Fakat adli amaçlı denetimden farklı olarak, elde edilen bilgi herhangi bir ceza yargılamasında da kullanılamayacağından, iletişimi denetlenen kişinin belki de hiçbir zaman bu müdahaleden haberdar olmaması gibi bir sonuç da doğurabilecektir. Kaldı ki, önleme amaçlı denetim, ortada herhangi bir suç, şüpheli veya sanık olmadığı durumda uygulanmaktadır. Bu nedenle, iletişimin önleme amaçlı denetimi açısından, özel yaşamın gizliliğini oluşturan esaslı değer ve işlevlerin korunmasının önemi bir kez daha ortaya çıkmaktadır.

Kıta Avrupası ve Anglo Sakson hukuku anlayışları arasındaki - Kıta Avrupasının düzenlemeci, Anglo Sakson hukukunun içtihadı yaklaşımı - farklılığın, özel yaşamın ve iletişimin gizliliği haklarına iletişimin denetlenmesi yoluyla müdahale edilmesine dair düzenlemelerde de kendini gösterdiği söylenebilir. Fakat bununla birlikte, iki hukuk anlayışının da, küçük düzenleme farklılıklarıyla da olsa konuya korumacı yaklaştığı görülebilir. Nitekim Avrupa Birliği mevzuatı, kişisel bilginin korunması bağlamında hareket ederken; A.B.D. hukuku ise makul özel yaşam beklentisi çerçevesinde özel yaşamın kapsamının belirlenmesi üzerine yoğunlaşmaktadır.

Türk hukuku bakımından, özellikle önleme amaçlı iletişimin denetlenmesi ve bu denetimin özel yaşamın ve iletişimin gizliliği bağlamında düzenlenmesi oldukça yenidir. Türk hukuku bakımından, kişisel verilerin korunması hususunun Avrupa Birliği mevzuatı dayanak alınarak oluşturulduğu söylenebilir. Kişisel verilerin

korunması ile ilgili řu an yürürlükte veya tasarı halinde olan düzenlemeler, Türk hukukunda telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetimi dolayısıyla elde edilen bilgilere yönelik yeterli korumayı sağlamamaktadır. Bu nedenle, özellikle oluşturulacak yeni düzenlemelerde bu bilgilerin kişisel veri niteliğı kabul edilmeli ve böylece kişisel verilerin korunması güvencelerinden yararlanılması sağlanmalıdır. Zira bu güvencelerden yararlanılması durumunda kişisel verinin işlenebilmesi için ilgili kişinin rızasının aranması ve bilgilendirilmesi, verinin işlenmesi sırasında veriye ulaşma, veriyi düzeltme, silme, veriye ulaşmayı engelleme ve itiraz hakkının korunması gibi ilkeler sadece denetim sonucunda elde edilen bilgiler değerlendirilirken değıl; denetimin uygulandığı sırada da göz önünde bulundurulacaktır.

Yeni oluşturulan mevzuatta iletişimin denetlenmesine dair ilkelerin ise, hem Avrupa hem de A.B.D. yaklaşımındaki ortak ilkelerle düzenlendiğı görölmektedir. Buna göre, ayrı bir yasal düzenlemeyle, hakim kararı zorunlu kılınarak, belirli bir süre için iletişimin denetlenebileceğı öngörölmüştür. Fakat 5397 sayılı Kanun bu temel unsurları güvence altına almış olsa da, AİHM'nin de üzerinde durduğı bir temel hak ve özgürlüğü sınırlayan yasanın açıklık ve öngörülebilirlik gibi unsurlarını her yönüyle eksiksiz karşılamamaktadır.

Her şeyden önce, 5397 sayılı Kanun'daki, iletişimin denetlenmesine dair hakim kararında veya yazılı emirde tedbir uygulanacak kişinin kimliğı, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespiti imkan veren kodundan “belirlenebilenler”in bulunması hükmü yeniden düzenlenmelidir. Bu düzenleme yapılırken, 5397 sayılı Kanun'un bir temel hak ve özgürlüğün sınırlanmasına dayanak teşkil eden bir yasa olarak gerekli güvenceyi sağlama ve yasallık ilkesini tam olarak karşılama zorunluluğı göz önünde bulundurulmalıdır. Böylece bu bilgilerden sadece birinin, örneğın telefon numarasının belirlenmesinin dahi denetim faaliyetinin yapılmasına karar verilmesi için yeterli olabileceğı anlayışı terkedilerek; bilgilerin tümünün belirtilmesi aranmalıdır. Nitekim adli amaçlı denetime nazaran, önleme amaçlı denetimin uygulanmasının çok daha kolay şartlara bağlanması gerektiğı genel kabulü de değışmelidir. Zira önleme amaçlı denetim, adli

amaçlı denetime nazaran özel yaşamın ve iletişimin gizliliğine daha az müdahale oluşturmamakta; aksine ilgili hak ve özgürlüklerin daha ağır ihlallerine neden olabilmektedir.

5397 sayılı Kanun, ayrıca, denetimin uygulanması kararı vermek üzere, hakimın bir makul neden incelemesi ortaya koymasını da öngöreceğ şekilde düzenlenmeli ve herkesin, her durumda iletişiminin denetlenebileceğı ve böylece özel yaşamının gizliliğinin ihlal edilebileceğı anlayışı ortadan kaldırılmalıdır. Bununla birlikte, iletişimin denetlenmesinin sadece dinleme olmadığı göz önünde bulundurularak, denetimin her türü - iletişimin dinlenmesi, kaydedilmesi, tespiti ve sinyal bilgilerinin kaydedilmesi - aynı hassasiyet ve fakat kendine özgü koşullar dikkate alınarak düzenlenmelidir. Örneğın, iletişimin denetlenmesi sonucu elde edilen ve kişisel veri niteliğinde kabul edilebilecek olan bilgilerin yok edilmesine dair usul ve güvenceler açıkça düzenlenmelidir.

Özel yaşamın ve iletişimin gizliliğı hakkının ihlali sonucunu doğurabilecek başlıca tedbirlerden biri olan önleme amaçlı iletişimin denetlenmesi, temel hak ve özgürlüklerin sınırlandırılmasına dair Türk anayasa hukuku ve AİHM anlayışı da dikkate alınarak değerlendirilmelidir. Telekomünikasyon yoluyla yapılan iletişimin önleme amaçlı denetlenmesine dair hukuki yaklaşım, özel yaşamın gizliliğı hakkını daha az zedeleyecek başkaca bir yol bulunmaması durumunda bu tedbire başvurulabileceğı esası temel alınarak yeniden şekillenmelidir.

KAYNAKÇA

KİTAP VE MAKALELER

- Agre, Philip E.: “Beyond the Mirror World: Privacy and the Representational Practices of Computing”, **Privacy and the Representation Technology and Privacy: The New Landscape**, Ed. by. Philip E. Agre, Marc Rotenberg, London, England, The MIT Press, 1997.
- Allen, Anita L.: “Coercing Privacy,” **William and Mary Law Review**, C.XL.III, 1999, (Çevrimiçi) <http://go.galegroup.com.ezp-prod1.hul.harvard.edu>, 2 Ekim 2011.
- Allen, Anita L.: “Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm,” **Conn L. Rev.** C.XXXII, 1999-2000, s. 861-875.
- Allen, Anita L.: “Coercing Privacy,” **William and Mary Law Review**, C. XL.III, Mart 1999.
- Arpacı, Abdülkadir: **Kişiler Hukuku (Gerçek Kişiler)**, İstanbul, Beta, 2. bs., 2000.
- Arsava, A. Füsün: “Avrupa Temel Haklar Şartı,” **Ankara Avrupa Çalışmaları Dergisi**, C.V, No: 1, 2005.
- Arslan Öncü, Gülay: **Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması Hakkı**, İstanbul, Beta, 2011.

Artuk, Mehmet Emin, Gökçen, Ahmet
Yenidünya, Caner A.:

Ceza Hukuku Genel Hükümler, 5. bs.
Ankara, Turhan, 2011.

Asinari, Maria Veronica Perez:

“Legal Constraints for the Protection of
Privacy and Personal Data in Electronic
Evidence Handling,” **International
Review of Law Computers &
Technology**, C.XVIII, No:2, Temmuz
2004, s. 231-250.

Bainbridge, David:

Data Protection, Great Britain, CLT
Professional Publishing, 2000.

Başalp, Nilgün:

**Kişisel Verilerin Korunması ve
Saklanması**, Ankara, Yetkin, 2004.

Barendt, Eric:

“Privacy and Freedom of Speech”, **New
Dimensions in Privacy Law:
International and Comparative
Perspectives**, Ed. by. Andrew T.
Kenyon, Megan Richardson, UK,
Cambridge University, 2006.

Bates, Alan:

“Privacy - A Useful Concept,” **Soc. F.**,
C.XLII, 1963-1964.

Bell, Robert SK, Ray, Neil:

EU Electronic Communications Law,
UK, Richmond, 2004.

Bellia, Patricia L.:

“Surveillance Law Through Cyberlaw’s
Lens,” **George Washington Law
Review**, C.LXXII, 2003-2004, s. 1375-
1458.

- Bennett, Colin J.: **Regulating Privacy: Data Protection and Public Policy in Europe and the United States**, USA, Cornell University, 1992.
- Bezanson, Randall P.: "The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990," **California Law Review**, C.LXXX, Ekim 1992, s. 1133-1175.
- Bezanson, Randall P.: "Privacy, Personality, and Social Norms," **Case Western Reserve Law Review**, C.XLI, 1990-1991, s. 681-687.
- Bignami, Francesca: "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining," **Boston College Law Review**, C.XLVIII, 2007, s. 609-698.
- Blousten, Edward: **Privacy as an Aspect of Human Dignity**, Aktaran Daniel J. Solove, USA, Harvard University Press, 2008.
- Booth, Sharon, Jenkins, Richard, Moxon, David, Semmens, Natasha, Spencer, Christopher, Taylor, Mark, Townend, David: **What are Personal Data: A Study Conducted for the UK Information Commissioner**, The University of Sheffield, 2004.
- Cammilleri-Subrenat, Anne, Levallois-Barth, Claire: **Sensitive Data Protection in the European Union**, Bruxelles, Bruylant, 2007.

- Carey, Peter: **E-Privacy and Online Data Protection**, UK, Butterworths Lexis Nexis, t.y.
- Cate, Fred H.: **Privacy in the Information Age**, Washington, DC, Brookings Institution, 1997.
- Cate, Fred H.: **The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It**, USA, First Amendment Center, 2003.
- Civelek Yüksel, Dilek : **Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi**, T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı, Bilgi Toplumu Dairesi Başkanlığı, Nisan 2011.
- Cohen, Julie: “Examined Lives: Informational Privacy and the Subject as Object”, Aktaran Solove, Schwartz, **Privacy, Information, and Technology**, USA, Wolters Klower, 2009.
- D’Afflitto, Rosario Imperiali: “European Union Directive on Personal Privacy Rights and Computerized Information,” **Villanova Law Review**, C.XLI, Aralık 1996, s. 305-323.
- De Burca, Grainne: “Beyond the Charter: How Enlargement Has Enlarged the Human Rights Policy of the European Union,” **Fordham International Law Journal**, C.XXVII, 2003-2004, s. 679-714.
- DeCew, Judith W.: “Review the book ‘Privacy, Intimacy, and Isolation’ by Julie Inness,” **Ethics**, C.CIV, Ekim 1993, s. 206-207.

- Diffie, Whitfield, Landau, Susan: **Privacy on the Line, The Politics of Wiretapping and Encryption**, USA, MIT Press, 2007.
- Dural, Mustafa, Ögüz, Tufan: **Türk Özel Hukuku, Cilt II, Kişiler Hukuku**, İstanbul, Filiz, 2011.
- Etzioni, Amita: **The Limits of Privacy**, USA, Basic Books, 1999.
- Farber, Daniel: "Book Review/Privacy, Intimacy, and Isolation by Julie C. Inness," **Constitutional Commentary**, C.X, 1993, s. 510-519.
- Farr, Sebastian, Oakley, Vanessa: **EU Communications Law**, 2. bs., London, Sweet&Maxwell, 2006.
- Fischer, L. Richard: **Privacy and Accuracy of Personal Information**, North Carolina Banking Institute, C.III, 1999, s. 11-29.
- Freedman, Warren: **The Right of Privacy in the Computer Age**, USA, Greenwood, 1987.
- Freiwald, Susan: "Online Surveillance: Remembering the Lessons of the Wiretap Act," **Alabama Law Review**, C.LVI, 2004-2005, s. 9-84.

- Freund, Paul: **Address at the American Law Institute, 52nd Annual Meeting, Aktaran J. Braxton Craven, Jr., "Personhood: The Right to be Let Alone," Duke L. J., C.1976, 1976.**
- Fried, Charled: **"Privacy," Yale L. J., C.LXXVII, 1967-1968, s. 475-493.**
- Gaither, Trent R.: **"The Aguilar-Spinelli Doctrine: In Requiem," Houston Law Review, C.XXI, Ekim 1984, s. 955-997.**
- Garzaniti, L.J.H.F.: **Telecommunications, Broadcasting and the Internet: EU Competition Law and Regulation, 2. bs., London, Sweet&Maxwell, 2003.**
- Gavison, Ruth: **"Privacy and the Limits of Law," The Yale Law Journal, C.LXXXIX, No: 3, 1980, s. 421-471.**
- Gellman, Robert: **"Does Privacy Law Work", Privacy and the Representation Technology and Privacy: The New Landscape, Ed. by. Philip E. Agre, Marc Rotenberg, London, England, The MIT Press, 1997.**
- Gerety, Tom: **"Redefining Privacy," Harvard Civil Rights-Civil Liberties Law Review, C.XII, No: 2, 1977, s. 233-296.**
- Godkin, E. L.: **Libel and Its Legal Remedy, Aktaran Solove, Understanding Privacy, USA, Harvard University Press, 2008.**

- Goldman, Janlori: “Privacy and Individual Empowerment in the Interactive Age”, **Privacy: New Risks and Opportunities**, Ed. by. Yves Poullet, Cecile de Terwangne, Paul Turner, Belgique, Centre de Recherches Informatique et Droit, 1997, s. 61-76.
- Gormley, Ken: “One Hundred Years of Privacy,” **Wisconsin Law Review**, C.MCMXCII, 1992, s. 1335-1441.
- Gönen, Doruk: **Tüzel Kişilerde Kişilik Hakkı ve Korunması**, İstanbul, XII Levha, 2011.
- Gözler, Kemal: **Türk Anayasa Hukuku Dersleri**, 10. bs., Bursa, Ekin, Ekim 2010.
- Gözler, Kemal, Kaplan, Gürsel: **İdare Hukuku Dersleri**, 11. baskıdan tıpkı ek baskı, Bursa, Ekim, 2011.
- Gutwirth, Serge: **Privacy and the Information Age**, Çev. Raf Casert, USA, Rowman&Littlefield, 2002.
- Hakeri, Hakan, Ünver, Yener: **Ceza Muhakemesi Hukuku Temel Bilgiler**, 6. bs., Ankara, Adalet, 2012.
- Hatemi, Hüseyin: **Gerçek Kişiler Hukuku (Kısa Ders Kitabı)**, İstanbul, Vedat, 2005.
- Helvacı, Serap: **Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar** (MK md. 24/a I/İMK md. 28a fıkra I), İstanbul, Beta, 2001.

- Hixson, Richard F.: **Privacy in a Public Society**, USA, Oxford University, 1987.
- Holtzman, David H.: **Privacy Lost, How Technology Is Endangering Your Privacy**, USA, Jossey-Bass, 2006.
- Hyatt, Michael S.: **Invasion of Privacy: How to Protect Yourself in the Digital Age**, Washington, D.C., Regnery, 2001.
- Information Commissioner's Office: **The 'Durant' Case and Its Impact on the Interpretation of the Data Protection Act 1998**.
- Information Commissioner's Office: "UK Privacy Watchdog Spearheads Debate on the Future of European Privacy Law," press release, 7 July 2008, (Çevrimçi)
http://www.ico.gov.uk/upload/documents/pressreleases/2008/ico_leads_debate_070708.pdf, 11 Aralık 2011.
- Inness, Julie C.: **Privacy, Intimacy and Isolation**, Oxford, New York, 1992.
- İçel, Kayıhan, Evik, Hakan A.: **Ceza Hukuku Genel Hükümler 2. Kitap, Suçun Yapısal Unsurları ve Özel Görünüş Şekilleri**, 4. bs., İstanbul, Beta, 2007.
- İçel, Kayıhan, Ünver, Yener: **Kitle Haberleşme Hukuku**, 8. bs., İstanbul, Beta, 2009.

- İnceoğlu, Sibel:
“ABD Anayasa Hukukunda Mahremiyet Hakkı,” **İnsan Hakları Yıllığı**, C. XIX-XX, 1997-1998, s. 173-186.
- Johnson, Jeffery L.:
“Constitutional Privacy,” **Law and Philosophy**, C.XIII, No:2, 1994.
- Kaboğlu, İbrahim Ö.:
Özgürlükler Hukuku, 6. bs., İstanbul, İmge, 2002.
- Kang, Jerry:
“Information Privacy in Cyberspace Transactions,” **Stanford Law Review**, C.L, 1997-1998, s. 1193-1294.
- Kaymaz, Seydi:
Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Ankara, Seçkin, 2009.
- Kenyon, Andrew T.
Richardson, Megan:
“New Dimensions in Privacy: Communications Technologies, Media Practices and Law”, **New Dimensions in Privacy Law: International and Comparative Perspectives**, Ed. by. Andrew T. Kenyon, Megan Richardson, UK, Cambridge University, 2006.
- Keskin, Serap:
“Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi,” **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C.LIX, No:1-2, 2001, s. 155-180.

Kilkelly, Ursula:

Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı, Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesinin Uygulanmasına İlişkin Kılavuz, İnsan Hakları El Kitapları No:1, Strasbourg, Avrupa Konseyi İnsan Hakları Genel Müdürlüğü, 2001.

Klosek, Jacqueline:

The War on Privacy, London, Praeger, 2007.

Koenig, Christian, Bartosch, Andreas, Braun, Jens-Daniel, Romes, Marion:

EC Competition and Telecommunications Law, 2. bs., the Netherlands, Kluwer Law International, 2009.

Kuner, Christopher:

European Data Protection Law, Corporate Compliance and Regulation, 2. bs., New York, Oxford, 2007.

Kunter, Nurullah, Yenisey, Feridun, Nuhoglu, Ayşe:

Muhakeme Hukuku Dahı Olarak Ceza Muhakemesi Hukuku, 17. bs., İstanbul, Beta, Nisan 2010.

Küzeci, Elif:

Kişisel Verilerin Korunması, Ankara, Turhan, 2010.

Lessig, Lawrence:

"Privacy and Attention Span," **The Georgetown Law Journal**, C.LXXXIX, 2000-2001, s. 2063-2072.

Lichtblau, Eric:

Eric Lichtblau, **Defending '03 Law, Justice Dept. Seeks Abortion Records**, The New York Times, 12 Şubat 2004.

- Livermore, Joseph M.: “The Draper-Spinelli Problem,” **Arizona Law Review**, C.XXI, 1979, s. 946-958.
- Locke, John: **Second Treatise on Government**, 1690, Aktaran Solove, **Understanding Privacy**, USA, Harvard University Press, 2008.
- Lyon, David: **Surveillance after September 11**, UK, Polity, 2008.
- Mahmutoğlu, Fatih Selami: “Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi,” **Polise Görev, Yetki ve Sorumluluk Veren Mevzuat Uygulamaları Eğitim Projesi (MUYEP) Tebliğleri - 2**, EGM Yayınları Katalog No: 444, Eğitim Dairesi Başkanlığı Yayın No: 43, 2008, Ankara, s. 405-418.
- Mahmutoğlu, Fatih Selami: “Ceza ve Ceza Yargılama Hukukunda Özel Yaşam”, **Özel Yaşamın Gizliliği Paneli**, 18 Ekim 2008, TTB Yayını 154, s. 100-109.
- Manolescu, Dan: “Data Protection as a Fundamental Right,” **Effective Justice Solutions**, Published as part of the Effectius Newsletter, Issue 5, 2010.
- McCullagh, Karen: “Protecting ‘Privacy’ through Control of ‘Personal’ Data Processing: A Flawed Approach,” **International Review of Law, Computers & Technology**, C.XXIII, No:1-2, Mart-Temmuz 2009, s. 13-24.

McMahon, Patrick J.:

Counterterrorism Technology and Privacy, Cantigny Conference Series, Conference Report, USA, McCormick Tribune Foundation, 2005.

McMurry, Julie J.:

“Privacy in the Information Age: The Need for Clarity in the ECPA,” **Washington University Law Quarterly**, C.LXXVIII, 2000, s. 597-622.

Millen, C M:

The Right to Privacy and its Natural Law Foundations in the Constitutions of the United States and Ireland, Ireland, Blackhall, 1999.

Mills, Jon L.:

Privacy: The Lost Right, New York, Oxford, 2008.

Morano-Foadi, Sonia,
Andreadakis, Stelios:

“Reflections on the Architecture of the EU after the Treaty of Lisbon: The European Judicial Approach to Fundamental Rights,” **European Law Journal**, C.XVII, No:5, Eylül 2011.

Mulligan, Deirde K.:

“Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act,” **George Washington Law Review**, C.LXXII, 2003-2004, s. 1557-1598.

Munir, Abu Bakar,
Yasin, Siti Hajar Mohd.:

Privacy and Data Protection, a Comparative Analysis with Special Reference to the Malaysian Proposed Law, Malaysia, Sweet&Maxwell, 2002.

- Murphy, Richard S.: "Property Rights in Personal Information: An Economic Defense of Privacy," **The Georgetown Law Journal**, C.LXXXIV, 1995-1996, s. 2381-2417.
- Neill, Elizabeth: **Rites of Privacy and the Privacy Trade: On the Limits of Protection for the Self**, London, McGill-Queen's University, 1984.
- Newman, Abraham L.: **Protectors of Privacy: Regulating Personal Data in the Global Economy**, USA, Cornell University, 2008.
- Northouse, Clayton: "Providing Security and Protecting Liberty", **Protecting What Matters: Technology, Security, and Liberty since 9/11**, Ed. by. Clayton Northouse, Washington, D.C., Brookings Institution, 2006, s. 3-18.
- Oder, Bertil Emrah: **Avrupa Birliği'nde Anayasa ve Anayasacılık**, İstanbul, Anahtar, 2004.
- Oğuzman, M. Kemal, Seliçi, Özer: **Kişiler Hukuku (Gerçek ve Tüzel Kişiler)**, İstanbul, Filiz, 2011
- Oliver, Wesley Macneil: "The Modern History of Probable Cause," **Tennessee Law Review**, C.LXXVIII, 2010-2011, s. 377-429.
- Ortiz, Daniel: "Privacy, Autonomy, and Consent," **Harvard Journal of Law and Public Policy**, C.XII, 1989, s. 91-97.

Özay, İl Han:

Günüşğinde Yönetim, İstanbul, Alfa, 2002.

Özbek, Veli Özer, Kanbur, M. Nihat

Doğan, Koray, Bacaksız, Pınar, Tepe, İlker: **Ceza Muhakemesi Hukuku**, 2. bs., Ankara, Seçkin, 2011.

Özbudun, Ergun:

Türk Anayasa Hukuku, Ankara, 12. bs., 2011.

Özcan, Hüseyin:

Yasama Bağışıklıkları, Ankara, Seçkin, 2006.

Öztan, Bilge:

Şahsın Hukuku, Hakiki Şahıslar, 7. bs, Ankara, Turhan, 1997.

Öztürk, Bahri, Tezcan, Durmuş,
Erdem, Mustafa Ruhan, Sırma, Özge
Saygılar, Yasemin F., Alan, Esra:

Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, Ed. by. Bahri Öztürk, 3. bs., Ankara, Seçkin, 2011.

Petronio, Sandra:

Boundaries of Privacy, Dialectics of Disclosure, New York, State University of New York Press, 2002.

Post, Robert C.:

“Rereading Warren and Brandeis: Privacy, Property, and Appropriation,” **Case Western Reserve Law Review**, C.XLI, 1990-1991, s. 647-680.

Prosser, William,:

“Privacy,” **Cal. L. Rev.**, C. XLVIII, No:3, 1960, s. 383-423.

Quinn, Michael A.:

“Criminal Procedure,” **Creighton Law Review**, C.XV, 1981.

Rachlinski, Jeffrey J., Guthrie, Chris
Wistrich, Andrew J.:

“Probable Cause, Probability, and Hindsight,” **Journal of Empirical Legal Studies**, C.VIII, 72-98, Aralık 2011.

Raines, Curtis:

Attack on Privacy, USA, Judson Press, 1974.

Rappaport, Aaron J.:

“Beyond Personhood and Autonomy: Moral Theory and the Premises of Privacy,” **Utah Law Review**, C.II, 2001, s. 441-507.

Reindenberg, Joel R.:

“E-Commerce and Trans-Atlantic Privacy,” **Houston Law Review**, C.XXXVIII, 2001-2002.

Regan, Priscilla M.:

“Privacy, Government Information, and Technology,” **Public Administration Review**, C.XLVI, No:6, Kasım-Aralık 1986.

Richards, Neil M.:

“Reviewing the Digital Person: Privacy and Technology in the Information Age by Daniel J. Solove,” **Georgetown Law Journal**, C.XCIV, Nisan 2006,

Robin, Paul H., Lenard, Thomas M.:

Privacy and the Commercial Use of Personal Information, USA, Kluwer Academic, 2002.

Rodota, Stefano:

“Beyond the EU Directive: Directions for the Future, Privacy: New Risks and Opportunities”, Ed. by. Yves Poullet, Cecile de Terwangne, Paul Turner, Belgique, Centre de Recherches Informatique et Droit, 1997.

- Rosen, Jeffrey: "Purposes of Privacy: A Response," **The Georgetown Law Journal**, C.LXXXIX, s. 2117-2137.
- Rosen, Jeffrey: "Privacy in Public Places," **Cardozo Studies in Law and Literature**, C.XII, No:1, 2000, s. 167-191.
- Rosen, Jeffrey: **The Unwanted Gaze: The Destruction of Privacy in America**, Aktaran Solove, Schwartz, **Privacy, Information, and Technology**, USA, Wolters Klower, 2009.
- Ross, Susan Dente: **Deciding Communication Law: Key Cases in Context**, New Jersey, Lawrence Eri Baum Associates, 2004.
- Roos, Megan: "Definiton of the Problem: The Impossibility of Compliance with Both European Union and United States Law," **Transnational Law & Contemporary Problems**, C.XIV, t.y.
- Saydam, Mehmet: **Ceza Muhakemesi Kanununa Göre Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi**, İstanbul, On İki Levha, 2011.
- Schachter, Madeleine: **Informational and Decisional Privacy**, USA, Carolina Academic, 2003.
- Schwartz, Paul M.: "Privacy and Democracy in Cyberspace," **Vand. L. Rev.**, C. LII, 1999, s. 1609-1702.
- Schwartz, Paul M.: "Property, Privacy, and Personal Data," **Harvard Law Review**, C.CXVII, No: 7, 2004, s. 2055-2128.

- Silverberg, Marshall H.: "Anonymus Tips, Corroboration, and Probable Cause: Reconciling the Spinelli/Draper Dichotomy in Illinois v. Gates," **American Criminal Law Review**, C.XX, 1982, s. 99-126.
- Simitis, Spiros: **Unpublished Address, Information Privacy and the Public Interest**, Annenberg Washington Program, Aktaran Fred H. Cate, **Privacy in the Information Age**, Washington, DC, Brookings Institution, 1997.
- Simitis, Spiros: "From the Market to the Polis: The EU Directive on the Protection of Personal Data," **Iowa Law Review**, C.LXXX, 1994-1995, s. 445-469.
- Slobogin, Christopher: **Privacy at Risk: The New Government Surveillance and the Fourth Amendment**, USA, The University of Chicago, 2007.
- Sokullu-Akıncı, R. Füsun: **Polis: Toplumsal Bir Kurum Olarak Gelişmesi, Polis Alt-Kültürü ve İnsan Hakları**, İstanbul, 1990.
- Solove, Daniel J., Schwartz, Paul M.: **Privacy, Information, and Technology**, 2. bs., USA, Wolters Klower, 2009.
- Solove, Daniel J., Schwartz, Paul M.: **Information Privacy Law**, 3. bs., USA, Aspen, 2009.
- Solove, Daniel J.: **Understanding Privacy**, USA, Harvard University Press, 2008.

- Sözüer, Adem: “Türkiye’de ve Karşılaştırmalı Hukukta Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi,” **İHFM**, C.LV, No:3, 1997, s. 65-110.
- Steiner, Josephine, Woods, Lorna: **EU Law**, 10. bs., New York, Oxford, 2009.
- Stratford, Jemima: “Striking the Balance: Privacy v Freedom of Expression under the European Convention on Human Rights”, **Developing Key Privacy Rights**, Ed. by. Madeleine Colvin, USA, Hart, 2002, s. 13-44.
- Street, F. Lawrence, Grant, Mark P.: **Law of the Internet**, USA, Lexis Law, 2000.
- Sykes, Charles J.: **The End of Privacy**, New York, St. Martin’s Press, 1999.
- Şahin, Cumhur: **Ceza Muhakemesi Hukuku I**, 2. bs., Ankara, Seçkin, 2011.
- Şen, Ersan: **Türk Hukuku’nda Telefon Dinleme, Gizli Soruşturmacı, X Muhabir**, 5. bs., Ankara, Seçkin, 2011.
- Şen, Ersan: “Anglo Sakson Hukukunda Özel Hayatın Gizliliği ve Korunması Hakkı,” **İstanbul Üniversitesi Mukayeseli Hukuk Araştırmaları Dergisi**, No:18, İstanbul, 1990, s. 83-88.
- Şimşek, Oğuz: **Anayasa Hukukunda Kişisel Verilerin Korunması**, İstanbul, Beta, 2008.

Tanör, Bülent, Yüzbaşıoğlu, Necmi:

1982 Anayasasına Göre Türk Anayasa Hukuku, 9. bs., İstanbul, Beta, 2009.

Taşkın, Mustafa:

Adli ve İstihbari Amaçlı İletişimin Denetlenmesi, Ankara, Seçkin, 2008.

Tezcan, Durmuş, Erdem, Mustafa Ruhan
Önok, R. Murat :

Teorik ve Pratik Ceza Özel Hukuku, 5. bs., Ankara, Seçkin, 2007.

Uzeltürk, Sultan:

1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı, İstanbul, Beta, 2004.

Velecky, Labor C.:

“The Concept of Privacy”, **Privacy**, Ed. by. John B. Young, USA, John Wiley&Sons, 1978, s. 13-35.

Velu, Jacques:

“The European Convention on Human Rights and the Right to Respect for Private Life, the Home and Communications,” **Privacy, and Human Rights, Reports and Communications Presented at the Third International Colloquy About the European Convention on Human Rights, Organised by the Belgian Universities and the Council of Europe, with the Support of the Belgian Government, Brussels, September-3 October 1970**, Ed. by. A. H. Robertson, London, Manshester University Press, 1973, s. 12-128.

Yüzbaşıoğlu, Necmi:

Anayasa Hukukunun Temel Metinleri, İstanbul, Beta, 2006.

- Yüzbaşıoğlu, Necmi: **Türk Anayasa Yargısında Anayasallık Bloku**, İstanbul, İ.Ü. Basımevi ve Film Merkezi, 1993.
- Warren, Samuel D., Brandeis, Louis D.: “The Right to Privacy,” **Harvard Law Review**, C.IV, No:5, 1890, s. 193-220.
- Westin, Alan: **Privacy and Freedom**, Aktaran Daniel J. Solove, Paul M. Schwartz, **Privacy, Information, and Technology**, USA, Wolters Klower, 2009.
- Westin, Alan F.: “Science, Privacy, and Freedom: Issues and Proposals for the 1970s Part I The Current Impact of Surveillance on Privacy,” **Columbia Law Review**, C.LXVI, No:6, 1966, s. 1003-1050.
- Wiesbrock, Anja: Case Note – Case C-555/07, Küçükdeveci v. Swedex, Judgment of the Court (Grand Chamber) of 19 January 2010.
- Whitman, James Q.: “The Two Western Cultures of Privacy: Dignity versus Liberty,” **Yale Law Journal**, 113.6, Nisan 2004.
- Yüksel, Saadet: **Constitutional Changes of Turkey in 2001 under the Framework of the EU Adaptation Process**, Annales, C.XXXIX, No:56, 2007, s. 153-165.

Yüksel, Saadet:

“Avrupa Birliği’nin Anayasa Süreci,”
Ergon A. Çetingil ve Rayegan Kender’e 50. Birlikte Çalışma Yılı Armağanı, İstanbul, 2007, s. 1256-1276.

“Engaging Privacy and Information Technology in a Digital Age”, Ed. by. James Waldo, Herbert S. Lin, and Lynette L. Millett, Washington, DC, The National Academic Press, 2007.

“New European Union Privacy Rules Go Into Effect,” **The Computer & Internet Lawyer**, C.XXI, No:1, January 2004.

“The Right to Privacy in Nineteenth Century America,” **Harvard Law Review**, C.XCIV, No:8, Haziran 1981, s. 1892-1910.

“Dinleme Yapılmıyor”, Bilgi ve İletişim Teknolojileri Dünyası, (Çevrimiçi) <http://www.bitdunyasi.com/tr/?Sayfa=Detay&Id=1447>, 30 Ocak 2012.

SÖZLÜKLER

Büyük Türkçe Sözlük, Türk Dil Kurumu, (Çevrimiçi) <http://tdkterim.gov.tr/bts/>, 12 Kasım 2011.

İletişim Sözlüğü, Erol Mutlu, 2. bs., Ankara, Ark, 1995.

Cambridge Dictionaries Online, (Çevrimiçi) http://dictionary.cambridge.org/dictionary/business-english/meter_2, 10 Ocak 2012.

MAHKEME KARARLARI, İLGİLİ YASAL DÜZENLEMELER ve ULUSALÜSTÜ RESMİ BELGELER

Act no 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (Amended by the Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data), Annotated text.

Act on the Protection of Personal Data (transposing into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), (Çevrimiçi) <http://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM>, 21 Aralık 2011.

Adli ve Önleme Aramaları Yönetmeliği, Resmi Gazete No. 25832, 1 Haziran 2005.

Avrupa Temel Haklar Şartı, Charter of Fundamental Rights of the European Union, C 364/10, 18.12.2000.

Case of Halford v. The United Kingdom (Application No. 20605/92), Strasbourg, Final Judgment 25 Haziran 1997.

Case of Kruslin v. France, (Application No. 11801/85), Strasbourg, 24 Nisan 1990.

Case of Amann v. Switzerland, (Application No. 27798/95), Strasbourg, 16 Şubat 2000.

Case of Niemietz v. Germany, (Application no. 13710/88), Strasbourg, 16 Aralık 1992.

Case of Khan v. The United Kingdom, (Application No. 35394/97), Strasbourg, 12 Mayıs 2000.

Case of Malone v. The United Kingdom (Application No. 8691/79), Strasbourg, 2 Ağustos 1984.

Case of Kopp v. Switzerland, (Application No. 13/1997/797/1000), Strasbourg, 25 Mart 1998.

Case of Gaskin v. The United Kingdom, (Application No. 10454/8), Strasbourg, 7 Temmuz 1989.

Case of Leander v. Sweeden, (Application No. 9248/81), Strasbourg, 26 Mart 1987.

Case of Klass and others v. Germany (Application No. 5029/71), Strasbourg, 6 Eylül 1978.

Case of Perry v. The United Kingdom (Application No. 63737/00), Strasbourg, Final Judgment 17 Ekim 2003.

Case of Dudgeon v. The United Kingdom, (Application No. 7525/76), Strasbourg, 22 Ekim 1981.

Case of Kroon and Others v. The Netherlands (Application No. 18535/91), Strasbourg, 27 Ekim 1994.

Case of P.G. and J.H. v. The United Kingdom (Application No. 44787/98), Strasbourg, Final Judgment 25 December 2001, (Çevrimiçi) <http://cmiskp.echr.coe.int/tkp197/view.asp?item=5&portal=hbkm&action=html&highlight=p.g.%20%7C%20j.h.&sessionid=81832097&skin=hudoc-en>, 15 Kasım 2011.

Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik, Resmi Gazete No. 26434, 14 Şubat 2007.

Council of Europe – ETS no. 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981, <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>, 23 Ekim 2011.

Consolidated Version of the Treaty Establishing the European Community, 24.12.2002, C 325/147.

“Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union”, **Official Journal of the European Union**, C.LI, 9 May 2008, C 115/19.

Council of European Parliamentary Assembly, Resolution 428 (1970) containing a declaration on mass communication media and human rights, (Çevrimiçi) <http://www.assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta70/ERES428.htm#323> Kasım 2011.

Data Protection Act 1998, C.XXIX, (Çevrimiçi) <http://www.legislation.gov.uk/ukpga/1998/29/section/1>, 3 Aralık 2011.

Data Protection Act 1998 Legal Guidance, (Çevrimiçi)
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf, 11 Aralık 2011.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23.11.1995 P.0031-0050, (Çevrimiçi) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>, 23 Ekim 2011.

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal L 024, 30/01/1998 P. 0001 – 0008, (Çevrimiçi) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML>, 7 Aralık 2011.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal of the European Communities, 31 July 2002.
Draft Charter of Fundamental Rights of the European Union, Charte 4473/00, Brussels, 11 October 2000.

Doe v. Bolton, 410 U.S. 179 (1973).

Draft Treaty establishing a Constitution for Europe, Submitted to the President of the European Council in Rome, Conv 850/03, Brüksel, 18 Temmuz 2003.

Durant v. FSA [2003] EWCA Civ 1746, Royal Court of Justices Strand, London, WC2A 2LL, 8 December 2003.

E. 1963/16, K. 1963/83, K.t. 8 Nisan 1963, Anayasa Mahkemesi kararı.

E. 1996/68, K. 1999/1, K.t. 6 Ocak 1999, Anayasa Mahkemesi kararı.

E. 1968/61, K. 1969/23, K.t. 29 Nisan 1969, Anayasa Mahkemesi kararı.

E. 1971/41, K. 1971/67, K.t. 17 Ağustos 1971, Anayasa Mahkemesi kararı.

E. 1972/1, K. 1972/20, K.t. 27 Nisan 1972, Anayasa Mahkemesi kararı.

E. 1977/1, K. 1977/20, K.t. 5 Nisan 1977, Anayasa Mahkemesi kararı.

E. 1985/8, K. 1986/27, K.t. 26 Kasım 1986, Resmi Gazete No. 19544, 14 Ağustos 1987, Anayasa Mahkemesi kararı.

E. 1988/50, K. 1989/27, K.t. 23 Haziran 1989, Resmi Gazete No. 20302, 4 Ekim 1989, Anayasa Mahkemesi kararı.

E. 1996/68, K. 1999/1, K.t. 6 Ocak 1999, Resmi Gazete No. 24292, 19 Ocak 2001, Anayasa Mahkemesi kararı.

E. 2002/166, K. 2004/3, K.t. 21 Ocak 2004, Resmi Gazete No. 25510, 2 Temmuz 2004, Anayasa Mahkemesi kararı.

E. 2005/43, K. 2008/143, K.t. 18 Eylül 2008, Resmi Gazete No. 27089, 23 Aralık 2008, Anayasa Mahkemesi kararı.

E. 2006/4.MD-122, K. 2006/162, Ceza Genel Kurulu.

E. 2007/2795, K.t. 14/10/2008, Danıştay 10. Dairesi.

E. 2008/13862, K. 2009/479, K.t. 22.01.2009, Anayasa Mahkemesi kararı.

E. 2008/874, K. 2008/7160, 04/06/2008, Yargıtay 9. Ceza Dairesi.

E. 2010/751, K. 2011/96, K.t. 13/04/2011, Yargıtay Hukuk Genel Kurulu.

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 10 Temmuz 2008.

Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), In the version published on 20 December 20, 1990 (BGBl.I 1990 S.2954), as amended by the law of 14 September, 1994 (BGBl. I S. 2325), (Çevrimiçi) <http://www.iuscomp.org/gla/statutes/BDSG.htm>, 11 Aralık 2011.

Katz v. United States, 389 U.S. 347 (1967).

Kişisel Verilerin Korunması Kanun Tasarısı, T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, Sayı: 1812, 22 Nisan 2008, (Çevrimiçi) <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf>, 3 Ocak 2011.

“OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, (Çevrimiçi)
http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&en-USS_01DBC.html, 23 Ekim 2011.

OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part One, (Çevrimiçi)
http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html#guidelines, 18 Aralık 2011.

Olmstead v. United States, 277 U.S. 438 (1928).

Organic Law 15/1999 of 13 December on the Protection of Personal Data, Unofficial translation that has been updated according to the changes operated in the Act after the Sentence 292/200 of the Spanish Constitutional Court, madde 7, (Çevrimiçi)
http://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/SPAIN_Organiclaw_15_99.pdf, 21 Aralık 2011.

Personal Data Act (1998:204); issued 29 April 1998, (Çevrimiçi)
<http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf>, 28 Aralık 2011.

Roe et al. v. Wade, 410 U.S. 113 (1973).

Swiss Federal Act on Data Protection of 19th June 1992 (Status as per 3rd October 2000), (Çevrimiçi) <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.CH>, 27 Ocak 2011.

The Constitution of the United States of America, English original text of the Constitution of 1789, together with Amendments I to XXVII (Ratified 5-7-1992), Doc. No 110-50, House of Representatives, United States Government Printing Office, Washington, 2007.

The Foreign Intelligence Surveillance Act, 50 USCS § 1801- § 1803.

The Pen Register Act, 18 USCS § 3121-3127.

The Wiretap Act, 18 USCS § 2516 - §2518.

United States v. United States District Court for the Eastern District of Michigan et al., 407, U.S. 297, 1972.

Whalen v. Roe, 429 U.S. 589 (February 22, 1977), No. 75-839, (Çevrimiçi) <http://www.caselaw.lp.findlaw.com>, 23 Mayıs 2010.

11 ve 14 No'lu Protokoller ile Değişik İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme ve 1, 4, 6, 7, 12 ve 13 No'lu Protokoller, Türkçe Çeviri, Avrupa İnsan Hakları Mahkemesi Yazı İşleri Müdürlüğü, Haziran 2010.

1982 Anayasası, (Çevrimiçi) http://heinonline.org.ezp-prod1.hul.harvard.edu/HeinDocs/cowdocs/tr_1982_2010_turk.pdf, 26 Kasım 2010.

1961 Anayasası, Resmi Gazete No. 10859, Resmi Gazete tarihi: 20 Temmuz 1961.

657 sayılı 14/07/1965 tarihli Devlet Memurları Kanunu, Resmi Gazete No. 12056, Resmi Gazete tarihi: 23 Temmuz 1965.

1602 sayılı 04/07/1972 tarihli Askeri Yüksek İdare Mahkemesi Kanunu, Resmi Gazete No. 14251, Resmi Gazete tarihi: 20 Temmuz 1972.

2559 sayılı, 4/7/1934 tarihli Polis Vazife ve Salahiyet Kanunu, Resmi Gazete No. 2751, Resmi Gazete tarihi: 14 Temmuz 1934.

2803 sayılı, 10/03/1983 tarihli Jandarma Teşkilat, Görev ve Yetkileri Kanunu, Resmi Gazete No. 17985, Resmi Gazete tarihi: 12 Mart 1983.

5 USCS § 552a, Current through PL 112-73, approved 12/20/11, Title 5. Government Organization and Employees, Part I. The Agencies Generally, Chapter 5. Administrative Procedure, Subchapter II. Administrative Procedure.

5320 sayılı Ceza Muhakemesi Kanununun Yürürlük ve Uygulama Şekli Hakkında Kanun, Resmi Gazete No. 25772, Resmi Gazete tarihi: 31 Mart 2005.

5237 sayılı 26/09/2004 tarihli Türk Ceza Kanunu, Resmi Gazete No. 25611, Resmi Gazete tarihi: 12 Ekim 2004.

5271 sayılı Ceza Muhakemesi Kanunu, Resmi Gazete No. 25673, Resmi Gazete tarihi: 17 Aralık 2004.

5353 sayılı Ceza Muhakemesi Kanununda Değişiklik Yapılmasına Dair Kanun'un 17. maddesi, Resmi Gazete No. 25832, Resmi Gazete tarihi: 1 Haziran 2005.

5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Resmi Gazete No. 25884, Resmi Gazete tarihi: 23 Temmuz 2005.

5442 sayılı, 10/6/1949 tarihli İl İdaresi Kanunu, Resmi Gazete No. 7236, Resmi Gazete tarihi: 18 Haziran 1949.

5681 sayılı Polis Vazife ve Salahiyet Kanununda Değişiklik Yapılmasına Dair Kanun m. 3, 2 Haziran 2007, Resmi Gazete No. 26552, Resmi Gazete tarihi: 14 Haziran 2007.

5809 sayılı Elektronik Haberleşme Kanunu, Resmi Gazete No. 27050, Resmi Gazete tarihi: 10 Kasım 2008.

5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun, Resmi Gazete No. 27580, Resmi Gazete tarihi: 13 Mayıs 2010.

6110 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Resmi Gazete No. 27846, Resmi Gazete tarihi: 14 Şubat 2011.

5651 sayılı Kanun, Resmi Gazete No. 26530, Resmi Gazete tarihi: 23 Mayıs 2007.

4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanununun Uygulanmasına İlişkin Yönetmelik, Resmi Gazete No. 24299, Resmi Gazete tarihi: 26 Ocak 2001.

26513 sayılı ve 5 Mayıs 2007 tarihli 4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanununun Uygulanmasına İlişkin Yönetmeliğin Yürürlükten Kaldırılmasına Dair Yönetmelik.

ÖZGEÇMİŞ

Saadet Yüksel lisans eğitimini 2004 yılında tamamladığı İstanbul Üniversitesi Hukuk Fakültesi'nden, 2006 yılında üstün başarıyla Avrupa Birliği hukuku yüksek lisans derecesini almıştır. Yüksel, ikinci yüksek lisansını Harvard Hukuk Fakültesi'nde tamamlamış ve “Türkiye’de Yeni Bir Anayasa Yapımı: Zorluklar ve Karşılaştırmalı Örnekler Çerçevesinde Çözüm Önerileri” isimli Harvard’a sunduğu bitirme tezi onur derecesiyle kabul edilmiştir. Yüksel, halen İstanbul Üniversitesi Hukuk Fakültesi Anayasa Kürsüsünde araştırma görevlisi olarak çalışmaktadır.

Georgetown Hukuk Fakültesi'nde de misafir öğretim elemanı ve araştırmacı olarak bulunmuş olan Yüksel, aynı zamanda, “Avrupa Birliği’nde İşçilerin Serbest Dolaşımı ve Türk İşçilerinin Statüsü” isimli kitabın yazarıdır. Özellikle anayasa dizayn ve yapım süreçleri ve Avrupa Birliği’ne üyelik sürecinde Türkiye’deki anayasa değişiklikleri üzerine çalışan Yüksel’in yayımlanmış makalelerinden bazıları “AB’ye Uyum Sürecinde Türkiye’deki 2001 Anayasa Değişikliklerinin Yeri”, “Avrupa Birliği’nin Anayasa Süreci” ve “Türkiye’de Anayasa Yapım Sürecindeki Usuli Sorunlar”olarak sayılabilir.