



TÜRKİYE BÜYÜK MİLLET MECLİSİ

YASAMA DÖNEMİ

24

YASAMA YILI

3

SIRA SAYISI: 489

**HABERLEŞME ÖZGÜRLÜĞÜNE VE
ÖZEL HAYATIN GİZLİLİĞİNE YÖNELİK
İHLALLERİN TESPİTİ VE ÖNLENMESİNE
İLİŞKİN TEDBİRLERİN BELİRLENMESİ
AMACIYLA KURULAN**

**MECLİS ARAŞTIRMASI KOMİSYONU
RAPORU**

Haziran 2013

İÇİNDEKİLER

KISALTMALAR.....	ix
TABLolar DİZİNİ.....	xviii
ŞEKİLLER DİZİNİ.....	xix
KOMİSYON BAŞKANININ SUNUŞU	1
ÖNERGE METİNLERİ	8
TAKDİM YAZISI	35

BİRİNCİ BÖLÜM

KOMİSYONUN KURULUŞU VE ÇALIŞMALARI.....	37
1.1 Meclis Araştırması Önergelerinin Özeti.....	37
1.2 Komisyonun Kuruluşu.....	38
1.3 Komisyonun Görev, Yetki ve Süresi.....	40
1.4 Komisyon Çalışmaları	40
1.4.1 Komisyon Toplantıları.....	42
1.4.1.1 Hukuk Alt Komisyonu Toplantıları.....	46
1.4.1.2 Teknik Alt Komisyon Toplantıları	48
1.4.2 Komisyonca Gerçekleştirilen Çalışma Ziyaretleri	48
1.4.2.1 13 Mart 2013 Tarihli Çalışma Ziyaretleri.....	49
1.4.2.2 14 Mart 2013 Tarihli Çalışma Ziyaretleri.....	51
1.4.2.3 Teknik Alt Komisyonca Gerçekleştirilen Ziyaretler	53
1.5 Komisyona İntikal Eden Bilgi ve Belgeler.....	55

İKİNCİ BÖLÜM

ÖZEL HAYATIN GİZLİLİĞİ VE HABERLEŞME ÖZGÜRLÜĞÜ.....	56
2.1 Özel Hayatın Gizliliği ve Korunması	56
2.1.1 Genel Olarak.....	56

2.1.2 Özel Hayatın Gizliliği	56
2.1.3 Haberleşme Özgürlüğü	59
2.1.4 Özel Hayatın Korunması	61
2.1.5 İletişimin Denetlenmesini Gerektiren Sebepler	63
2.2 Mukayeseli Hukukta İletişimin Denetlenmesi	64
2.2.1 Genel olarak	64
2.2.2 Almanya	65
2.2.3 Fransa	67
2.2.4 İngiltere	69
2.2.5 Avusturya	70
2.2.6 İtalya	71
2.3 Türk Hukukunda İletişimin Denetlenmesi	72
2.3.1 Tarihsel Gelişim	72
2.3.1.1 1961 ve 1982 Anayasaları	72
2.3.1.2 1412 Sayılı Ceza Muhakemeleri Usulü Kanunu	73
2.3.1.3 2559 Sayılı Polis Vazife ve Salahiyet Kanunu	73
2.3.1.4 2803 Sayılı Jandarma Teşkilat Görev ve Yetkileri Kanunu	74
2.3.1.5 2937 Sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu	74
2.3.1.6 4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu	75
2.3.2 Adli Amaçlı İletişimin Denetlenmesi	75
2.3.2.1 Genel Olarak	75
2.3.2.2 İletişimin Tespiti	76
2.3.2.3 İletişimin Dinlenmesi ve Kaydedilmesi	77
2.3.2.4 Sinyal Bilgilerinin Değerlendirilmesi	78
2.3.2.5 Mobil Telefonun Yerinin Tespiti	78

2.3.2.6 İletişimin Denetlenmesinin Koşulları.....	79
2.3.2.7 İletişimin Denetlenmesi Yasağı.....	90
2.3.2.8 Tesadüfen Elde Edilen Deliller.....	93
2.3.2.9 Hukuka Aykırı İletişimin Denetlenmesi ve Yaptırımı	94
2.3.3 Önleme Amaçlı İletişimin Denetlenmesi	97
2.3.3.1 İletişimin Denetlenmesinin Koşulları.....	101
2.3.3.2 Elde Edilen Bilgilerin Niteliği ve Kullanılması	107
2.3.3.3 Keyfiligi Önleyici Güvenceler ve Hukuka Aykırılığın Yaptırımı.....	108

ÜÇÜNCÜ BÖLÜM

İLETİŞİMİN DENETLENMESİ TEDBİRİNİN UYGULAMASI..... 110

3.1 İletişimin Denetlenmesi Tedbirinin Uygulaması.....	110
3.1.1 Kararı Yerine Getirecek Kişi ve Kurumlar.....	110
3.1.2 Kararın Yerine Getirilmesi	111
3.2 Emniyet Teşkilatı.....	114
3.2.1 Adli Amaçlı İletişimin Denetlenmesi	114
3.2.1.1 Uygulamada Dikkat Edilmesi Gerekenler.....	114
3.2.1.2 İletişimin Denetlenmesi Yöntemleri	123
3.2.1.3 İletişimin Denetlenmesi Sistematiği.....	127
3.2.1.4 İletişimin Denetlenmesi Yasak Olan ve Özel Usullere Tabi Kişiler.....	131
3.2.2 Önleme Amaçlı İletişimin Denetlenmesi	138
3.2.2.1 İletişimin Denetlenmesi Süreci.....	139
3.2.2.2 Önleme Amaçlı İletişimin Denetlenmesi Sonucu Yapılan Operasyonlardan Örnekler.....	141
3.2.2.3 İstihbarat Faaliyetlerinin Sonuçları	142
3.3 Jandarma Teşkilatı.....	143
3.3.1 Telekomünikasyon Yoluyla İletişimin Tespiti, Dinlenmesi ve Kayda Alınmasına İlişkin Uygulamalar	143

3.3.2 Adli Teknik Takip Faaliyetlerinin İcrası	144
3.3.2.1 Mahkeme Kararı Alınmadan Önce Yapılan İşlemler	144
3.3.2.2 Mahkeme Kararı Alındıktan Sonra Yapılan İşlemler	144
3.3.2.3 Mahkeme Kararının Sona Ermesini Müteakip Yapılan İşlemler	145
3.3.3 Önleyici Teknik Takip Faaliyetlerinin İcrası	146
3.3.3.1 Mahkeme Kararı Alınmadan Önce Yapılan İşlemler	146
3.3.3.2 Mahkeme Kararı Alındıktan Sonra Yapılan İşlemler	146
3.3.3.3 Mahkeme Kararının Sona Ermesini Müteakip Yapılan İşlemler	147
3.3.4 Teknik Takip Faaliyetlerinin İcra Edildiği Ortam	147
3.3.5 Teknik Takip Faaliyetlerinin Denetimi	147
3.3.6 Teknik Takip Faaliyetlerinin Sonuçları	149
3.4 Milli İstihbarat Teşkilatı	152
3.4.1 İstihbari Amaçlı İletişimin Denetlenmesi Faaliyetleri	153
3.4.1.1 Kapsamı	153
3.4.1.2 Kararı Vermeye Yetkili Makam	154
3.4.1.3 Kararın/ Yazılı Emrin İçeriği	154
3.4.1.4 Kararın Süresi	155
3.4.1.5 Kararın Sona Ermesi	155
3.4.1.6 Denetim	155
3.4.1.7 Cezai Hükümler	155
3.4.2 Adli Amaçlı İletişimin Denetlenmesi Faaliyetleri	156
3.4.2.1 Kapsamı	157
3.4.2.2 Dinleme Yasakları	157
3.4.2.3 Kararı Vermeye Yetkili Makam	158
3.4.2.4 Kararın İçeriği	158
3.4.2.5 Kararın Süresi ve Uygulanması	158

3.4.2.6 Kararın Sona Ermesi.....	158
3.4.2.7 Cezai Hükümler.....	159
3.4.3 İstihbari ve Adli Amaçlı İletişimin Denetlenmesi Tedbirlerinin Karşılaştırması	160
3.5 Telekomünikasyon İletişim Başkanlığı	161
3.5.1 Kuruluşu	161
3.5.2 İdari Yapısı	162
3.5.3 Görevleri.....	163
3.5.4 Kararların Uygulanması	167

DÖRDÜNCÜ BÖLÜM

TEKNİK UYGULAMALAR, YÖNTEMLER VE TEDBİRLER	169
4.1 Kavramlar ve Tarihsel Gelişim	169
4.2 Teknik Dinleme ve İzlemeler	172
4.2.1 Cihazlı Takipler	172
4.2.1.1 Kapalı Devre Cihazlarla Dinleme ve İzlemeler.....	173
4.2.1.2 Açık Devre Cihazlarla Dinleme ve İzlemeler.....	176
4.2.1.3 Şebeke Dinlemeleri.....	182
4.2.1.4 Dost Sistem Suiistimaliyle Takipler	183
4.2.1.5 Akustik Dinlemeler	184
4.3 Dinleme ve İzleme Cihazları İthalatı	186
4.3.1 Genel Olarak İthalat Gümrük Prosedürleri.....	186
4.3.2 Dinleme ve İzleme Cihazlarının İthalat Prosedürü.....	189
4.3.2.1 Dinleme ve İzleme Cihazlarının GTİP’inin Tespiti	189
4.3.2.2 Dinleme ve İzleme Cihazlarının İthalatı.....	190
4.3.2.3 Dinleme ve İzleme Cihazlarının İthalat Denetimine İlişkin Mevzuat	191
4.3.2.4 Dinleme ve İzleme Cihazlarının İthalat Vergileri	191

4.3.2.5 Dinleme ve İzleme Cihazlarının İthalat Verileri	192
4.3.2.6 Dinleme ve İzleme Cihazlarının Gümrük Kontrolleri	192
4.3.2.7 Dinleme ve İzleme Cihazlarının Yakalama Verileri	193
4.4 Frekans Spektrumu	194
4.4.1 Spektrum Hakkında Genel Bilgiler	194
4.4.1.1 Frekans Nedir?	194
4.4.1.2 Dalga Nedir?	194
4.4.1.3 Elektromanyetik Dalga	195
4.4.1.4 Elektromanyetik Spektrum	196
4.4.1.5 Spektrum Yönetimi	198
4.4.1.6 Ülkemizde Spektrum Yönetimi	199
4.4.2 Tahsisler	200
4.4.2.1 Spektrumun İzlenmesi ve Denetlenmesi	201
4.4.2.2 Milli Monitör Sistemi	202
4.5 Kablosuz Haberleşme	203
4.5.1 Cep Telefonu Teknolojileri	203
4.5.1.1 2G Teknolojisi	203
4.5.1.2 2.5G Teknolojisi	204
4.5.1.3 GPRS	205
4.5.1.4 EDGE	205
4.5.1.5 3G Teknolojisi	206
4.5.1.6 WCDMA (UMTS- IMT-DS)	207
4.5.1.7 Diğer 3G Teknolojileri	208
4.5.1.8 4G Teknolojiler	209
4.5.2 GSM Temel Kavramlar ve Şebeke Elemanları	210
4.5.2.1 Cep telefonu (MS: Mobile Station)	210

4.5.2.2 Baz istasyonu sistemi (BSS: Base Station System).....	211
4.5.2.3 Baz istasyonu (BTS: Base Transceiver Station).....	211
4.5.2.4 Baz istasyonu kontrol birimi (BSC: Base Station Controller).....	212
4.5.2.5 Transkoder	212
4.5.2.6 Şebeke Anahtarlama Sistemi (NSS: Network Switching System).....	212
4.5.2.7 MSC.....	213
4.5.2.8 HLR	213
4.5.2.9 VLR	213
4.5.2.10 EIR.....	214
4.5.2.11 AUC.....	214
4.5.2.12 IWF.....	215
4.5.2.13 EC	215
4.6 Mahremiyet ve Gizlilik.....	215
4.6.1 Kişisel Bilgiler.....	218
4.6.2 TTNET-Phorm Ortaklığı ile Mahremiyet İhlali	219
4.6.3 TürkTrust Hatalı Sertifika Dağıtımı	219
4.6.4 Sağlık Bilgileri.....	220
4.6.5 Varlık Bilgileri.....	220
4.6.6 Konum/Güzergâh Bilgileri (GPS)	220
4.6.7 Teknik Saldırı Yöntemleri ve Amaçları	221
4.7 Veri Güvenliği ve Kriptoloji.....	227
4.7.1 Veri Tabanı Güvenliği	229
4.7.2 Bulut Bilişim Güvenliği	231
4.7.3 Kamu Kurumlarının Ortak Ağ ve Veri Tabanı.....	233
4.7.3.1 Dünyadaki Uygulamalar ve Hâlihazırda Ülkemizdeki Durum	233
4.7.3.2 Bilim ve Teknoloji Yüksek Kurulu Kararları.....	233

BEŞİNCİ BÖLÜM

SONUÇ VE ÖNERİLER	234
5.1 Hukuki Öneriler	236
5.2 Teknik Öneriler	264
KARAR CETVELİ	270
MUHALEFET ŞERHLERİ.....	271
KAYNAKÇA.....	296
EK-TUTANAK ÖZETLERİ	302

KISALTMALAR

1G	Birinci Nesil Cep Telefonu Şebekesi (1 st Generation)
2G	İkinci Nesil Cep Telefonu Şebekesi (2 nd Generation)
3G	Üçüncü Nesil Cep Telefonu Şebekesi (3 rd Generation)
3GPP	Third Generation Partnership Program
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AİHM	Avrupa İnsan Hakları Mahkemesi
AK Parti	Adalet ve Kalkınma Partisi
AR-GE	Araştırma-Geliştirme
ATM	Otomatik Paraçekme Makinası (Automated Teller Machine)
AUC	Kimlik Doğrulama Merkezi (Authentication Centre)
AVM	Alışveriş Merkezi
Ay	Anayasa
BDP	Barış ve Demokrasi Partisi
BGA	Basit Güç Analizi
Bkz	Bakınız
BM	Birleşmiş Milletler
BoD	Talebe Göre Bant Genişliği (Bandwidth on Demand)
BSC	Baz İstasyonu Kontrol Birimi (Base Station Controller)
BSS	Baz İstasyonu Sistemi (Base Station System)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
BTS	Baz istasyonu (Base Transceiver Station)
BTYK	Bilim ve Teknoloji Yüksek Kurulu
C	Cilt

CCTV	Kapalı Devre Televizyon (Closed Circuit Television)
CDMA	Kod Bölmeli Çoklu Erişim (Code Division Multiple Access)
CDMA2000	Kod Bölmeli Çoklu Erişim-2000 Teknolojisi
CEPT	Avrupa Posta ve Telekomünikasyon İdareleri Birliği (Comité Européen des Postes et Telecommunications)
CHP	Cumhuriyet Halk Partisi
CMK	Ceza Muhakemesi Kanunu
CMSV	Kontrol, Bakım-Onarım ve İkmal Aracı (Control, Mending and Supply Vehicle)
CMUK	Ceza Muhakemeleri Usulü Kanunu
ÇASÖMK	Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu
D-AMPS	Sayısal Gelişmiş Mobil Telefon Sistemi (Digital Advanced Mobile Phone System)
DDoS	Dağılmalı Servis dışı Bırakma (Distributed Denial of Service)
DECT	Sayısal Gelişmiş Kablosuz Haberleşme (Digital Enhanced Cordless Telecommunications)
DNS	Alan Adı Sistemi (Domain Name Server)
DoS	Servis dışı Bırakma (Denial of Service)
DSSS	Doğrudan Sıralı Yaygın Spektrum (Direct Sequence Spread Spectrum)
E	Esas
EC	Yankı Giderici (Echo Canceller)
ECSD	Gelişmiş Devre Anahtarlama Veri (Enhanced Circuit Switched Data)
e-Devlet	Elektronik Devlet Uygulamaları
EDGE	Küresel Evrim için Gelişmiş Veri Hızları

	(Enhanced Data for Global Evolution)
EDS	Elektronik Denetleme Sistemi
EHF	30 GHz - 300 GHz Bandı (Extreme High Frequency)
EHK	Elektronik Haberleşme Kanunu
EIR	Teçhizat Kimlik Kütüğü (Equipment Identity Register)
EMC	Egan-Marino Şirketi (Egan-Marino Corporation)
ETSI	Avrupa Haberleşme Standartları Enstitüsü (European Telecommunications Standard Institute)
FATİH	Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi
FH	Frekans Atlama (Frequency Hoping)
FM	Frekans Modülasyonu
Gbps	Saniyede 1 Milyar Bitlik Veri Aktarım Hızı
GBT	Genel Bilgi Toplama
GHz	GigaHertz
GPRS	Genel Paket Telsiz Servisi (General Packet Radio Service)
GPS	Küresel Konumlandırma Sistemi (Global Positioning System)
GSM	Avrupa Cep Telefonu Standardı (Groupe Spécialé Mobile - Global System for Mobile Communication)
GTİP	Gümrük Tarife İstatistik Pozisyonu
GÜVAS	Gümrük Veri Ambarı Sistemi
HF	3 MHz - 30 MHz Bandı (High Frequency)
HLR	Sabit Abone Kütüğü (Home Location Register)
HP	Hewlett-Packard
HSCSD	Yüksek Hızlı Devre Anahtarlama Veri (High Speed Circuit Switched Data)
HTS	Historical Traffic Search

Hz	Hertz
IBM	Uluslararası Çalışma Makineleri (International Business Machines)
ICAO	Uluslararası Sivil Havacılık Örgütü (International Civil Aviation Organization)
ICCI	Tümleşik Devre Kart Tanımlayıcısı (Integrated Circuit Card Identifier)
IDS	Atak Tespit Sistemi (Intrusion Detection System)
IE	Microsoft İnternet Gezgini (Internet Explorer)
IEC	Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission)
IEEE	Elektrik ve Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers)
IMEI	Uluslararası Mobil Teçhizat Kimliği (International Mobile Equipment Identity)
IMO	Uluslararası Denizcilik Örgütü (International Maritime Organization)
IMSI	Uluslararası Mobil Abone Kimliği (International Mobile Subscriber Identity)
IMT	Uluslararası Mobil Telekomünikasyonları (International Mobile Telecommunications)
IMT-2000	IMT-2000 Standardı
IMT-A	İleri IMT (IMT Advanced)
IMT-DS	IMT Doğrudan Yayılmış (IMT-Direct Spread)
IMT-FT	IMT Frekans Bölgesi (IMT Frequency Time)
IMT-MC	IMT Çoklu Taşıyıcı (IMT Multicarrier)
IMT-SC	IMT Tek Taşıyıcı (IMT Single Carrier)

IMT-TC	IMT Zaman Kodu (IMT Time Code)
IP	İnternet Protokol Adresi
IPS	Atak Engelleme Sistemi (Intrusion Prevention System)
IS	Geçici Standart (Interim Standard)
ISO	Uluslararası Standartlaştırma Örgütü (International Organization for Standardization)
IT	Bilişim Teknolojileri (Information Technology)
ITU	Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)
ITU-R	Uluslararası Telekomünikasyon Birliği Telsiz Haberleşmesi Bölümü (International Telecommunication Union-Radio Communication Sector)
IWF	Birlikte Çalışma İşlevi (Interworking Function)
İKK	İstihbarata Karşı Koyma
J.Gn.K	Jandarma Genel Komutanlığı
J.K	Jandarma Komutanlığı
K	Karar
Kbit/s	Saniyede 1000 Bitlik Veri Aktarım Hızı
KDV	Katma Değer Vergisi
kHz	KiloHertz
KİHBİ	Kaçakçılık İstihbarat Harekât ve Bilgi Toplama
KOBİ	Küçük ve Orta Boyutlu İşletme
KOM	Kaçakçılık ve Organize Suçlarla Mücadele Dairesi Başkanlığı
LAI	Konum Alanı Kimliği (Location Area Identity)
LAN	Yerel Alan Şebekesi (Local Area Network)
LF	30 kHz - 300 kHz Bandı (Low Frequency)

LTE	Uzun Vadeli Evrim (Long Term Evolution)
LTE-A	İleri LTE (Long Term Evolution Advanced)
m	madde
Mbps	Saniyede 1 Milyon Bitlik Veri Aktarım Hızı
MF	300 kHz -3000 kHz Bandı (Medium Frequency)
MHP	Milliyetçi Hareket Partisi
MHz	MegaHertz
MIMO	Çoklu Girdi Çoklu Çıktı (Multiple Input, Multiple Output)
MİT	Milli İstihbarat Teşkilatı
MMS	Milli Monitör Sistemi
MOBBC	Mobil Radyo-TV Yayınları Ölçüm Sistemi (Mobile Broadcast Measurement System)
MOBDF	Mobil Yön Kestirme ve Monitör İstasyonu (Mobile Direction Finding Station)
MOBESE	Mobil Elektronik Sistem Entegrasyonu
MS	Mobil İstasyonu (Mobile Station)
MSC	Mobil Hizmetler Anahtarlama Merkezi (Mobile Services Switching Center)
MSISDN	Mobil İstasyonu Uluslararası Servisler Sayısal Ağı (Mobile Station International Services Digital Network)
NCC	Milli Kontrol Merkezi (National Control Center)
NLJD	Yarıiletken Tespit Detektörü (Non-Linear Junction Detector)
NSS	Şebeke Anahtarlama Merkezi (Network Switching System)
OFDM	Ortogonal Frekans Bölmeli Çok Yönlendirme (Orthogonal Frequency Division Multiplexing)
ÖTV	Özel Tüketim Vergisi

PC	Kişisel Bilgisayar (Personel Computer)
PDC	Kişisel Sayısal İletişim (Personal Digital Communications)
PDF	Basılabilir Belge Dosyası (Printable Document File)
PDFM	Portatif DF ve Monitör Teçhizatı (Portable Direction Finding Measurement Equipment)
PSTN	Genel Aktarmalı Telefon Şebekesi (Public Switched Telephone Network)
PTT	Posta ve Telgraf Teşkilatı Genel Müdürlüğü
PVSK	Polis Vazife ve Salahiyetleri Kanunu
RAND	Rastgele Sayı (Random Number)
RDX	Royal Demolition Explosive (Patlayıcı)
RF	Radyo Frekans
RMC	Bölge Monitör Kontrol Merkezi (Regional Monitor Center)
RRS	Bölge Uzaktan Kumandalı Sabit Monitör İstasyonu (Remote Regional Station)
RSA	Rivest, Shamir ve Adleman Yöntemi
RTT	Telsiz Aktarım Teknolojisi (Radio Transmission Technology)
s	Sayfa
SHF	3 GHz - 30 GHz Bandı (Super High Frequency)
SIM	Abone Kimlik Modülü (Subscriber Identity Module)
SMS	Kısa Mesaj Servisi (Short Message Service)
SPAM	Toplu Halde Gönderilen İstenmeyen E-Posta Mesajı
SRES	İmzalı Cevap Anlamına Gelen Kripto Değişkeni (Signed Response)
SSL	Güvenli Giriş Katmanı (Secure Socket Layer)
TADOC	Türkiye Uyuşturucu ve Organize Suçlarla Mücadele Akademisi
TBMM	Türkiye Büyük Millet Meclisi

TC	Transkoder
TCK	Türk Ceza Kanunu
TD-SCDMA	Zaman Bölmesi – Eşzamanlı Kod Bölmeli Çoklu Erişim (Time Division - Synchronous Code Division Multiple Access)
THF	300 GHz - 3000 GHz bandı (Tremendously High Frequency)
THz	TeraHertz
TİB	Telekomünikasyon İletişim Başkanlığı
TMK	Terörle Mücadele Kanunu
TMSI	Geçici Mobil Abone Kimliği (Temporary Mobile Subscriber Identity)
TNT	Trinitrotoulen (Patlayıcı)
TOBB	Türkiye Odalar ve Borsalar Birliği
TRRS	Bölge Uzaktan Kumandalı Seyyar Monitör İstasyonu (Travelling Remote Regional Station)
TTNET	Türk Telekom İnternet Hizmeti
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TV	Televizyon
UHF	300 MHz - 3 GHz Bandı (Ultra High Frequency)
UMTS	Evrensel Mobil Haberleşme Servisi (Universal Mobile Telecommunication Service)
USB	Evrensel Seri Veriyolu (Universal Serial Bus)
USOM	Ulusal Siber Olaylara Müdahale Merkezi
UTRA	Evrensel Karasal Radyo Erişimi (Universal Terrestrial Radio Access)
UTRA-FDD	UTRA – Frekans Bölgesi Çift Yönlmesi (UTRA – Frequency Domain Duplexing)

UTRA-TDD	UTRA – Zaman Bölgesi Çift Yönlmesi (UTRA – Time Domain Duplexing)
UWB	Aşırı Genişbant (Ultra Wideband)
UWC	Evrensel Kablosuz Haberleşmeler (Universal Wireless Communications)
UWC-136	Evrensel Kablosuz Haberleşmeler - 136 Standardı
vb	ve benzeri
vd	ve devamı
VHF	30 MHz - 300 MHz Bandı (Very High Frequency)
VLF	3 kHz - 30 kHz Bandı (Very Low Frequency)
VLR	Ziyaretçi Abone Kütüğü (Visitor Location Register)
VMS	Görüntülü Mesaj Servisi (Video Message Service)
VOIP	Voice Over Internet Protokol
vs	Vesaire
WAN	Geniş Alan Şebekesi (Wide Area Network)
WAP	Kablosuz Uygulama Protokolü (Wireless Application Protocol)
WCDMA	Genişbant CDMA (Wideband CDMA)
WI-FI	Kablosuz Ağ Bağlantısı Standardı (Wireless Fidelity)
Wimax	Worldwide Interoperability for Microwave Access
WLAN	Kablosuz Yerel Alan Şebekesi (Wireless Local Area Network)
YÖK	Yüksek Öğretim Kurumu

TABLOLAR DİZİNİ

Tablo 1- Komisyon Üyeleri.....	39
Tablo 2- Komisyon Uzmanları.....	41
Tablo 3- Komisyon Toplantıları.....	43
Tablo 4- Hukuk Alt Komisyonu Toplantıları.....	46
Tablo 5- Teknik Alt Komisyon Toplantıları.....	48
Tablo 6- Adli Amaçlı İletişimin Denetlenmesi Türleri.....	113
Tablo 7- Adli Amaçlı İletişimin Denetlenmesinin Uygulanması Aşamaları.....	116
Tablo 8- Tutanak Örneği.....	117
Tablo 9- İmha Süreci (CMK 137).....	121
Tablo 10- İmha Tutanağı Örneği.....	122
Tablo 11- İletişimin Denetlenmesi Yöntemleri.....	123
Tablo 12- İletişim Yöntemleri.....	124
Tablo 13- Mukayeseli Hukuka Göre Adli Amaçlı İletişimin Denetlenmesi.....	138
Tablo 14- Jandarma Genel Komutanlığınca İcra Edilen Teknik Takip Faaliyetleri Neticesinde Elde Edilen Sonuçlar.....	151
Tablo 15- Dinleme ve İzleme Cihazlarının İthalat Denetimine İlişkin Mevzuat.....	191
Tablo 16- Dinleme ve İzleme Cihazları İthalat Vergileri.....	191
Tablo 17- Dinleme ve İzleme Cihazları İthalat Verileri.....	192
Tablo 18- Dinleme ve İzleme Cihazlarının Yakalama Verileri.....	193
Tablo 19- Frekans Tablosu.....	198

ŞEKİLLER DİZİNİ

Şekil 1. GPS Cihazı	127
Şekil 2. El Kaide Operasyonu	141
Şekil 3. El Kaide Operasyonu Sonuçları	141
Şekil 4. Sıradan Ses Kayıt Cihazları	173
Şekil 5. Araba Anahtarı Şeklinde Gizli Ses Kayıt Cihazı – Anahtarlık Kamera	174
Şekil 6. Minyatür Kamera ve Mikrofon	174
Şekil 7. CCTV Kameraları	175
Şekil 8. Ultrasonik Böcek Devresi	177
Şekil 9. 3G ile Çalışabilen Kameralı GSM Dinleme ve İzleme Modülü	178
Şekil 10. Dörtlü Elektrik Uzatması İçerisine Saklanmış GSM Böcek	179
Şekil 11. GSM Devresi Yurt Dışından Getirildikten Sonra Monte Edilmiş Cihaz	179
Şekil 12. Peçetelik İçerisine Gizlenmiş Wi-Fi Böcek	180
Şekil 13. FM Böcek	181
Şekil 14. Pasif Böcek Devresi İllüstrasyonu	182
Şekil 15. Apartman Dâhilindeki Telefon Hattı Dağıtım Kutusu	183
Şekil 16. Lazer Dinleme Cihazı ile Ortam Dinlemesi	184
Şekil 17. Birinci ve İkinci Dünya Savaşları Arasındaki Yıllarda Hollanda Ordusu Hava Savunma Sisteminin Bir Parçası Olarak Geliştirilmiş Akustik Dinleme Cihazları	185
Şekil 18. Akustik Dinleme Cihazı	186
Şekil 19. Eşya Gümrük Kontrol Dağılımı	188

Şekil 20. Dinleme ve İzleme Cihazları Gümrük Kontrol Dağılımı	193
Şekil 21. Elektromanyetik Frekans Spektrumu	197
Şekil 22. GSM Mimarisi.....	204
Şekil 23. 3G Teknolojileri	208
Şekil 24. Sophos Labs Araştırma Sonuçları	223
Şekil 25. Bulut Bilişim	231

KOMİSYON BAŞKANININ SUNUŞU

Özel hayatın gizliliği ve korunması hakkı Anayasa’da olduğu gibi Avrupa İnsan Hakları Sözleşmesi’nde, İnsan Hakları Evrensel Bildirgesi’nde ve Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme’de güvence altına alınan kişiye sıkı sıkıya bağlı, dokunulmaz, devredilmez ve vazgeçilmez temel insani haklardan biridir.

Anayasa’da “Özel Hayatın Gizliliği ve Korunması” başlığı altında özel hayatın gizliliği (m. 20), konut dokunulmazlığı (m. 21) ve haberleşme hürriyeti (m. 22) olmak üzere üç temel kişisel hak yer almaktadır. Anayasa’nın “Özel Hayatın Gizliliği” başlıklı 20’nci maddesinde herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu ve özel hayatın ve aile hayatının gizliliğine dokunulamayacağı hükme bağlanmış ve “Haberleşme Hürriyeti” başlıklı 22’nci maddesinde herkesin haberleşme hürriyetine sahip olduğu ve haberleşmenin gizliliğinin esas olduğu düzenlemesine yer verilmiştir.

Ayrıca 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 usulünce verilmiş hâkim kararı olmadıkça yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciinin yazılı emri bulunmadıkça haberleşmenin engellenemeyeceği ve haberleşmenin gizliliğine dokunulamayacağı hususu anayasal güvence altına alınmıştır.

İnsan Hakları Evrensel Bildirgesi’nin 12’nci maddesinde “*Hiç kimsenin mahremiyetine, ailesine, evine ya da yazışmalarına keyfi bir şekilde karışamayacağı*” düzenlenmiştir.

Tarafı olduğumuz Avrupa İnsan Hakları Sözleşmesi’nin 8. maddesinde de herkesin haberleşmesine saygı gösterilmesi hakkına sahip olduğu kurala bağlanmıştır. Ayrıca bu hakka bir kamu otoritesinin müdahalesinin ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda orantılılık ilkesine uygun olarak ve kanunla öngörülmüş olmak şartıyla söz konusu olabileceği belirtilmiştir.

Bu düzenlemelere göre kişiler arasındaki haberleşme içeriklerinin suç öncesi veya belli bir suça ilişkin soruşturma kapsamında Anayasa ve kanunların belirlediği şartlar

çerçevesinde öğrenilmesi veya kayda alınması hukuka uygun görülmektedir.

Bu bağlamda son yıllarda artan örgütlü suçlarla mücadelede klasik ceza muhakemesi tedbirlerinin yetersiz kalması nedeniyle ve yeni tedbirler kapsamında iletişimin denetlenmesi bütün dünyada olduğu gibi ülkemizde de uygulanmaya başlanmıştır. Başta 5271 sayılı Ceza Muhakemesi Kanunu'nda olmak üzere 2559 sayılı Polis Vazife ve Salahiyet Kanunu, 2803 sayılı Jandarma Teşkilatı Görev ve Yetkileri Kanunu ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nda iletişimin adli veya önleyici amaçla denetlenmesine ilişkin düzenlemeler getirilmiştir. Bu düzenlemeler çerçevesinde, telekomünikasyon yoluyla iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine ilişkin kararların, hangi kurumlar tarafından hangi şartlarda alınabileceği, kararların hangi mahkemeler tarafından verilebileceği, kararların taşınması gereken zorunlu unsurlar, bu kararların hangi kolluk birimlerince yerine getirileceği ve kayıtların kimlerin sorumluluğunda olduğu hususları mevzuatımızda ayrıntılı olarak belirlenmiştir.

Buna göre, hâkim kararı bulunmadıkça, gecikmesinde sakınca bulunan durumlarda ise yirmi dört saat içinde hâkim onayı alınmadıkça dinleme yapılabilmesi hukuken mümkün değildir.

4422 sayılı Kanunun yürürlükte olduğu dönemde önleme amaçlı iletişimin denetlenmesi tedbirleri, anılan Kanunda, belirli suçların aydınlatılması amacıyla düzenlenmiş hükümlerin geniş yorumlanması sonucu uygulanabilmekteydi. Bu çerçevede önleme amaçlı iletişimin denetlenmesi faaliyetlerinin yasal zemine kavuşturulması ve uluslararası standartlarda uygulanmasının sağlanması amacıyla, TBMM tarafından 03.07.2005 tarihinde çıkarılan 5397 sayılı Kanunla 2559, 2803 ve 2937 sayılı Kanunlarda değişiklik yapılmasının yanında aynı zamanda Telekomünikasyon İletişim Başkanlığı (TİB) de kurulmuştur. Daha önce hukukumuzda yer almayan bu Kurumla birlikte adli ve önleyici amaçlı iletişimin denetlenmesi faaliyetlerine ilişkin iş ve işlemlerin tek merkezden yürütülmesi sağlanmıştır.

Böylece iletişimin denetlenmesi faaliyetlerinin nasıl yürütüleceği konusunda var olan belirsizlik ve denetimsizlikler ortadan kaldırılmış, adli ve önleme amaçlı iletişimin denetlenmesi faaliyetlerinin suiistimal edilmesinin önüne geçilmiş ve yetkili kurumlarca yapılan bu faaliyetlerin uluslararası standartlarda uygulanması sağlanmıştır.

Yapılan düzenlemelerle iletişimin denetlenmesine ilişkin kararların kolluk birimlerince TİB’e gönderilmesi zorunluluğu getirilerek, mahkeme kararı olmaksızın iletişime müdahale edilmesinin önüne geçilmiştir. Bu sayede, temel hak ve özgürlüklere müdahalenin tipik bir örneği olan iletişimin denetlenmesi faaliyetlerinin hukuka uygunluğunun denetimi mümkün hale gelmiştir.

Milli güvenlik, toplumun huzur ve refahı için adli ve istihbari süreçlerin aksamadan yürütülmesi, taleplerin ivedi şekilde karşılanarak suç ve suçlu ile etkin mücadele edilmesi ve suça ilişkin somut delillerin adli mercilere aktarılması süreçlerinin Avrupa İnsan Hakları Sözleşmesi, Avrupa İnsan Hakları Mahkemesi İçtihatları ve Anayasa ile belirlenen kıstaslara uygun olarak yerine getirilmesi açısından adli merciler, kolluk birimleri ve işletmeciler (gsm, pstn, sth, ISS’ler gibi 400’den fazla işletmeci) arasında TİB’in kuruluşu ile oluşan bu senkronize yapı hayati öneme sahiptir.

Suçla ve suçlularla etkin mücadele edebilmek için önemli bir yere sahip olan bu tedbir, özel hayatın gizliliği ve haberleşme hürriyetini de yakından ilgilendirmektedir. Zira insanın mutluluğu için önemli olan özel hayata saygı gösterilmesi hakkı, onun kişiliği için temel bir hak olup yeteri kadar korunmadığı takdirde kişilerin ve toplumun kendini huzurlu hissetmesi ve güven içerisinde yaşaması mümkün değildir. Bu nedenle mevzuata aykırı davranılarak kişiler arasındaki haberleşme içeriklerinin hukuka aykırı biçimde *tespiti, dinlenmesi ve kayda alınması* halinde fiiller suç oluşturacak ve failler 5237 sayılı Türk Ceza Kanunu’nun ilgili hükümlerine göre cezalandırılacaktır. Bununla birlikte kişilerin gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının görüntülü veya sesli olarak saptanması ve kaydedilmesi de suç oluşturacaktır.

Ülkemizde tüm bu yasal düzenlemelere ve etkin cezai yaptırımlara rağmen gerek yasal düzenlemelerden ve gerekse uygulamadan kaynaklanan bazı sorunların olduğu görülmektedir. Kamuoyunda da yasa dışı biçimde konuşmaların dinlendiği, kayda alındığı ve bu kayıtların kimi zaman basın yayın yoluyla hukuka aykırı bir şekilde kullanıldığı yönünde yaygın bir kanaat oluşmaktadır. Bu kanaatin oluşmasında iletişimin denetlenmesi tedbirinin son çare olarak uygulanması gerektiği şeklindeki ilkeye riayet edilmeksizin ilk başvuru tedbir olarak uygulanmasının da önemli etkisi bulunmaktadır.

Toplumun tamamına yakınında “dinleniyor muyum acaba” şeklinde bir endişenin bulunması demokratik hukuk devletinde kabul edilemez bir olgudur. En kısa zamanda bu

alğının ortadan kaldırılıp, başkasının hak ve özgürlüğünü ihlal etmeyen, kişi özgürlüklerinin korunmasına ve mahremiyetine saygı gösterilen güvenli, şeffaf, kanunlara uygun ortamların oluşturulması gerekmektedir. Bu anlamda mevcut cezaların bu tarz suçların işlenmesinde caydırıcılık niteliğini artırmak için bu tarz fiilleri işleyenlere uygulanacak müeyyidelerin genişletilmesi yoluna da gidilmelidir.

Bu noktada güvenlik/özgürlük dengesinin de iyi gözetilmesi ve kantarın topuzunun güvenlik yanına kaymasının önlenmesi gerekmektedir.

Kamuoyunda ciddi rahatsızlık meydana getiren bu durumun dikkate alınarak, sorunun çözüm yollarının ve alınması gereken yasal, idari, istihbari ve gerekli diğer tüm tedbirlerin tespiti amacıyla, Türk kamuoyunun pek de alışık olmadığı bir şekilde Türkiye Büyük Millet Meclisinde grubu bulunan iktidar ve muhalefet partilerinin tamamının ortak iradeleriyle, Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan Meclis Araştırması Komisyonumuz kurulmuş ve çalışmalarına başlamıştır.

Komisyonumuz dört aylık çalışma süresi içerisinde konuyla ilgili tüm paydaşların görüşlerini almış; Adalet Bakanlığı, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı, Milli İstihbarat Teşkilatı, Telekomünikasyon İletişim Başkanlığı, Türkiye Barolar Birliği, Türkiye Bilimsel ve Teknolojik Araştırma Kurumundan konuyla ilgili ayrıntılı bilgi almış; TÜRKSAT, Türk Telekom, Avea, Turkcell, Vodafone gibi şirketlerin sunumlarını dinlemiş ve bu kurum ve şirketlerde yerinde incelemelerde bulunmuştur. Yasa dışı dinlemelerde kullanılan böcek diye tabir edilen cihazların yurt dışından ithaline ilişkin olarak uygulamalara ve alınması gereken önlemlere ilişkin Ekonomi Bakanlığı ile Gümrük ve Ticaret Bakanlığı yetkililerinin bilgilerine başvurulmuştur. Komisyon çalışmalarının daha etkin yürütülebilmesi, çalışma süresinin daha verimli kullanılabilmesi amacıyla biri araştırma konusunun hukuki diğeri teknik yönünde çalışmak üzere iki Alt Komisyon kurulmuştur.

Alt Komisyonlar aracılığıyla, basın yayın kuruluşlarının temsilcileri, akademisyenler, sivil toplum kuruluşları ve istihbarat görevi yürütmüş kişilerin bilgi ve deneyimleri ile araştırma konusuna ilişkin çözüm önerileri alınmıştır.

Komisyonumuzca, yargı kurumlarının yürütülmekte olan ve kamuoyunun yakından takip ettiği özel hayatın gizliliğine yönelik ihlallere ilişkin somut bazı davalardan olan Cumhuriyet Halk Partisi eski Genel Başkanı Deniz Baykal, Milliyetçi Hareket Partisi

milletvekili adayları ve Adalet ve Kalkınma Partisi Genel Başkanı ve Başbakan Recep Tayyip Erdoğan'ın yasa dışı dinlenmesi ve izlenmesi hakkındaki soruşturma ve kovuşturmalara ilişkin Anayasa'nın 138'inci maddesinin üçüncü fıkrasında ifadesini bulan “*görülmekte olan bir dava hakkında Yasama Meclisinde yargı yetkisinin kullanılması ile ilgili soru sorulamayacağı, görüşme yapılamayacağı veya herhangi bir beyanda bulunulamayacağı*” hükmü gereğince herhangi bir araştırma yapılmamıştır.

Yürütülen çalışmalar sırasında kişiler arasındaki haberleşme içeriklerinin hukuka aykırı bir biçimde tespiti, dinlenmesi ve kayda alınması veya kişilerin gizli yaşam alanlarına girerek veya başka suretle başkaları tarafından görünmesi mümkün olmayan bir özel yaşam olayının görüntülü veya sesli olarak saptanması ve kaydedilmesi, kimi zaman bunların medya ortamlarında yayınlanması gibi suç teşkil eden faaliyetlerin nasıl ve hangi araçlar kullanılarak yapıldığının, araçların nasıl temin edildiğinin, bu araçların imali, ithalatı ve bulundurulması konusunda yasal bir kısıtlama bulunup bulunmadığının ve yaşanan sorunların çözümü amacıyla alınması gereken yasal, idari, istihbari ve diğer önlemlerin neler olabileceğinin tespiti amaçlanmıştır.

Komisyonumuz haberleşme özgürlüğü ve özel hayatın gizliliğine ilişkin ihlallerin tespiti ve bunlara ilişkin tedbirlerin belirlenmesi hususunda medyanın, akademi ve yargı dünyasının, istihbarat birimlerinin, ilgili kamu kurum ve kuruluşları ile sivil toplum örgütlerinin desteği ile çalışmalarını tamamlamıştır.

Çalışmalarımız sonunda hazırlanan raporumuz beş bölümden oluşmaktadır. Birinci Bölümde Komisyonumuzun kuruluşu, yapmış olduğu toplantılar ve çalışma ziyaretleri hakkında bilgi verilmiştir.

Özel Hayatın Gizliliği ve Haberleşme Özgürlüğü başlıklı İkinci Bölümde özel hayatın gizliliği ve korunması hakkının ne anlama geldiği ve hukuk sistemimizde nasıl düzenlendiğine, iletişimin denetlenmesi tedbirinin mukayeseli hukukta ve Türk hukukunda nasıl düzenlenmiş bulunduğuna, hangi hallerde bu tedbire başvurulabileceğine, hangi hallerde başvurulamayacağına, hukuka aykırılık halinde ne gibi yaptırımların uygulanabileceğine değinilmiştir.

Üçüncü Bölümde iletişimin denetlenmesi tedbirinin uygulamasının nasıl olduğu anlatılmıştır. Dördüncü Bölümde ise, teknik uygulamalar, yöntemler ve tedbirlerin nasıl olduğu açıklanmıştır.

Son olarak Sonuç ve Öneriler Bölümünde ise, çalışmalarımız sonucunda

ulaştığımız netice, ülkemizde ortaya çıkan sorunların kaynağı ve bu sorunların çözümüne dair yasal, idari, istihbari ve teknik önlemlerin neler olabileceğine dair tespitlerimiz yer almaktadır.

Komisyonumuz, haberleşme özgürlüğüne ve özel hayatın gizliliğine yönelik ihlallerin son derece önemli bir sorun olduğu bilinciyle çalışmış, haberleşme özgürlüğü ve özel hayatın gizliliğinin en temel kişisel haklar olduğunu ve bu haklara yönelik ihlallerin kesin olarak önlenmesi gerektiğini çalışmalarının her aşamasında vurgulamıştır.

Bu itibarla, titizlik ve özveri ile hazırladığımız bu Raporun, özel hayatın gizliliğinin sağlanması amacıyla belirlenecek politikalar için bir yol haritası niteliğinde olacağını ve Raporda yer verilen önerilerin ilgili kurum ve kuruluşlar tarafından en kısa sürede değerlendirileceğine yürekten inanıyoruz.

Komisyonumuzun kurulmasına vesile olan Adalet ve Kalkınma Partisi, Cumhuriyet Halk Partisi, Milliyetçi Hareket Partisi ve Barış ve Demokrasi Partisi Gruplarına; Komisyon çalışmalarımızın yürütülmesinde desteklerini esirgemeyen Türkiye Büyük Millet Meclisi Başkanı Sayın Cemil ÇİÇEK’e; Raporun ortaya çıkmasındaki gayretli çalışmaları, emekleri ve fikirleri dolayısıyla Komisyon Üyesi milletvekillerimize; Komisyonumuza sunum yapan, bilgi, belge sunan ve çalışmalarımıza katkı sağlayan bakanlıklara, kurum ve kuruluşlara, meslek örgütlerine, sivil toplum kuruluşlarına, akademisyenlere ve şahıslara; mesai mefhumu gözetmeksizin özveriyle çalışan Komisyon uzmanlarımıza ve Komisyon çalışmalarının kamuoyuyla paylaşılmasına katkı sağlayan medya mensuplarına en içten teşekkürlerimi sunar, Raporumuzun, Ülkemize ve milletimize hayırlı olmasını dilerim.

Yusuf BAŞER
Yozgat Milletvekili
Komisyon Başkanı

Dönem: 24

Yasama Yılı: 3

TBMM

(S. Sayısı: 489)

**İzmir Milletvekili Rıza TÜRMEK ve 25 Milletvekilinin (10/74),
Milliyetçi Hareket Partisi Grubu Adına Grup Başkanvekilleri İzmir Milletvekili
Okta YURAL ve Mersin Milletvekili Mehmet ŞANDIR'ın (10/471),
İstanbul Milletvekili Mustafa Sezgin TANRIKULU ve 30 Milletvekilinin (10/472),
Adalet ve Kalkınma Partisi Grubu Adına Grup Başkanvekilleri Giresun Milletvekili
Nurettin CANIKLI, Kayseri Milletvekili Mustafa ELİTAŞ, İstanbul Milletvekili Ayşe
Nur BAHÇEKAPILI, Adıyaman Milletvekili Ahmet AYDIN, Kahramanmaraş
Milletvekili Mahir ÜNAL ve 135 Milletvekilinin (10/473),
Şırnak Milletvekili Hasip KAPLAN ve 21 Milletvekilinin (10/474),
Barış ve Demokrasi Partisi Grubu Adına Grup Başkanvekilleri Iğdır Milletvekili
Pervin BULDAN ve Bingöl Milletvekili İdris BALUKEN'in (10/475),**

**Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve
Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Bir Meclis Araştırması
Açılmasına İlişkin Önergeleri ve (10/74, 471, 472, 473, 474, 475) Esas Numaralı Meclis
Araştırması Komisyonu Raporu**

ÖNERGE METİNLERİ

1. İzmir Milletvekili Rıza Türmen ve 25 Milletvekilinin, Telefon Dinlemelerinin Araştırılarak Alınması Gereken Önlemlerin Belirlenmesi Amacıyla Meclis Araştırması Açılmasına İlişkin Önergesi (10/74)

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Yasal olmayan telefon dinlemeleri Türkiye'de büyük bir hukuksal ve toplumsal sorun niteliği kazanmıştır. Bu gibi yasal olmayan telefon dinlemeleri ve bunların basın yoluyla kamuoyuna açıklanması özel yaşamın ağır bir biçimde ihlalidir.

En son olarak Genelkurmay Başkanlığı gibi bir devletin en gizli sırlarının bulunduğu bir kurumun da dinlenmiş olması soruna bir de güvenlik boyutunu eklemiş bulunmaktadır. Bu kaotik ortamdan yararlanan Başbakanın dahi yasa dışı dinlemelerden şikâyetçi olduğu ortadadır.

Yasal olmayan telefon dinlemelerinin kamuoyunda uyandırdığı derin kaygılara rağmen dinleyenleri bulmak için yeterli çaba gösterilmediği görülmektedir. Kamuoyunda yer alan bu konudaki duyarlılığa karşı TBMM'nin hareketsiz kalmaması gerektiği düşünülmektedir.

Bu nedenle, bu konuda alınabilecek önlemlerin saptanması ve uzmanların görüşlerine başvurulması için TBMM içtüzüğünün 104. ve 105. maddeleri ve Anayasa'nın 98. maddesi gereğince bir meclis araştırması açılmasını arz ederiz.

- | | |
|-----------------------|-------------|
| 1) Rıza Türmen | (İzmir) |
| 2) Candan Yüceer | (Tekirdağ) |
| 3) Erdal Aksünger | (İzmir) |
| 4) Bülent Kuşoğlu | (Ankara) |
| 5) Aydın Ağan Ayaydın | (İstanbul) |
| 6) Mehmet Şeker | (Gaziantep) |
| 7) İhsan Özkes | (İstanbul) |
| 8) Atilla Kart | (Konya) |
| 9) Tufan Köse | (Çorum) |

- | | |
|------------------------------|-------------|
| 10) Mehmet Ali Ediboğlu | (Hatay) |
| 11) Ramazan Kerim Özkan | (Burdur) |
| 12) Kazım Kurt | (Eskişehir) |
| 13) Sinan Aydın Aygün | (Ankara) |
| 14) Özgür Özel | (Manisa) |
| 15) Metin Lütfi Baydar | (Aydın) |
| 16) Salih Fırat | (Adıyaman) |
| 17) Aytuğ Atıcı | (Mersin) |
| 18) Nurettin Demir | (Muğla) |
| 19) Mustafa Sezgin Tanrıkulu | (İstanbul) |
| 20) Ali Özgündüz | (İstanbul) |
| 21) Ferit Mevlüt Aslanoğlu | (İstanbul) |
| 22) Ali Rıza Öztürk | (Mersin) |
| 23) Sena Kaleli | (Bursa) |
| 24) Celal Dinçer | (İstanbul) |
| 25) Mehmet Şevki Kulkuloğlu | (Kayseri) |
| 26) Malik Ecder Özdemir | (Sivas) |

2. Milliyetçi Hareket Partisi Grubu adına Grup Başkanvekilleri İzmir Milletvekili Oktay Vural ve Mersin Milletvekili Mehmet Şandır'ın, yasa dışı telefon ve ortam dinleme iddialarının araştırılarak alınması gereken önlemlerin belirlenmesi amacıyla bir Meclis araştırması açılmasına ilişkin önergesi (10/471)

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Anayasada teminat altına alınan özel hayatın gizliliği ve korunması kapsamında özellikle haberleşme hürriyetinin, gayrimeşru yol ve yöntemlerle yapılan dinlemeler ve bunların servis edilmesiyle yoğun bir şekilde çığnendiği bilinmektedir. AKP Hükümeti'nin bugüne kadar bu iddiaları gerektiği gibi araştırarak gereken tedbirleri yeterince almadığı Başbakanın dinlenmesi iddiasıyla ortaya çıkmıştır. Bu nedenle, gerekçesini ekte sunduğumuz, yasa dışı dinleme ve gözetleme ile kamu görevlilerinin yaptığı dinlemelerin denetimi, bunların gerçekleştirildiği teknik imkân ve kabiliyetler ile yapılanmaların tespiti, idari, cezai ve hukuki düzenlemeler de dâhil olmak üzere alınacak tedbirlerin ve üretilecek çözümlerin tespiti için Anayasa'nın 98'inci, İçtüzüğü'nün 104-105'inci maddeleri gereğince Meclis araştırması açılmasını arz ederiz.

Oktay Vural
İzmir Milletvekili
MHP Grup Başkanvekili

Mehmet Şandır
Mersin Milletvekili
MHP Grup Başkanvekili

Gerekçe:

Gerçek demokrasilerin en belirgin niteliği "Çoğulculuktur". Herkesin düşündüğünü ifade edebildiği, istediği gibi yaşayabildiği bir rejimin adıdır demokrasi. Çoğulculuğun çerçevesini Anayasa'da belirtilen hak ve hürriyetlere getirilen tanımlar tayin eder. Bu tanımlardan birisi de Anayasa'mızın "Haberleşme hürriyeti" başlığını taşıyan 22'nci maddesidir. Bu maddede haberleşmenin gizliliğine atıfta bulunmaktadır. 22'nci maddeye göre gizliliğin temini için hâkim kararı, gecikmesinde sakınca bulunan hâllerde de yirmi dört saat içerisinde hâkim kararına çevrilmek kaydıyla yetkili merciin kararı gerekmektedir. Gizliliğin ihlali, başta özel hayatın ve konut dokunulmazlığının ihlali ve düşüncelerini rahatlıkla ifade edebilmenin engellenmesi olmak üzere birçok insan hak ve hürriyetinin ortadan kaldırılmasına da sebebiyet vermektedir.

Son yıllarda Anayasa'da teminat altına alınan haberleşme hürriyetinin gayrimeşru yöntemlerle yapılan dinlemelerle çığnendiği yönünde birçok olaylar ve iddialar

kamuoyuna yansımıştır. Hükümet bugüne kadar bu iddiaları bihakkın araştırıp, kamuoyunu rahatlatmak yerine beylik cümlelerle geçiştirmeyi ve iddiaları vuzuha kavuşturmadan üstünü örtbas etmeyi tercih etmiştir. Bu duruş, çoğulcu demokrasilerde halkın iradesi ile gelmiş bir hükümetin duruşu olmamalıdır. Hükümetin bu duyarsızlığı herkeste ve her kesimde rahatsızlık yaratmaktadır.

Üstelik dinlemenin hangi yöntemlerle yapıldığı, alınan dinleme izninin sınırlarının ne olduğu tam olarak anlaşılamayan uygulamalarla bazı mahkemelerin insan hürriyetini ortadan kaldıran mahkûmiyet kararları verdiği adli çevreler tarafından sıkça dillendirilmekte, bu konuda halktaki kaygılar daha da belirginleşmektedir.

Öte yandan, kamu görevlilerinin yaptığı dinlemelerin denetimi de ayrı bir sorun olarak karşımızdadır. Bu denetimlerinin fiili ve hukuki sınırlarının belirlenmesi gerektiği açıktır. Özellikle yasa dışı dinleme ve gözetleme ile ilgili sorumlularının bulunmaması bu dinleme ve gözetlemelerin birtakım kamu görevlileri tarafından yapıldığına ilişkin kanaatin yerleşmesine yol açmıştır. Nitekim Sayın Başbakanın dinleme konusunda bazı kamu görevlilerinin de olabileceği hususundaki ifadeleri bu kanaatin yansımasıdır. Oysaki devleti yöneten iradenin bu kaygıları ortadan kaldırması gerekmektedir. Bu durum, birbirlerine ve devletine karşı güvensizlik hisseden bir toplum yaratılmasına yol açmakta ve sonucu, ağır sosyal travmalara sebebiyet vermektedir.

Bu dinlemelerin zaman zaman siyaset arenasında da bir araç olarak kullanılması, sandıkta görülemeyen hesapların gayrimeşru dinlemelerle görülmek istenmesi böylece muhalefetin ve siyasetin tanzim edilmek istenmesi ve susturulması girişimlerine şahit olmak, yine son on yıldır ülkemizin karşılaştığı gerçeklerden biri hâline gelmiştir.

Kanun yapıcılar ve kanunu uygulayan hukuk adamlarının ise iktidar baskıları ile dinlemelerin nasıl ve kimler tarafından yapıldığı ile ilgilenmek yerine, dinlemelerin ortaya çıkardığı dedikodu ve söylentilerle ilgilenmeleri ve bu gündem ile meşgul olmaları demokratik hukuk devletlerinde rastlanılmayacak bir zafiyet oluşturmıştır.

Kamuoyuna yansıyan gayrimeşru dinlemelerin faillerinin bugüne kadar ortaya çıkarılamamış olması da bu iddiaları teyit eder niteliktedir.

Son günlerde ülkenin Başbakanının makam odasının dinlenebilmiş olması ihtimali ve bunun bizzat Başbakanca dillendirilmiş olması, yıllarca muhalefet tarafından ortaya

atılan bu iddiaların ciddiyetini bir kez daha ortaya koymakla birlikte, insanlarımızın daha güvensiz ve daha otokrat bir toplumda yaşadıklarına dair korkularını kuvvetlendirmiştir.

Gayrimeşru dinleme hadisesine ülke Başbakanının bizzat muhatap olması insanımızı çaresiz, karamsar ve güvensiz yapmıştır.

Anayasa Mahkemesinin Yüce Divan sıfatıyla gördüğü "Yargıda Rüşvet" davasında soruşturma esnasında elde edilen delillerin, dinleme ve ses kayıtlarının hukuka aykırı bulunmuş olması ve tüm sanıkların beraat ettirilmiş olması, öte taraftan bazı alt derece mahkemelerin hâlâ daha gayrimeşru dinlemelere dayanarak mahkûmiyet kararları veriyor olması da ayrı bir hukuki tartışma başlatmıştır.

Anayasa'da teminat altına alınan özel hayatın gizliliği ve korunması kapsamında özellikle haberleşme hürriyetinin, gayrimeşru yol ve yöntemlerle yapılan dinlemeler ve bunların servis edilmesiyle yoğun bir şekilde çiğnendiği bilinmektedir. AKP Hükümeti'nin bugüne kadar bu iddiaları gerektiği gibi araştırarak gereken tedbirleri yeterince almadığı Başbakanın dinlenmesi iddiasıyla ortaya çıkmıştır. Bu nedenle, gerekçesini ekte sunduğumuz, yasa dışı dinleme ve gözetleme ile kamu görevlilerinin yaptığı dinlemelerin denetimi, bunların gerçekleştirildiği teknik imkân ve kabiliyetler ile yapılanmaların tespiti, idari, cezai ve hukuki düzenlemeler de dâhil olmak üzere alınacak tedbirleri ve üretilecek çözümlerin tespiti için Anayasa'nın 98'inci, İçtüzüğü'nün 104 ve 105'inci maddeleri gereğince Meclis araştırması açılmasını arz ederiz.

3. İstanbul Milletvekili Mustafa Sezgin Tanrıkulu ve 30 Milletvekilinin, yasa dışı telefon ve ortam dinleme iddialarının araştırılarak alınması gereken önlemlerin belirlenmesi amacıyla Meclis araştırması açılmasına ilişkin önergesi (10/472)

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Toplumun her kesiminde yoğun tepkiye neden olan telefon dinlemeleri konusundaki belirsizlik ve hukuk dışı uygulamalar devam etmektedir. Anayasa'mızın haberleşme hürriyeti ile ilgili 22'nci maddesi herkesin haberleşme özgürlüğüne sahip olduğunu belirtir ve bu özgürlüğün temelini gizlilik olduğunu vurgular. Benzer şekilde, Türk Ceza Kanunu'nda (TCK) yer alan özel hayatın korunmasıyla ilgili düzenlemelerde izinsiz biçimde görüşmelerin kaydedilmesini, bu kayıtların yayınlanması açıkça suç kabul edilmektedir. Ceza Muhakemesi Kanunu (CMK), cumhuriyet savcısı dinlemeler sonunda suç delili bulunmadıysa, bunu on beş gün içinde ilgili kişiye "telefonlarınız dinlenmiştir, suç unsuru bulunamamıştır" yönünde bilgi verilmesini öngörmektedir. Fakat ülkemizde yasa dışı dinlemelerin mahkemelerde hukuka aykırı bir şekilde yargılama konusu olduğu gibi, olmayan dinlemelerde rivayetlerden yola çıkılarak iktidara muhalefet olan kişilerin cezalandırılması aracı hâline gelmiştir.

Tüm bunlara rağmen Hükûmetin, dinlemelerin kimin tarafından, hangi tarihte, hangi yolla ve ne amaçla yapıldığı konusunda net ve yeterli açıklamalar yapmaması, gerekli önlemleri almaması dikkat çekicidir. Telefon dinlemeleri yoluyla ülkemizde âdeta bir korku imparatorluğu yaratılmakta, vatandaşlarımızın haberleşme özgürlüğü bir anlamda kısıtlanmaktadır. Kısıtlanan özgürlük ülkemizde öyle bir hâl almış durumdadır ki yargının üst makamlarında görev alan kişiler dahi dinlenildiklerini ve takip edildiklerini sıradan bir olay gibi yansıtmaktadır.

Ülkemizde, son yıllarda özellikle insan hakları konusunda hızı bir türlü kesilmeyen hak ihlallerinin belki de en açık örneğini yasa dışı telefon dinlemeleri ve takip edilmelerle yaşamaktayız. İktidarı eleştiren veya iktidar aleyhine taraf olan kişiler bu tehditle hemen hemen her an karşı karşıya gelmektedir. Bu yasa dışılığın önüne geçilmemesi ve hatta ülke Başbakanının seçim meydanlarında dinlenme kasetlerinin müjdecî rolünü benimsemesi, bu tehdidin hangi amaçla kullanıldığını en açık şekilde ortaya koymaktadır. Her türlü uyarılara ve telkine rağmen bu alanda yapılan bu hukuksuzluk, mahkemelerce meşrulaştırılmakta ve yargının bu hukuksuzluk üzerinden adalet dağıtması beklenmektedir.

Telefon dinlemeleri ve takip sadece seçim meydanları ile sınırlı kalmamış, Başbakan tarafından ana muhalefet partisi liderine karşı da bir tehdit olarak kullanılmak istenmiştir. Başbakan, partisinin bir grup toplantısında, önlenilemediği için utanılması gereken bu hukuksuzluğa rağmen övünerek ana muhalefet liderinin her adımının izlendiği ve takip edildiğini büyük bir heyecan ve gaffet içerisinde kamuoyuna açıklamıştır.

Vatandaşlarımız ise bu gelişmeler doğrultusunda dostane sohbetlerini dahi telefon ortamına taşımaktan çekinir olmuştur. Bu konuyu esas alan kamuoyu araştırmaları vatandaşlarımızın hemen hemen tamamının dinlendiği şüphesiyle yaşadığı ve bu hak gasbının iktidarın baskısı nedeniyle âdeta bir kadermişçesine kabullendiğini ortaya koymaktadır. İleri demokrasi söylemleri ile atılan naralarının, vatandaşların bu cevapları da göz önünde bulundurularak ileri zorbalık uygulamalarını temsil ettiğini ispatlamaktadır.

İktidarın varlığını sürdürmek amacıyla yarattığı bu korku ve zorba uygulamalar yaklaşan yerel seçim sürecinde ise muhalefet partilerinin yerel yönetim yöneticilerine karşı bir silah olarak kullanılmak istenmektedir. Seçimde sağlanamayan başarı, temel insan hakları katliamına dönüşen hukuksuzluk yoluyla kazanılmak istenmektedir. Belediye başkanlarının halka hizmet etmekten başka görevi ve niyeti yoktur. İktidarlara da halk belediye başkanları ile aynı gayeyi taşımak için halk tarafından görevlendirilmelerine rağmen, ülkemizde iktidar ayyuka çıkan başarısızlıklarını korku düzeni inşa ederek yok etmek bu hukuksuzluktan insanlık adına utanç başarısı elde etme yolunu seçmektedir.

Tüm Türkiye'nin yakındığı bu durum, hukuksuzluğa seyirci kalan iktidar tarafından da maalesef geç de olsa seslendirilmektedir. Başbakan dinlenme olayının bir yıl öncesinde gerçekleşmesine rağmen, bu vahim olayı sıradan ve ülkemiz için olağan bir şekilde paylaşmıştır. Hukuksuz dinlemelerden yazılan iddianamelerde savcılığı ele alan, muhalefeti bu yol ile sindirmeye çalışan Başbakan kendisinin de dinlendiğini itiraf ederek yıllarca meşru olarak gördüğü bu hukuksuzluktan yakınmıştır. Koruma sayısının dünya üzerinde birçok ülkenin ordu nitelenmesine yaklaşan Başbakanın bu iddiaları da araştırılması gereken öneme sahiptir. Dinlenme olayının neden bir yıl sonra açıklandığı ve iktidarın bu zamana dek sıradan bir gelişme olarak yorumladığı bu tür girişimlere neden bir anda tavır aldığının cevabını tüm kamuoyu merak etmekte ve öğrenmek istemektedir. "Benim valim", "Benim polisim", "Benim sırdaş MİT Müsteşarım" nitelemelerine rağmen -ki son niteleme gayet ciddidir- ülke istihbaratı konusunda yetkili bir kişinin, Başbakanın

sırdaşı olmasına rağmen, bu hukuksuz istihbarat çalışması ne amaçla ve hangi menfaatle yapıldığının bilinmesi gerekmektedir. Bu konuda tüm kamuoyunun ortak tavrı nettir.

Kamuoyunu rahatsız eden, toplum nezdinde korku düzeni yaratılmasında etkili olan dinleme cihazlarına hangi yollarla ve nasıl ulaşıldığının tespit edilmesi, mahkeme kararı olmamasına rağmen hukuksuzca dinlemelerin hangi kitlelerce ve ne amaçla yapıldığının tespit edilmesi, Başbakanın bir yıl öncesinde gerçekleşen bir dinleme olayını açıklama zaman diliminin önemi ve gerekçesinin tespiti, bu dinlemenin kimler tarafından ve ne tür bir maksatla yapıldığının tespit edilmesi, ülkemizde siyasilere karşı şantaj aracı olarak kullanılmasının ne tür ihmaller sonucu yaygınlaştığının tespit edilmesi ve sorumlular hakkında yasal sürecin başlatılması, yargı kararı olmaksızın dinlemelerle menfaat elde etmek isteyen sorumluların tespit edilmesi ve haklarında yasal sürecin başlatılması ve son olarak toplum nezdinde oluşan kaygıları ortadan kaldırmak için gerekli önlemlerin belirlenmesi amacıyla Anayasa'mızın 98'inci, Türkiye Büyük Millet Meclisi İç Tüzüğü'nün 104'üncü ve 105'inci maddeleri gereğince Meclis araştırması açılması için gereğini saygılarımızla arz ederiz.

- | | |
|-----------------------------|-------------|
| 1) Mustafa Sezgin Tanrıkulu | (İstanbul) |
| 2) Gürsel Tekin | (İstanbul) |
| 3) Veli Ağbaba | (Malatya) |
| 4) Muharrem Işık | (Erzincan) |
| 5) Erdoğan Toprak | (İstanbul) |
| 6) Mehmet Şeker | (Gaziantep) |
| 7) Musa Çam | (İzmir) |
| 8) Mahmut Tanal | (İstanbul) |
| 9) Hasan Ören | (Manisa) |
| 10) Ayşe Nedret Akova | (Balıkesir) |
| 11) Mehmet Hilal Kaplan | (Kocaeli) |
| 12) Haluk Eyidoğan | (İstanbul) |
| 13) Süleyman Çelebi | (İstanbul) |
| 14) Kamer Genç | (Tunceli) |
| 15) Mehmet Ali Ediboğlu | (Hatay) |

- | | |
|-------------------------|------------------|
| 16) Bülent Tezcan | (Aydın) |
| 17) Ramazan Kerim Özkan | (Burdur) |
| 18) Namık Havutça | (Balıkesir) |
| 19) Haydar Akar | (Kocaeli) |
| 20) İhsan Özkes | (İstanbul) |
| 21) Doğan Şafak | (Niğde) |
| 22) Celal Dinçer | (İstanbul) |
| 23) Gürkut Acar | (Antalya) |
| 24) Haluk Koç | (Samsun) |
| 25) İzzet Çetin | (Ankara) |
| 26) Refik Eryılmaz | (Hatay) |
| 27) Mevlüt Dudu | (Hatay) |
| 28) Aytuğ Atıcı | (Mersin) |
| 29) Ali Sarıbaş | (Çanakkale) |
| 30) Osman Aydın | (Aydın) |
| 31) Ahmet Toptaş | (Afyonkarahisar) |

4. Adalet ve Kalkınma Partisi Grubu Adına Grup Başkanvekilleri Giresun Milletvekili Nurettin Canikli, Kayseri Milletvekili Mustafa Elitaş, İstanbul Milletvekili Ayşe Nur Bahçekapılı, Adıyaman Milletvekili Ahmet Aydın, Kahramanmaraş Milletvekili Mahir Ünal ve 135 Milletvekilinin, Yasa Dışı Telefon ve Ortam Dinleme İddialarının Araştırılarak Alınması Gereken Önlemlerin Belirlenmesi Amacıyla Bir Meclis Araştırması Açılmasına İlişkin Önergesi (10/473)

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Kişiler arasındaki haberleşme içeriklerinin hukuka aykırı biçimde tespiti, dinlenmesi ve kayda alınması veya kişilerin gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının görüntülü veya sesli olarak saptanması ve kaydedilmesi, kimi zaman bunların çeşitli medya ortamlarında yayınlanması gibi suç teşkil eden faaliyetlerin nasıl ve hangi araçlar kullanılarak yapıldığının, bu araçların nasıl temin edildiğinin, bu araçların imal, ithal ve bulundurulması konusunda yasal bir kısıtlama bulunup bulunmadığının ve yaşanan bu sorunun çözümü amacıyla alınması gereken yasal, idari, istihbari ve diğer önlemlerin tespiti için Anayasamızın 98, İçtüzüğü'nün 104 ve 105'inci maddeleri gereğince "Yasa dışı dinlemelerin ve teknolojik araçlarla özel hayatın gizliliğine yönelik ihlallerin tespiti, önlenmesi ve gerekli tedbirlerin alınması" konusunda bir Meclis araştırma komisyonu kurulmasını arz ve teklif ederiz.

- | | |
|-------------------------|-----------------|
| 1) Nurettin Canikli | (Giresun) |
| 2) Mustafa Elitaş | (Kayseri) |
| 3) Ayşe Nur Bahçekapılı | (İstanbul) |
| 4) Ahmet Aydın | (Adıyaman) |
| 5) Mahir Ünal | (Kahramanmaraş) |
| 6) Zeyid Aslan | (Tokat) |
| 7) Bülent Turan | (İstanbul) |
| 8) Ramazan Can | (Kırıkkale) |
| 9) Mehmet Doğan Kubat | (İstanbul) |
| 10) Enver Yılmaz | (İstanbul) |
| 11) Akif Çağatay Kılıç | (Samsun) |
| 12) Mehmet Müezzinoğlu | (Edirne) |

- | | |
|---------------------------|--------------|
| 13) Oya Eronat | (Diyarbakır) |
| 14) Harun Karaca | (İstanbul) |
| 15) Ali Ercoşkun | (Bolu) |
| 16) Ahmet Öksüzkaya | (Kayseri) |
| 17) Hüseyin Şahin | (Bursa) |
| 18) Ahmet Baha Öğütken | (İstanbul) |
| 19) Yılmaz Tunç | (Bartın) |
| 20) Sermin Balık | (Elâzığ) |
| 21) Ömer Faruk Öz | (Malatya) |
| 22) Cuma İçten | (Diyarbakır) |
| 23) Ertuğrul Soysal | (Yozgat) |
| 24) Necdet Ünüvar | (Adana) |
| 25) Mustafa Ataş | (İstanbul) |
| 26) İdris Şahin | (Çankırı) |
| 27) Gürsoy Erol | (İstanbul) |
| 28) Salim Uslu | (Çorum) |
| 29) Mine Lök Beyaz | (Diyarbakır) |
| 30) Mehmet Kerim Yıldız | (Ağrı) |
| 31) Derya Bakbak | (Gaziantep) |
| 32) Mustafa Bilici | (Van) |
| 33) Fatih Çiftci | (Van) |
| 34) İsmail Aydın | (Bursa) |
| 35) Ali Boğa | (Muğla) |
| 36) Çiğdem Münevver Ökten | (Mersin) |
| 37) Osman Kahveci | (Karabük) |
| 38) Hasan Ali Çelik | (Sakarya) |
| 39) Nusret Bayraktar | (Rize) |
| 40) Ekrem Çelebi | (Ağrı) |
| 41) Muammer Güler | (Mardin) |

42) İlyas Şeker	(Kocaeli)
43) Nurcan Dalbudak	(Denizli)
44) H. Hami Yıldırım	(Burdur)
45) Ayşenur İslam	(Sakarya)
46) Abdullah Nejat Koçer	(Gaziantep)
47) Aydın Bıyıklıoğlu	(Trabzon)
48) Alpaslan Kavaklıoğlu	(Niğde)
49) Abdülkerim Gök	(Şanlıurfa)
50) Mehmet Ersoy	(Sinop)
51) Vural Kavuncu	(Kütahya)
52) Osman Boyraz	(İstanbul)
53) Ali Rıza Alaboyun	(Aksaray)
54) Mahmut Mücahit Fındıklı	(Malatya)
55) Muzaffer Baştopçu	(Kocaeli)
56) Durdu Mehmet Kastal	(Osmaniye)
57) Mehmet Akyürek	(Şanlıurfa)
58) Tülay Bakır	(Samsun)
59) Mustafa Şahin	(Malatya)
60) Abdurrahim Akdağ	(Mardin)
61) Türkan Dağoğlu	(İstanbul)
62) Hacı Bayram Türkoğlu	(Hatay)
63) Adnan Yılmaz	(Erzurum)
64) Ünal Kacır	(İstanbul)
65) Tülay Kaynarca	(İstanbul)
66) Mustafa Gökhan Gülşen	(Kastamonu)
67) Sevim Savaşer	(İstanbul)
68) Muzaffer Aslan	(Kırşehir)
69) Ahmet Haldun Ertürk	(İstanbul)
70) Oktay Saral	(İstanbul)

71) Bilal Uçar	(Denizli)
72) Cahit Bağcı	(Çorum)
73) Osman Ören	(Siirt)
74) Mustafa Kemal Şerbetçioğlu	(Bursa)
75) Feyzullah Kıyıklık	(İstanbul)
76) Muhammet Bilal Macit	(İstanbul)
77) Mehmet Yüksel	(Denizli)
78) Faruk Septioğlu	(Elâzığ)
79) Hasan Fehmi Kinay	(Kütahya)
80) Soner Aksoy	(Kütahya)
81) Ahmet Yeni	(Samsun)
82) Ülker Güzel	(Ankara)
83) Mehmet Ali Okur	(Kocaeli)
84) Mehmet Cemal Öztaylan	(Balıkesir)
85) Mehmet Emin Dindar	(Şırnak)
86) Ali Şahin	(Gaziantep)
87) Burhan Kuzu	(İstanbul)
88) Şamil Tayyar	(Gaziantep)
89) Ahmet Kutalmış Türkeş	(İstanbul)
90) Tevfik Ziyaeddin Akbulut	(Tekirdağ)
91) Hüseyin Çelik	(Gaziantep)
92) Kemalettin Aydın	(Gümüşhane)
93) Halil Mazıcıoğlu	(Gaziantep)
94) Mehmet Öntürk	(Hatay)
95) Nevzat Pakdil	(Kahramanmaraş)
96) Adem Yeşildal	(Hatay)
97) Haluk Özdalga	(Ankara)
98) Mehmet Geldi	(Giresun)
99) Zülfü Demirbağ	(Elâzığ)

100) Recep Özel	(Isparta)
101) Yunus Kılıç	(Kars)
102) Hüseyin Samani	(Antalya)
103) Şirin Ünal	(İstanbul)
104) Hasan Karal	(Rize)
105) Ali İhsan Yavuz	(Sakarya)
106) Muzaffer Yurttaş	(Manisa)
107) İlknur Denizli	(İzmir)
108) Tülay Babuşcu	(Balıkesir)
109) Ziver Özdemir	(Batman)
110) Hüseyin Filiz	(Çankırı)
111) Muhyettin Aksak	(Erzurum)
112) Hilmi Bilgin	(Sivas)
113) Mevlüt Akgün	(Karaman)
114) Yüksel Özden	(Muğla)
115) İsmet Su	(Bursa)
116) Muzaffer Çakar	(Muş)
117) Ali Turan	(Sivas)
118) Ebu Bekir Gizligider	(Nevşehir)
119) Erol Kaya	(İstanbul)
120) Süreyya Sadi Bilgiç	(Isparta)
121) Osman Çakır	(Düzce)
122) Sıtkı Güvenç	(Kahramanmaraş)
123) Azize Sibel Gönül	(Kocaeli)
124) Mustafa Öztürk	(Bursa)
125) İbrahim Korkmaz	(Düzce)
126) Salih Koca	(Eskişehir)
127) Gökçen Özdoğan Enç	(Antalya)
128) Muhammed Murtaza Yetiş	(Adıyaman)

129) Şuay Alpay	(Elâzığ)
130) Metin Külünk	(İstanbul)
131) Özlem Yemişçi	(Tekirdağ)
132) İsmail Güneş	(Uşak)
133) Adem Tatlı	(Giresun)
134) Nihat Zeybekci	(Denizli)
135) Hakan Çavuşoğlu	(Bursa)
136) Abdullah Çalışkan	(Kırşehir)
137) Ülker Can	(Eskişehir)
138) Nesrin Ulema	(İzmir)
139) İlhan Yerlikaya	(Konya)
140) Öznur Çalık	(Malatya)

Gerekçe:

Anayasamızda kişinin hak ve ödevleri başlığı altında temel hak ve hürriyetlerin korunması amacıyla özel hayatın gizliliği ve haberleşme hürriyeti güvence altına alınmıştır.

Anayasa'nın 12. maddesinde, *“Herkes, kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir. Temel hak ve hürriyetler, kişinin topluma, ailesine ve diğer kişilere karşı ödev ve sorumluluklarını da ihtiva eder.”* hükmüne yer verilmiştir. Anayasa'nın 13. maddesinde ise, temel hak ve hürriyetlerin, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği, bu sınırlamaların Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı belirtilmiştir.

Anayasa'nın 20. maddesi ile özel hayatın gizliliği ve korunması güvence altına alınmıştır. Maddenin birinci fıkrasında *herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu ve özel hayatın ve aile hayatının gizliliğine dokunulamayacağı*; ikinci fıkrasında ise özel hayatın gizliliğine ilişkin hakkın sınırlandırılma koşulları belirtilmiştir.

Anayasa'nın 22. maddesinde ise herkesin haberleşme hürriyetine sahip olup haberleşmenin gizliliğinin esas olduğu, maddede sayılan durumlar dışında herhangi bir nedenle bu hürriyetin engellenemeyeceği öngörülmüştür. 22.maddeye göre; *“Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır./Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar./İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.”*

Anayasa Mahkemesi'ne göre; “Anayasa'nın 22. maddesinde öngörülen haberleşme özgürlüğü, kişinin kesintiye uğramadan ve sansür edilmeden başkalarıyla iletişim kurma hakkıdır. Bu özgürlük, çok daha geniş bir alanı kaplayan “özel hayatın” bir yönünü oluşturur. Dolayısıyla *“haberleşmenin gizliliği”* kavramı, özel hayatın gizliliği kavramı içinde yer alır....Özel hayatın gizliliği ile haberleşmenin gizliliği, her türlü yasa dışı müdahaleye karşı Anayasa ve diğer yasalarla güvence altına alınmıştır.” (AYMK.E.2008/115,K. 2011/86,T. 2.6.2011;AYMK.E. 1996/68 ,K. 1999/1,T. 6.1.1999)

Anayasa'nın 22. maddesinde öngörülen bu güvence, hiç şüphesiz, üçüncü şahısların haberleşme özgürlüğüne yasa dışı müdahalelerini de kapsamaktadır.

Tarafı olduğumuz ve onaylamakla iç hukuk mevzuatına dahil ettiğimiz "Avrupa İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi"nin 8. maddesinde de herkesin haberleşmesine saygı gösterilmesi hakkına sahip olduğu kurala bağlanmış, bu hakka bir kamu otoritesinin müdahalesinin ancak, ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlâkın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda gerekli olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabileceği belirtilmiştir.

Kişiler arasındaki haberleşme içeriklerinin suç öncesi veya belli bir suça ilişkin soruşturma kapsamında Anayasa ve kanunların belirlediği koşullar çerçevesinde öğrenilmesinin veya kayda alınmasının hukuka uygun olduğu muhakkaktır.

1412 sayılı CMUK.nun yürürlükte olduğu 1999 öncesi dönemde haberleşmenin dinlenmesi ve denetlenmesi konusunda herhangi bir düzenleyici kural öngörülmemiştir. Uygulamada CMUK.nun 91. maddesinde yer alan, sanığa gönderilen mektuplar ve sair mersulenin zapt edilebileceğine ilişkin kuralın kıyasen uygulanması suretiyle haberleşmeler denetlenmiş ise de bu tür kanıt derlemeleri özellikle öğretilerde yoğun eleştirilere konu edilmiştir.

Ülkemizde iletişimin denetlenmesi ve telefonların dinlenmesi, 1 Haziran 2005 tarihine kadar 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu, bu tarihten itibaren ise 5271 sayılı Ceza Muhakemesi Kanunu ile düzenlenmiştir.

Bu kapsamda 1/6/2005 tarihinde yürürlüğe giren 5271 sayılı Ceza Muhakemesi Kanununun 135 ve devamı maddelerinde, bir suç dolayısıyla yapılan soruşturma ve kovuşturmada “İletişimin tespiti, dinlenmesi ve kayda alınması” ve “Teknik araçlarla izleme yoluyla” ses veya görüntü kaydının alınabilmesine dair usul ve esaslar düzenlenmiştir. Anılan düzenlemeler suçların soruşturulması sırasında ve sanık takibi amacıyla kolluk kuvvetlerince iletişime yapılan müdahaleye ilişkin olup, sadece suç işlendikten sonra” yapılan, adli amaçlı dinlemeleri kapsamaktadır. Ayrıca, 5271 sayılı Ceza Muhakemesi Kanununda yapılan düzenlemeye göre, dinleme adli kolluk tarafından gerçekleştirilecektir.

5271 sayılı Ceza Muhakemesi Kanununun;

1- *“İletişimin tespiti, dinlenmesi ve kayda alınması”* kenar başlıklı 135. maddesinde, bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişiminin tespit edilebileceği, dinlenebileceği, kayda alınabileceği ve sinyal bilgilerinin değerlendirilebileceği, Cumhuriyet savcısı tarafından verilen kararların derhâl hâkimin onayına sunulacağı; 135.maddenin 6.fıkrasında ise;Bu madde kapsamında dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümlerin ancak fıkrada sayılan (katalog) suçlarla ilgili olarak uygulanabileceği;

2- *“Kararların yerine getirilmesi, iletişim içeriklerinin yok edilmesi”* kenar başlıklı 137. maddesinde, 135. maddeye göre verilen kararın uygulanması sırasında şüpheli

hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hâkim onayının alınamaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhâl son verileceği; bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtların Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durumun bir tutanakla tespit edileceği; tespit ve dinlemeye ilişkin kayıtların yok edilmesi halinde soruşturma evresinin bitiminden itibaren, en geç onbeş gün içinde, Cumhuriyet başsavcılığının, tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgisine yazılı olarak bilgi verileceği;

3- "*Teknik araçlarla izleme*" kenar başlıklı 140. maddesinde, maddede sayılan suçların işlendiği hususunda kuvvetli şüphe sebeplerinin bulunması ve başka suretle delil elde edilememesi halinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetlerinin ve işyerinin teknik araçlarla izlenebileceği, ses veya görüntü kaydının alınabileceği, teknik araçlarla izlemeye hâkim, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından karar verileceği, Cumhuriyet savcısı tarafından verilen kararların yirmidört saat içinde hâkim onayına sunulacağı;

hükme bağlanmıştır.

Diğer yandan suç ve suçluluk ile mücadelede istihbarat vazgeçilmez bir araçtır. İstihbarat çalışmaları ise, bilgi toplamak ve depolamak şeklinde olduğundan, özel hayat ve aile hayatı ile yakından ilgilidir. Elektronik yoldan yapılan iletişimin suç öncesi alanda dinlenmesi ise, haberleşme hürriyeti ile ilgilidir. Anayasal düzenlemeler karşısında, Türkiye’de istihbarat hizmetleri ancak bir kanuna dayalı olarak yapılabilecektir. İstihbarat teşkilatları tarafından yürütülen faaliyetler; suç ile ilişkili olmayıp kuruluş yasalarında yer alan görevleri kapsamında ulusal güvenliğin sağlanması amacıyla, demokratik hukuk devletine yönelik tehdit unsurlarına ilişkin olarak düzenli ve sistemli bilgi toplama ve değerlendirmeyi gerekli kıldığından; 3.7.2005 tarih ve 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile AB kriterleri, Anayasanın 22 nci maddesinde yer alan temel ilkeler ve 5271 sayılı Ceza Muhakemesi Kanununda belirtilen esaslara bağlı kalınarak, iletişime müdahalenin "hangi hallerde" yapılacağı, "karar mercii" ve "süresi" şeklindeki temel unsurlara yer verilmek suretiyle "*önleyici amaçlı istihbarat dinlemesi*" ne dair düzenlemeler yapılmıştır. Bu çerçevede 2559 sayılı Polis Vazife ve Salahiyet Kanununun ek 7. maddesinde, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun ek 5. maddesinde, 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat

Teşkilatı Kanununun "Yetkiler" kenar başlıklı 6. maddesinde, önleyici, koruyucu veya istihbari tedbirler kapsamında telekomünikasyon yoluyla yapılan iletişimin *hâkim kararıyla tespit edilebileceği*, dinlenebileceği, sinyal bilgilerinin değerlendirilebileceği ve kayda alınabileceği düzenlenmiştir.

Öte yandan 3.7.2005 tarih ve 5397 sayılı Kanunun 1.maddesi ile 2559 sayılı Polis Vazife ve Salahiyet Kanununun ek 7. Maddesine eklenen fıkra hükümlerine göre; *“Bu maddede belirtilen işlemler ile 5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak dinlemeler, Telekomünikasyon Kurumu bünyesinde, Kurum başkanına doğrudan bağlı “Telekomünikasyon İletişim Başkanlığı” adıyla kurulan tek bir merkezden yürütülür.Bu maddede belirlenen usûl ve esaslara aykırı dinlemeler hukuken geçerli sayılmaz ve bu şekilde dinleme yapanlar hakkında 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu hükümlerine göre işlem yapılır.”*

Yukarıda açıklanan hükümler çerçevesinde, telekomünikasyon yoluyla iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine ilişkin kararların, hangi kurumlar tarafından hangi şartlarda alınabileceği, kararların hangi mahkemeler tarafından verilebileceği, kararların taşınması gereken zorunlu unsurlar, bu kararların hangi kolluk birimlerince yerine getirileceği ve kayıtların kimlerin sorumluluğunda olduğu hususlar mevzuatta ayrıntılı olarak belirlenmiştir. Telekomünikasyon İletişim Başkanlığı tarafından resen dinleme yapılmamakta, dinlemeler talep üzerine mahkemelerce verilen kararlar çerçevesinde yerine getirilmektedir. Buna göre, hâkim kararı bulunmadıkça, gecikmesinde sakınca bulunan durumlarda ise yirmidört saat içinde hâkim onayı alınmadıkça dinleme yapılabilmesi hukuken mümkün değildir.

5237 sayılı Türk Ceza Kanunu’nun 132 ila 140.maddelerinde *“Özel Hayata Ve Hayatın Gizli Alanına Karşı Suçlar”* yaptırıma bağlanmış; 2/7/2012 tarihli ve 6352 sayılı Kanun ile söz konusu maddelerdeki cezalar da artırılmıştır.

TCK’nın “Haberleşmenin gizliliğini ihlal” başlıklı 132.maddesine göre;

“Madde 132- (1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. **(Ek cümle: 2/7/2012-6352/79 md.)** Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

TCK’nın “Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması” başlıklı 133.maddesine göre;

“Madde 133- (1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.

(3) **(Değişik: 2/7/2012-6352/80 md.)** Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dört bin güne kadar adli para cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

TCK’nın “Özel hayatın gizliliğini ihlal” başlıklı 134.maddesine göre;

“Madde 134- (1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.

(2) **(Değişik: 2/7/2012-6352/81 md.)** Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

Yukarıda açıklanan mevzuat çerçevesinde; kişiler arasındaki haberleşme içeriklerinin hukuka aykırı biçimde tespiti, dinlenmesi ve kayda alınması suç olduğu gibi ;kişilerin gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının görüntülü veya sesli olarak saptanması ve kaydedilmesi de suçtur.

Tüm bu yasal düzenlemelere ve etkin cezai yaptırımlara rağmen kamuoyunda böcek, gizli kamera veya uzaktan dinleme sistemi gibi dünyadaki teknik gelişmelerin bu konudaki sağladığı tüm imkân ve yöntemleri yasa dışı biçimde kullanarak kişiler arasındaki konuşmaların dinlendiği, kayda alındığı ve bu kayıtların kimi zaman basın yayın yoluyla hukuka aykırı bir şekilde kullanıldığı yönünde kamuoyunda bir algı olduğu gözlemlenmektedir.

Bu çerçevede;

-Ses ve görüntü kaydedici cihazları kişilerin konut veya işyerlerine hukuka aykırı biçimde yerleştirmek suretiyle ses ve görüntü kaydı yapılması;

-Üstün teknolojik araçlarla belli bir mesafeden kişinin bulunduğu ortamda yapılan konuşmaların hukuka aykırı olarak dinlenmesi ve kayda alınması;

-Bilgisayar üzerinden kişisel verilerin yasa dışı yollarla ele geçirilmesi veya kişiye ait ses ve görüntülerin rızası dışında elde edilmesi,

-Kişilerin cep telefonlarının mesajlaşma trafiğini veya kayıtlı bilgilerinin yasa dışı yollarla izlenmesi ve kaydedilmesi;

Gibi kamuoyunda ciddi rahatsızlık meydana getiren sorunların vatandaşlarımızdan gelen yoğun şikayet ve talepler dikkate alınarak, sorunun çözüm yolları ve alınması gereken yasal, idari, istihbari ve gerekli diğer tüm tedbirlerin tespiti amacıyla Türkiye Büyük Millet Meclisi tarafından bir araştırma yapılması kamuoyunun yasama organından bir beklentisi haline gelmiştir.

Bu bağlamda yasa dışı dinlemelerin hangi araçlar kullanılarak yapıldığının, bu araçların nasıl temin edildiğinin, bu araçların imal ithal ve bulundurulması konusunda mevzuatta herhangi bir eksiklik olup olmadığı ve yaşanan bu sorunun çözümü amacıyla alınması gereken yasal, idari ve istihbari ve diğer önlemlerin tespiti için yüce meclisimize sorumluluk düşmektedir. Yüce meclisimizin bu sorumluluğu yerine getirmesi için bir meclis araştırma komisyonu kurulması gerekmektedir.

5. Şırnak Milletvekili Hasip Kaplan ve 21 Milletvekilinin, yasa dışı telefon ve ortam dinleme iddialarının araştırılarak alınması gereken önlemlerin belirlenmesi amacıyla bir Meclis araştırması açılmasına ilişkin önergesi (10/474)

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

"Gizli dinleme", "Teknik takip" adı ile bilinen, dinleme ve izleme gündemden düşmüyor. Bu gidişle gündemden düşecek gibi de gözüküyor. İnsanların özel, siyasi, mesleki ve aile hayatları daima merak ve ilgi konusu olmuştur. Ancak bunun bir sınırının olduğu ve insanların, bu sınırı çizen yasalara ve uygulayıcılarına güvenmek istediği tartışmasız ortadadır. Hem yasal ve hem de yasa dışı dinleme ve izlemelere karşı, kişi hak ve hürriyetlerinin etkin bir şekilde korunmasının zamanı çoktan gelmiştir. Bu husus herkesin ortak sorunudur. Gizli dinleme ve izleme ile ilgili yürürlükteki hukuk kuralları tam olarak uygulanmalı, bu konuda yetersiz olan hukuk kuralları en kısa sürede giderilmelidir. Yıllardan beri süregelen ve en son olarak da Başbakan Sayın Recep Tayyip Erdoğan'ın kendi açıklamasıyla ortaya çıkan Başbakanın evinin altındaki çalışma ofisi ile Türkiye Büyük Millet Meclisindeki makam odasında gizli dinleme cihazları tespit edilmiştir. Bu konuda gerekli araştırmaların yapılması ve önlemlerin alınması için Anayasanın 98'inci, İçtüzüğü'nün 104 ve 105'inci maddeleri uyarınca Meclis araştırması açılmasını arz ve teklif ederiz.

- | | |
|----------------------------|--------------|
| 1) Hasip Kaplan | (Şırnak) |
| 2) Pervin Buldan | (İğdır) |
| 3) İdris Baluken | (Bingöl) |
| 4) Sırrı Sakık | (Muş) |
| 5) Murat Bozlak | (Adana) |
| 6) Halil Aksoy | (Ağrı) |
| 7) Ayla Akat Ata | (Batman) |
| 8) Hüsamettin Zenderlioğlu | (Bitlis) |
| 9) Emine Ayna | (Diyarbakır) |
| 10) Nursel Aydoğan | (Diyarbakır) |
| 11) Altan Tan | (Diyarbakır) |
| 12) Adil Kurt | (Hakkâri) |

13) Esat Canan	(Hakkâri)
14) Sırrı Süreyya Önder	(İstanbul)
15) Sebahat Tuncel	(İstanbul)
16) Mülkiye Birtane	(Kars)
17) Erol Dora	(Mardin)
18) Ertuğrul Kürkcü	(Mersin)
19) Demir Çelik	(Muş)
20) İbrahim Binici	(Şanlıurfa)
21) Nazmi Gür	(Van)
22) Özdal Üçer	(Van)

Gerekçe:

Gizli dinleme, telekulak, haberleşmenin ve kişilik haklarının ihlali gündemini korumakla birlikte her geçen gün daha da artmaktadır. Başbakanın Anayasa Mahkemesine, Genelkurmay Başkanlığından Hükûmete, siyasi partilerden bürokrasiye, iş adamlarından sade vatandaşa kadar hemen hemen herkes dinlemeden şikâyet etmekte ve kaygı duymaktadır. Adına "çete", "gladio", "derin devlet" veya "kontrgerilla" ne denirse densin yasa dışı suç örgütlerinin en çok başvurduğu bu yöntem sonucu ortalığa saçılanlar dehşet verici hâle gelmiştir. Teknoloji, bilişim, uydu yayınları derken cep telefonlarından "böcek" tabir edilen dinleme cihazlarına, lazer ışınlarından çanaklara, SMS, e-mail, İnternet üzerinden normal yaşamda hayatın her alanına giren gizli dinlemeyi en çok suç çeteleri, dedektifler, rakip şirketler, siyasi muhalifler hemen hemen herkes ilgi alanı içinde görmektedir. Gizlilik kaydı olan en üst düzey askerî görüşmeler, uluslararası görüşmeler önceden sosyal medyaya düşmektedir.

Yazılı ve görsel medyaya yansıyanlar bu konuda güvenlik ortamının sıfıra indiği, hiç kimsenin güvencesinin kalmadığı, her yapılanın da yapanın yanına kâr kaldığı bir uygulama hukuk devletini derinden yaralamaktadır. Yabancı ajanlar cirit atmakta, yerli iş birlikçiler üç kuruşa ülkenin sırlarını satmaktadır. Siyasi, sivil alan, ticaret, asker, polis, yargıda tedirginlik had safhaya ulaşmıştır.

Mikro ses kayıt cihazları, dijital ses ve telefon kayıt cihazları, casus kalem, gözlük, anahtarlık kameralar, mikro kulaklıklar, dinleme sistemleri, GSM ortam dinleme, bilgisayardan dinleme, izleme, her türlü cihaz sokakta, İnternet üzerinden alışverişlerde

ekmek peynir gibi rahatlıkla satılmakta ve alınabilmektedir. Bu tür cihazlarla tehdit, şantaj, kişilik haklarına saldırı, yasa dışı menfaat sağlama sıradan vaka hâline gelmiştir. Ceza yargılamasının en tartışılan delil türü olarak "gizli dinleme" kayıtları geçiyor, ortalık kasetlerden, ses kayıtlarından geçilmiyor.

Gizli dinleme, kişilerin özel hayatları kapsamındaki bilgilere izinsiz erişerek onların özel hayat haklarını ihlal eden bir durumdur. Özel hayat hakkı ya da mahremiyet hakkı olarak isimlendirilen ve gizli dinleme ile ihlal edilen bu hak, gerek Avrupa İnsan Hakları Sözleşmesi gibi milletlerarası belgelerde gerekse de hemen hemen tüm ülkelerin anayasalarında, temel haklar kategorisine konulmuştur. Esasen gizli dinlemenin bir anayasal hak ihlali olduğu dolaylı olarak 1950 Avrupa Temel Özgürlüklerin ve İnsan Haklarının Korunması Sözleşmesi'nin 8'inci maddesinde, Türkiye'de Anayasa'nın 22'nci maddesinde belirtilmekte olup cezai müeyyidelerde TCK'nın 133 ve 140'ıncı maddelerinde belirtilmektedir.

İnsanlığın ulaştığı evrensel gelişmişlik seviyesi ve bu seviyede beliren ortak akıl, bireyin özel hayatını ve iletişimini mutlak bir koruma altına almıştır. Bu koruma, sadece kuvvetli bir suç şüphesinin varlığı hâlinde, suçla bozulan toplumsal barış ve huzurun yeniden tesisi amacıyla, başka yoldan delil elde etme imkânı da yoksa ve hâkim tarafından karar verilmiş olması şartıyla askıya alınabilmektedir. Ortak akıl, toplumsal gelişme imkânının açık tutulması amacıyla, bireysel özgürlüklerin azami seviyede gerçekleştirilip, korunması gayesi arasındaki özel iletişimini dinleyen ya da kaydeden kişi, kim olursa olsun, hukuka uygun olarak verilmiş bir hâkim kararına dayanmıyorsa suç işlemektedir. Bu kişi veya kişilerin yaptığı kayıt delil olmayacağı gibi, bu suretle elde ettiği bilgiyi tanık olarak da beyan edemez, bu hususta verdiği beyan da mutlak olarak hukuka aykırıdır. Özel hayat hakkını koruyan ceza normları gözden geçirilmeli, bu suçların yaptırımları ağırlaştırılmalıdır. Bu çerçeveye, tümü ile hukuka aykırı olarak yapılan gizli dinlemeler, dinleme ve takipler sonucu elde edilen veri ve delillerin kötüye kullanılması, bunları yapan kamu görevlilerinin şikâyetine bağlı olmaksızın daha ağır cezalarla cezalandırılmaları dâhil edilmelidir.

İletişimin denetlenmesi kararları gizli olduğundan ve ilgilisi tarafından hemen itiraza konu edilemediğinden, bu tür kararların alınması ve uygulamaları sırasında somut olayın özellikleri karşısında yasal şartların bulunup bulunmadığı sıkı bir şekilde incelenmeli, iletişimin denetlenmesi kararlarında sadece soyut yasal dayanaklara değil,

somut gerekçelere yer verilmeli, karar veren makam dışında konusunda uzman hâkimler tarafından yerine getirilmelidir.

Tüm bu konuların araştırılması, yasal düzenlemelerin yapılması ve önlemlerin alınması için araştırma komisyonu kurulmasında yarar bulunmaktadır.

6. Barış ve Demokrasi Partisi Grubu adına Grup Başkanvekilleri Iğdır Milletvekili Pervin Buldan ve Bingöl Milletvekili İdris Baluken'in, yasa dışı telefon ve ortam dinleme iddialarının araştırılarak alınması gereken önlemlerin belirlenmesi amacıyla Meclis araştırması açılmasına ilişkin önergesi (10/475)

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Muhaberatın, özel hayatın gizliliğini ortadan kaldıran ve açık bir insan hakkı ihlali teşkil eden ortam dinlemesi hususunda neler yapılabileceği ve mevcut sorunların gündeme taşınması amacıyla Anayasanın 98'inci, İçtüzüğü'nün 104 ve 105'inci maddeleri gereğince Meclis Araştırması açılması için gereğini BDP Grubu adına arz ederiz.

Pervin Buldan

İdris Baluken

Iğdır Milletvekili

Bingöl Milletvekili

BDP Grup Başkanvekili

BDP Grup Başkanvekili

Gerekçe:

Kanuna aykırı biçimde yapılan ve adına ise ister önleme, ister adli, ister ortam dinlemesi densin, netice itibarıyla muhaberatın gizliliği esası ortadan kalkmış durumdadır. Son yıllarda hukuka aykırı dinlemeler artmış; bu durum, son birkaç yıldır tüm eleştiri ve hukuka aykırılığın giderilmesi adına yürütülen çabalara rağmen devam etmektedir. Önceleri Adalet Bakanlığı bu dinlemelerden haberdar olduklarını ve dinlemelerin hukuka uygun olduğunu belirtmişken, hâlihazırda durumun kontrolden çıktığı malumdur. Zira hâkim, savcılar ile siyasetçiler de ortam dinlemelerinin mağduru olmuş durumdadırlar.

Oysa ceza yargılamasında hukuka uygun olmayan kanıtlar hükme esas alınamaz. Ceza Genel Kurulu 15/10/2002 gün ve 8-191/362 sayılı kararında "Demokratik bir hukuk devletinde delil elde etme, soruşturmanın temel amacı ve kolluğun görevi olmakla birlikte, bu amaç ve görev insan hakları ihlallerini meşrulaştırıcı ve hukuka aykırı davranmanın bir mazereti olamaz." görüşüyle hukuka aykırı kanıtları reddetmektedir. Yine Yargıtay Ceza Genel Kurulu 28/9/1999 gün ve 213/219 sayılı kararında da "Bir kanıt, yasa koyucunun öngördüğü koşullara göre elde edilmemişse, hükümde, bu kanıta dayanılamayacaktır." ifadesine yer vermiştir.

Anayasa Mahkemesi de bir kararında "Bu kuralla, hukuka aykırı biçimde sağlanan delillerin hükümde göz önüne alınmaması amaçlandığından söz konusu delillerin üçüncü

kişiler tarafından sağlanması hukuka aykırılığı ortadan kaldırmaz. Delilin elde ediliş biçimi, kişilerin Anayasa ile tanınmış haklarını ihlâl ediyorsa, onun hukuka aykırı olarak elde edildiğinin kabulü gerekir." hükmü ile kanuna aykırı delilin kabul edilemeyeceğini, kişi hak ve özgürlüklerinin bu itibarla ihlal edilemeyeceğini kaydetmiştir.

Nitekim, Anayasa'nın 22'nci maddesi uyarınca kural olarak herkes haberleşme özgürlüğüne sahiptir ve haberleşmenin gizliliği esastır. Tarafı olduğumuz ve onaylamakla iç hukuk mevzuatına dâhil ettiğimiz Avrupa İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi'nin 8'inci maddesinde de herkesin haberleşmesine saygı gösterilmesi hakkına sahip olduğu kurala bağlanmış, bu hakka bir kamu otoritesinin müdahalesinin ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda gerekli olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabileceği belirtilmiştir.

Ancak ne var ki bazı hâllerde bu durumun birincil mağduru olan hâkim ve savcılar dahi gizli dinlemeler yolu ile edinilen bu delillere başvurmakta, yine bu deliller ışığında hukuka aykırı kararlara imza atabilmektedirler. Oysa Yargıtay kararlarında da belirtildiği üzere, delil elde etmek adına yapılan gizli dinleme insan hakları ihlallerini meşrulaştırıcı yahut hukuka aykırı davranmanın bir mazereti olamaz. Bu itibarla, eğer dava dosyası içinde bulunan telefon dinleme tutanaklarının "hukuka aykırı kanıt niteliğinde olduğu" anlaşıldığı vakit dosyadan çıkarılması gerekir. Fakat günümüzde gelinen noktada, haberleşmenin gizliliği esası bertaraf edilmiş; herkesin muhaberatı açık, gizli dinlemeler ise fiilen yasal duruma gelmiştir.

Açıklamış olduğumuz üzere gelinen fazda temel kişi hak ve özgürlüklerinin en çok ihlal edildiği bu alana dair bir araştırma yapılarak yaşanan sorunların giderilmesi ve açık yasa ihlalinin önüne geçilerek hukuka olan güvenin yeniden tesisi adına bir komisyon kurularak inceleme yapılması gereklilik arz etmektedir.

TAKDİM YAZISI



TÜRKİYE BÜYÜK MİLLET MECLİSİ

Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve
Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan
Meclis Araştırması Komisyonu

Sayı : 53668891-130.05/128581

12.06.2013

Konu : Komisyon Raporu

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan (10/74, 471, 472, 473, 474, 475) Esas Numaralı Meclis Araştırması Komisyonu Anayasa'nın 98'inci ve İçtüzük'ün 104 ve 105'inci maddeleri çerçevesinde çalışmalarını tamamlamış bulunmaktadır.

12.02.2013 tarihinde göreve başlayan Komisyonun yaptığı çalışmalar sonucunda düzenlediği rapor ilişikte sunulmuştur.

Gereğini arz ederim.

Saygılarımla.

Yusuf BAŞER
Yozgat Milletvekili
Komisyon Başkanı

Ek:

1- Komisyon Raporu

**Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine
Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin
Tedbirlerin Belirlenmesi Amacıyla Kurulan (10/74, 471,
472, 473, 474, 475) Esas Numaralı Meclis Araştırması
Komisyonu Raporu**

BİRİNCİ BÖLÜM

KOMİSYONUN KURULUŞU VE ÇALIŞMALARI

1.1 Meclis Araştırması Önergelerinin Özeti

24'üncü Yasama Döneminde haberleşme özgürlüğüne ve özel hayatın gizliliğine yönelik ihlallerin tespiti ve önlenmesine ilişkin tedbirlerin belirlenmesi amacıyla bir Meclis araştırması komisyonu kurulmasına dayanak teşkil eden; İzmir Milletvekili Rıza TÜRMEK ve 25 Milletvekilinin (10/74), Milliyetçi Hareket Partisi Grubu adına Grup Başkanvekilleri İzmir Milletvekili Oktay VURAL ve Mersin Milletvekili Mehmet ŞANDIR'ın (10/471), İstanbul Milletvekili Mustafa Sezgin TANRIKULU ve 30 Milletvekilinin (10/472), Adalet ve Kalkınma Partisi Grubu adına Grup Başkanvekilleri Giresun Milletvekili Nurettin CANIKLI, Kayseri Milletvekili Mustafa ELİTAŞ, İstanbul Milletvekili Ayşe Nur BAHÇEKAPILI, Adıyaman Milletvekili Ahmet AYDIN, Kahramanmaraş Milletvekili Mahir ÜNAL ve 135 Milletvekilinin (10/473), Şırnak Milletvekili Hasip KAPLAN ve 21 Milletvekilinin (10/474) ve Barış ve Demokrasi Partisi Grubu adına Grup Başkanvekilleri Iğdır Milletvekili Pervin BULDAN ve Bingöl Milletvekili İdris BALUKEN'in (10/475) esas numaralı; haberleşme özgürlüğüne ve özel hayatın gizliliğine yönelik ihlallerin tespiti ve önlenmesine ilişkin tedbirlerin belirlenmesi amacıyla Anayasa'nın 98'inci ve Türkiye Büyük Millet Meclisi İçtüzüğü'nün 104 ve 105'inci maddeleri gereğince bir Meclis araştırması açılmasını isteyen önergelerin gerekçelerinde özetle;

- Anayasada teminat altına alınan özel hayatın gizliliği ve haberleşme hürriyetinin, gayrimeşru yol ve yöntemlerle yapılan dinleme ve izlemeler ile bunların kitle iletişim araçları vasıtasıyla yayınlanması suretiyle ihlal edildiği,
- Ülkemizde yasa dışı yollarla iletişim tespitinin ciddi bir hukuki ve toplumsal sorun niteliği kazandığı,
- Yasal olarak gerçekleştirilen iletişimin denetlenmesi tedbirinin uygulamasına ilişkin sorunlar olduğu,
- İletişimin denetlenmesi kararlarında yasal şartların eksiksiz bir şekilde yer alıp almadığının incelenmesinin uygun olacağı,
- Yasa dışı iletişim tespitinin kimler tarafından ve hangi araçlar kullanılarak yapıldığının tespit edilmesi gerektiği,

- Yasa dışı dinleme ve izleme yapılmasına imkân sağlayan araçların nasıl temin edildiği ve bu araçların imal, ithal ve bulundurulması konusunda mevzuatta bir eksiklik bulunup bulunmadığının tespitinin gerekli olduğu,
 - Yazılı ve görsel medyada özel hayatın gizliliğini ihlal eden çok sayıda görüntü ve dinleme kaydı yer aldığı,
 - Yasa dışı dinleme ve izlemeler ile ihlal edilen özel hayatın gizliliği hakkının Avrupa İnsan Hakları Sözleşmesi gibi uluslararası belgelerde yer aldığı ve anayasal bir hak olduğu,
 - Haberleşme özgürlüğünün ve özel hayatın gizliliğinin ihlal edilmesi sorununun çözümü amacıyla alınması gereken yasal, idari ve diğer önlemlerin belirlenmesi gerektiği,
- ifade edilmiştir.

1.2 Komisyonun Kuruluşu

Yukarıda özetlerine yer verilen Meclis Araştırması açılmasına ilişkin altı Önerge (10/74, 471, 472, 473, 474, 475) Türkiye Büyük Millet Meclisi Genel Kurulunun 22.01.2013 tarihli 55’inci Birleşiminde konularının benzer mahiyette olması nedeniyle birleştirilerek görüşülmüş ve “Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi” amacıyla bir Meclis Araştırması Komisyonu kurulması kararlaştırılmıştır.

Komisyonun kurulmasına ilişkin 22.01.2013 tarihli ve 1030 sayılı Türkiye Büyük Millet Meclisi Kararı’nda, araştırmayı yapacak Komisyonun 17 üyeden oluşması, Komisyonun çalışma süresinin Başkan, Başkanvekili, Sözcü ve Kâtip seçimi tarihinden başlamak üzere 3 ay olması ve Komisyonun gerektiğinde Ankara dışında da çalışma yapabilmesi hususlarına yer verilmiştir. Söz konusu Karar 30.01.2013 tarihli ve 28544 sayılı Resmî Gazete’de yayımlanmıştır.

Türkiye Büyük Millet Meclisi Genel Kurulunun 12.02.2013 tarihli 64’üncü Birleşiminde Komisyona üye seçimi yapılmıştır. Aynı tarihte yapılan Komisyon toplantısında ise Komisyonun Başkan, Başkanvekili, Sözcü ve Kâtip seçimi gerçekleştirilmiş ve bu seçimler sonucunda, Komisyon Başkanı, Başkanvekili, Sözcüsü ve Kâtipi ile üyeliklerini gösterir liste aşağıdaki şekilde oluşmuştur:

Tablo 1- Komisyon Üyeleri

ADI VE SOYADI	UNVANI	PARTİSİ	SEÇİM ÇEVRESİ
Zeyid ASLAN	BAŞKAN	AK Parti	Tokat
Yusuf BAŞER	BAŞKANVEKİLİ	AK Parti	Yozgat
Yılmaz TUNÇ	SÖZCÜ	AK Parti	Bartın
Mihrimah Belma SATIR	KÂTİP	AK Parti	İstanbul
Namık HAVUTÇA	ÜYE	CHP	Balıkesir
Ali ERCOŞKUN	ÜYE	AK Parti	Bolu
Bilal UÇAR	ÜYE	AK Parti	Denizli
İlhan CİHANER	ÜYE	CHP	Denizli
Enver ERDEM	ÜYE	MHP	Elazığ
Şuay ALPAY	ÜYE	AK Parti	Elazığ
Atila KAYA	ÜYE	MHP	İstanbul
Şirin ÜNAL	ÜYE	AK Parti	İstanbul
Erdal AKSÜNGER	ÜYE	CHP	İzmir
Hamza DAĞ	ÜYE	AK Parti	İzmir
Mehmet Siyam KESİMOĞLU	ÜYE	CHP	Kırklareli
Hasip KAPLAN	ÜYE	BDP	Şırnak
Fatih ÇİFTÇİ	ÜYE	AK Parti	Van

Komisyon üyelikleri seçimine ilişkin 12.02.2013 tarihli ve 1032 sayılı Türkiye Büyük Millet Meclisi Kararı 19.02.2013 tarihli ve 28564 sayılı Resmî Gazete’de yayımlanmıştır.

Komisyon Başkanı Tokat Milletvekili Zeyid ASLAN 02.05.2013 tarihinde Komisyon Başkanlığı ve üyeliğinden istifa etmiştir. Komisyonun 29.05.2013 tarihli ve

Başkanlık Seçimi gündemli son toplantısında Yozgat Milletvekili Yusuf BAŞER Komisyon Başkanı ve İzmir Milletvekili Hamza DAĞ Komisyon Başkanvekili seçilmişlerdir. Komisyon, bu tarihten sonraki çalışmalarını 29.05.2013 tarihinde Komisyon Başkanı seçilen Yozgat Milletvekili Yusuf BAŞER Başkanlığında yürütmüştür.

1.3 Komisyonun Görev, Yetki ve Süresi

12.02.2013 tarihinde gerçekleştirdiği ilk toplantısı ile çalışmalarına başlayan Komisyon; Anayasa'nın 98'inci, Türkiye Büyük Millet Meclisi İçtüzüğü'nün 104 ve 105'inci maddeleri ile diğer hükümleri çerçevesinde görev yapmıştır. Üç aylık çalışma süresi 12.05.2013 tarihinde sona eren Komisyon, İçtüzük'ün 105'inci maddesi gereğince 1 aylık ek süre talebinde bulunmuştur. Süre uzatımına ilişkin 1035 sayılı Türkiye Büyük Millet Meclisi Kararı, Genel Kurulun 07.05.2013 tarihli 100'üncü Birleşiminde alınmış ve 10.05.2013 tarihli ve 28643 sayılı Resmî Gazete'de yayımlanmıştır.

1.4 Komisyon Çalışmaları

12 Şubat 2013 tarihinde çalışmalarına başlayan Komisyon, bu tarihte yapmış olduğu ilk toplantısında çalışma programını belirlemiş ve bu çerçevede;

- Komisyonun gerekli görmesi halinde, yurt içinde ve yurt dışında, Komisyon olarak ya da oluşturulacak alt komisyonlar marifetiyle mahallinde inceleme ve araştırmalar yapmasına,
- Komisyon toplantılarında ve Ankara dışı çalışmalarda tam tutanak tutulmasına,
- Komisyonun Genel Kurul çalışma saatlerinde de çalışma yapabilmesi için İçtüzük'ün 35'inci maddesi uyarınca Başkanlık Divanından izin istenmesine,
- Komisyon çalışmalarını kamuoyuna duyurabilmek ve elektronik iletişim kurabilmek amacıyla internet sitesi kurulmasına ve elektronik posta adresi alınmasına,
- Komisyon süresince ilgili kurum ve kuruluşlardan konu ile ilgili uzman görevlendirilmesi ile ilgili işlemlerin ve yazışmaların yapılmasında, davet edilecek kişi ve kurumların tespiti hususlarında Komisyon Başkanlığının yetkili kılınmasına,
- Ankara dışı çalışmalarına katılan Komisyon Üyesi milletvekillerinin yasama çalışmalarından izinli sayılmasına,
- Yapılacak Ankara dışı inceleme ziyaretleri ve çalışmalara Komisyon uzmanları ile kamu kurum ve kuruluşlarından görevlendirilen personelin katılmasına,

- Komisyona verilen 3 aylık süre içerisinde çalışmaların bitmemesi halinde 1 aylık ek süre istenmesine,
- Rapor yazımında Komisyon Başkanlığına redaksiyon yetkisi verilmesine, karar vermiştir.

Söz konusu kararlara uygun olarak Komisyon, 12 Haziran 2013 tarihinde sona eren dört aylık çalışma süresi içerisinde on üç Komisyon toplantısı, sekiz Hukuk Alt Komisyon toplantısı ve dört Teknik Alt Komisyon toplantısı olmak üzere yirmi beş resmî toplantı yapmış ve araştırma konusu hakkında bilgi edinmek üzere akademisyenler, ilgili kamu kurum ve kuruluşları ile sivil toplum örgütlerinden yetkililer davet ederek görüşler almış, rapor yazımında değerlendirmek üzere yazışmalar yoluyla bilgi ve belge temin etmiştir. Ayrıca, Komisyon olarak dört ve Teknik Alt Komisyonu olarak altı ziyaret olmak üzere yerinde incelemelerde bulunmak amacıyla on çalışma ziyareti gerçekleştirmiştir.

Komisyon çalışmalarına ve rapor yazımına katkıda bulunmak üzere aşağıda adı, soyadı, kurumu ve unvanı belirtilen kişiler Komisyonda uzman olarak görev almışlardır.

Tablo 2- Komisyon Uzmanları

ADI VE SOYADI	KURUMU	UNVANI
Cemil ZEMHERİ	Türkiye Büyük Millet Meclisi Kanunlar ve Kararlar Başkanlığı	Yasama Uzmanı
İlhan YÜCEL	Türkiye Büyük Millet Meclisi Kanunlar ve Kararlar Başkanlığı	Yasama Uzman Yardımcısı
Selçuk TELLİ	Adalet Bakanlığı Teftiş Kurulu Başkanlığı	Adalet Müfettişi
Sinan GENÇ	Adalet Bakanlığı Kanunlar Genel Müdürlüğü	Tetkik Hâkimi
Adnan FİKİRLİ	İçişleri Bakanlığı Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı	4. Sınıf Emniyet Müdürü

Mevlüt AKGÜL	İçişleri Bakanlığı Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı	Komiser
Cenk Hakan KARADUMAN	İçişleri Bakanlığı Mülkiye Teftiş Kurulu Başkanlığı	Mülkiye Müfettişi
Osman AHSEN	İçişleri Bakanlığı Mülkiye Teftiş Kurulu Başkanlığı	Mülkiye Müfettişi
Eyüp GÜMÜŞ	Telekomünikasyon İletişim Başkanlığı	İletişim Uzmanı
Ömer BOZ	Telekomünikasyon İletişim Başkanlığı	İletişim Uzmanı
Ömer SAYILIR	Telekomünikasyon İletişim Başkanlığı	İletişim Uzmanı
Dr. Mehmet Sabır KİRAZ	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu	Uzman Araştırmacı
Yavuz ÖZTÜRK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu	Uzman Araştırmacı
Muzaffer ÇALIŞKAN	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü	Elektronik Mühendisi

1.4.1 Komisyon Toplantıları

Komisyon; son üçü alt komisyonların kurulmasına, çalışma programlarının belirlenmesine, çalışma süresinin uzatılmasına yönelik karar alınmasına ve Komisyon Başkanı seçimine ilişkin olmak üzere on üç adet toplantı gerçekleştirmiş ve bu toplantılarda on iki kurum ve kuruluştan otuz yedi uzmanın bilgisine başvurmuştur. Toplantılara ilişkin tarih, kurum ve katılımcı bilgileri aşağıdaki tabloda yer almaktadır.

Tablo 3- Komisyon Toplantıları

No	Tarih	Gündem/Kurum	Katılımcı
1	12.02.2013	Komisyon Başkanlık Divanı Seçimi	-
2	14.02.2013	Komisyonun çalışma programı ve bu programın uygulanmasında takip edilecek usul ve esaslar ile Komisyon çalışmaları için davet edilecek kişi ve kurumlar ile uzmanların belirlenmesi	-
3	20.02.2013	Adalet Bakanlığı	Yüksel HIZ Kanunlar Genel Müdürlü Dr. Yusuf Solmaz BALO Kanunlar Genel Müdür Yardımcısı Muharrem BARUT Kanunlar Genel Müdür Yardımcısı Doç. Dr. Mustafa TAŞKIN Kanunlar Daire Başkanı Atilla ÖZTÜRK Kanunlar Tetkik Hâkimi Hakan ŞEKER Kanunlar Tetkik Hâkimi Mehmet TEKKOYUN Kanunlar Tetkik Hâkimi
		Telekomünikasyon İletişim Başkanlığı	Osman Nihat ŞEN Başkanvekili Adil BİÇER Hukuk Daire Başkanı İlhan ELİEYİOĞLU Bilgi Sistemleri Daire Başkanı Ömer BOZ İletişim Uzmanı Ömer SAYILIR İletişim Uzmanı Eyüp GÜMÜŞ İletişim Uzmanı

4	21.02.2013	Emniyet Genel Müdürlüğü	Ömer TEKELİ Bilişim Suçlarıyla Mücadele Daire Başkanı (1.Sınıf Emniyet Müdürü) Gürsel AKTEPE İstihbarat Dairesi Başkan Yardımcısı (2.Sınıf Emniyet Müdürü) Hakan KARALI İstihbarat Daire Başkanlığı (Komiser)
		Jandarma Genel Komutanlığı	Fuat GÜNEY Teknik İstihbarat Daire Başkanı (Jandarma Kurmay Albay) Arif KALKAN Teknik İstihbarat Analiz Şube Müdürü (Jandarma Yarbay) Haydar HACIPAŞALIOĞLU Araştırma Geliştirme Kısım Amiri (Jandarma Muhabere Yüzbaşı) Oktay ESEN Teknik Takip Karar İşlem Kısım Amiri (Jandarma Kıdemli Başçavuş) Ömer KALEM Sistem Yönetim Şube Teknisyeni (Jandarma Muhabere Başçavuş)
5	27.02.2013	Millî İstihbarat Teşkilatı	-
6	28.02.2013	TÜBİTAK	Dr. Uğur SARAÇ Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdür Yardımcısı (Elektronik Mühendisi) Furkan ELİBOL Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Uzman Araştırmacı (Elektronik Yüksek Mühendisi)
7	06.03.2013	Gazi Üniversitesi	Prof. Dr. Şeref SAĞIROĞLU Fen Bilimleri Enstitüsü Müdürü
8	07.03.2013	Türkiye Barolar Birliği	Av. Talay ŞENOL Başkan Yardımcısı

		İstanbul Üniversitesi	Prof. Dr. Ersan ŞEN Siyasal Bilgiler Fakültesi Kamu Yönetimi Bölümü Hukuk Bilimleri Anabilim Dalı Öğretim Üyesi
9	20.03.2013	Bilgi Teknolojileri ve İletişim Kurumu	Atilla ARSLAN Teknik Düzenlemeler Daire Başkanı Özgür Fatih AKPINAR Tüketici Hakları Daire Başkanı Necati UĞURLU Spektrum İzleme Daire Başkanı Atilla ÖZTÜRK Hukuk Müşaviri
10	21.03.2013	TÜRK TELEKOM	Can ESEN Hukuk Başkanı Mehmet ATALAY Operasyon Başkanı Mehmet Yılmaz KÜÇÜK Hukuk Direktörü
		TÜRKSAT	Cemil SAĞIROĞLU Genel Müdür Yardımcısı Mustafa Zeki KALKAN Uydu Kontrol Direktörü Orhan ULUBEY Uydu Frekans Gözlem Direktörü Süleyman KUZU Uydu Hizmetleri Kurumsal Çözümler Direktörü Vekili Ünal ÖZDEM Kurumsal İletişim Direktörlüğü Kıdemli Uzmanı
11	27.03.2013	Alt Komisyonların Kurulması	-
12	02.05.2013	Alt Komisyon Çalışmalarının Değerlendirilmesi ve Çalışma Süresinin Uzatımına İlişkin Karar Alınması	-
13	29.05.2013	Komisyon Başkanı Seçimi	-

1.4.1.1 Hukuk Alt Komisyonu Toplantıları

Hukuk Alt Komisyonu; sekiz toplantı gerçekleştirerek, on dört kurum ve kuruluştan yirmi dokuz uzmanın bilgisine başvurmuştur. Toplantılara ilişkin tarih, kurum ve katılımcı bilgileri aşağıdaki tabloda yer almaktadır.

Tablo 4- Hukuk Alt Komisyonu Toplantıları

No	Tarih	Gündem/Kurum	Katılımcı
1	27.03.2013	Alt Komisyon Başkanı Seçimi	-
2	28.03.2013	Alt Komisyon çalışma programının belirlenmesi	-
3	02.04.2013	Milliyet Gazetesi	Fikret BİLA Milliyet Gazetesi Ankara Temsilcisi
		Sabah Gazetesi	Okan MÜDERRİSOĞLU Sabah Gazetesi Ankara Temsilcisi
		Zaman Gazetesi	Bülent KORUCU Zaman Gazetesi Genel Yayın Yönetmen Yardımcısı
4	03.04.2013	Habertürk Gazetesi	Erdal ŞEN Habertürk Gazetesi Ankara Temsilcisi
		Yeni Şafak Gazetesi	Abdülkadir SELVİ Yeni Şafak Gazetesi Ankara Temsilcisi
		Akşam Gazetesi	Çiğdem TOKER Akşam Gazetesi Ankara Temsilcisi
		Hürriyet Gazetesi	Ertuğrul ÖZKÖK Hürriyet Gazetesi Yazarı
5	04.04.2013	Hürriyet Gazetesi	Metehan DEMİR Hürriyet Gazetesi Ankara Temsilcisi
		Star Gazetesi	Mustafa KARTOĞLU Star Gazetesi Ankara Temsilcisi
		Taraf Gazetesi	Melih ALTINOK Taraf Gazetesi Ankara Temsilcisi
		Dicle Haber Ajansı	Abdurrahman GÖK Dicle Haber Ajansı Haber Müdürü
		Cumhuriyet Gazetesi	Akın ATALAY Cumhuriyet Gazetesi Genel Koordinatörü

6	10.04.2013	Emniyet Genel Müdürlüğü	Bülent ORAKOĞLU Emekli İstihbarat Daire Başkanı Osman AK Merkez Emniyet Müdürü Sabri UZUN Emekli İstihbarat Daire Başkanı
7	11.04.2013	Hürriyet Gazetesi	Sedat ERGİN - Hürriyet Gazetesi Yazarı
		Ekonomi Bakanlığı	Mehmet AZGİN İthalat Genel Müdürü Vekili Taşkın Barış ERGÜN İthalat Genel Müdürlüğü Mevzuat Dairesi Başkanı Murat TAŞKIN Ürün Güvenliği ve Denetimi Genel Müdürlüğü Daire Başkanı Hasan ÖNER İthalat Genel Müdürlüğü Şube Müdürü Fırat YELTEKİN İthalat Genel Müdürlüğü Dış Ticaret Uzman Yardımcısı Murat Can KILINÇ İthalat Genel Müdürlüğü Dış Ticaret Uzman Yardımcısı
8	17.04.2013	Gümrük ve Ticaret Bakanlığı	Ziya ALTUNYALDIZ Müsteşar Remzi AKÇİN Gümrükler Genel Müdürü Yusuf GÜNEY Gümrükler Muhafaza Genel Müdürü Sinem TAŞTAN Gümrük ve Ticaret Uzmanı
		Emniyet Genel Müdürlüğü	Emin ARSLAN Emekli Emniyet Genel Müdür Yardımcısı

1.4.1.2 Teknik Alt Komisyon Toplantıları

Teknik Alt Komisyon; dört toplantı gerçekleştirerek, dört kurum ve kuruluştan altı uzmanın bilgisine başvurmuştur. Toplantılara ilişkin tarih, kurum ve katılımcı bilgileri aşağıdaki tabloda yer almaktadır.

Tablo 5- Teknik Alt Komisyon Toplantıları

No	Tarih	Gündem/Kurum	Katılımcı
1	27.03.2013	Alt Komisyon Başkanı Seçimi	-
2	28.03.2013	Alt Komisyon çalışma programının belirlenmesi	-
3	03.04.2013	TÜRKTRUST A.Ş.	Musa Öner DEMİRKOL Yazılım Geliştirme ve Ar-Ge Müdürü
		Bilkent Üniversitesi	Prof. Dr. Ayhan ALTINTAŞ Elektrik-Elektronik Mühendisliği Bölümü Öğretim Üyesi Prof. Dr. Enis ÇETİN Elektrik-Elektronik Mühendisliği Bölümü Öğretim Üyesi
4	04.04.2013	Bilgi Güvenliği Derneği	Prof. Dr. Mustafa ALKAN Bilgi Güvenliği Derneği Başkanı Gazi Üniversitesi Teknoloji Fakültesi Elektrik-Elektronik Mühendisliği Bölüm Başkanı
		Türkiye Odalar ve Borsalar Birliği	Hasan Gazi ÖZER TOBB Türkiye Özel Güvenlik Hizmetleri Sektör Meclisi Başkanı Hakan ÇEVİKOĞLU Sektör Temsilcisi (ÜLKEM A.Ş.)

1.4.2 Komisyonca Gerçekleştirilen Çalışma Ziyaretleri

Komisyon, 12 Şubat 2013 tarihli ilk toplantısında aldığı Karar kapsamında Komisyon olarak ya da oluşturulacak alt komisyonlar marifetiyle yerinde inceleme ve araştırmalar yapmak amacıyla Komisyon olarak dört ve 27 Mart 2013 tarihinde oluşturulan iki alt komisyondan biri olan Teknik Alt Komisyonu aracılığıyla altı ziyaret olmak üzere aşağıda ayrıntılı olarak ele alınan on çalışma ziyareti gerçekleştirmiştir.

1.4.2.1 13 Mart 2013 Tarihli Çalışma Ziyaretleri

Komisyunun ilk çalışma ziyaretleri, 21 Şubat 2013 tarihli Komisyon toplantısında alınan Karar gereğince 13 Mart 2013 tarihinde Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanlığı ile Jandarma Genel Komutanlığı İstihbarat Dairesi Başkanlığına yapılmıştır. Bu çalışma ziyaretlerine Komisyon Başkanı Tokat Milletvekili Zeyid ASLAN, Komisyon Sözcüsü Bartın Milletvekili Yılmaz TUNÇ, Komisyon üyeleri Balıkesir Milletvekili Namık HAVUTÇA, Bolu Milletvekili Ali ERCOŞKUN, Denizli Milletvekili Bilal UÇAR, Denizli Milletvekili İlhan CİHANER, Elazığ Milletvekili Enver ERDEM, Elazığ Milletvekili Şuay ALPAY, İstanbul Milletvekili Şirin ÜNAL, İzmir Milletvekili Erdal AKSÜNGER, İzmir Milletvekili Hamza DAĞ, Kırklareli Milletvekili Mehmet Siyam KESİMOĞLU, Şırnak Milletvekili Hasip KAPLAN, Van Milletvekili Fatih ÇİFTÇİ ve Bağımsız İstanbul Milletvekili İhsan BARUTÇU ile Yasama Uzmanı Cemil ZEMHERİ ve Yasama Uzman Yardımcısı İlhan YÜCEL katılmıştır.

1.4.2.1.1 Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanlığı Ziyareti

Ziyarete ilk olarak Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkan Yardımcısı Gürsel AKTEPE tarafından Komisyon üyelerine sunum yapılmıştır. Yapılan sunumda istihbarat üretim faaliyetleri, yasa dışı dinleme ile mücadele kapsamında gerçekleştirilen çalışmalar ve İstihbarat Dairesi Başkanlığının operasyonel faaliyetleri ile ilgili bilgilere yer verilmiştir.

Sunumun istihbarat üretimi başlığını taşıyan ilk bölümünde istihbarat üretim sürecinin evreleri üzerinde durulduktan sonra; Devlet Denetleme Kurumu, Türkiye Büyük Millet Meclisi, İçişleri Bakanlığı Mülkiye Teftiş Kurulu ve Başbakanlık Teftiş Kurulu tarafından kurum faaliyetlerinin denetlenmesi ve bu kapsamda hesap verilebilirlik konularına değinilmiştir. Sunumun bu bölümünde, kurumun demokratik hukuk devleti ilkesinin sağladığı imkânlar çerçevesinde istihbarat ürettiği ve Emniyet Genel Müdürlüğünün bu üretime dolaylı bir katkı sunduğu dile getirilmiştir.

Sunumun ikinci bölümünde kurumun haberleşme ve özel hayatın gizliğinin ihlali kapsamında yasa dışı dinlemeleri önlemek amacıyla yurt çapında gerçekleştirdiği operasyonlara ilişkin bilgilere yer verilmiştir. Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanlığının bu amaçla çeşitli tarihlerde Ankara, İstanbul, Antalya, İzmir, Konya ve

Adana illerinde çeşitli operasyonlar düzenleyerek yasa dışı dinlemede kullanılan çok sayıda ekipman ele geçirdiği ifade edilmiştir.

Sunumun son bölümünde ise terörizmle mücadelede iletişimin denetlenmesine yer verilmiş, Tekirdağ'da El-Kaide terör örgütüne ve Cilve Gözü sınır kapısındaki bombalama olayına yönelik operasyonlar ile kurumun kayıp veya kaçırılmış çocukların bulunmasına yönelik faaliyetlerine ilişkin bilgi verilmiştir.

Sunumu takiben Komisyon Heyeti dinleme faaliyetinin gerçekleştirildiği odaları ve Başkanlıkça kullanılan cihazları yerinde inceleyip kurum yetkililerinden bilgi almıştır. Yalnızca yetkilendirilmiş personelin kartla girebildiği, doğrudan asansör bağlantısı bulunmayan bu odalarda, sadece iletişimin denetlenmesine tahsis edilmiş bir bilgisayar ağının bulunmasının yanı sıra, kullanılan bilgisayarlar şahsa tanımlı olup internet bağlantısı bulunmadığı ve alınan bu önlemlere ek olarak bu odalara herhangi bir iletişim aracının alınmasına izin verilmediği belirtilmiştir.

Komisyon Heyeti kurumun kullandığı bir mobil dinleme aracını inceleyip, araç hakkında bilgi aldıktan çalışmalarını tamamlayarak Kurumdan ayrılmıştır.

1.4.2.1.2 Jandarma Genel Komutanlığı İstihbarat Daire Başkanlığı Ziyareti

Komisyon ikinci ziyaretini Jandarma Genel Komutanlığı İstihbarat Dairesi Başkanlığına düzenlemiştir. Komisyon Heyeti ilk olarak İstihbarat Daire Başkanlığının Teknik - Takip Karar İşlem Merkezini ziyaret etmiş ve bu bölümde Heyete, Teknik - Takip Karar İşlem Kısım Amiri tarafından sunum yapılmıştır. Söz konusu sunumda; Jandarma Genel Komutanlığı bünyesinde telekomünikasyon yoluyla yapılan iletişimin dinlenmesi ve kayda alınmasına ilişkin bütün kararların güvenli bir elektronik ağ üzerinden bu Merkezde toplandığı, kararların Merkezde şekli incelemeye tabi tutulduğu, şekli incelemenin ardından Telekomünikasyon İletişim Başkanlığına yine güvenli bir elektronik ağ üzerinden gönderildiği ve ancak TİB tarafından da uygun görülen kararlar gereğince dinleme yapılabilirdiği ifade edilmiştir.

Heyet ikinci olarak, dinleme işlemlerinin yapıldığı odaları ve bu odalarda kullanılan cihazları yerinde inceleyip bölüm yetkililerinden bilgi almıştır. Bu bölümde yetkililer tarafından; bölüme giriş çıkışların sadece bölümde çalışan personelle sınırlı olduğu, bütün odalarda kartlı giriş sistemi yer aldığı ve görevli personel dışında amir konumunda

olanların bile bölüme giriş çıkışlarının kayıt altına alındığı, dinleme işlemini yapan her personele ait bir aidiyet numarası bulunduğu, dinleme yapılan bilgisayarlara yazıcı, tarayıcı, flash bellek, USB ve CD bağlantısı yapılmasının mümkün olmadığı, bilgisayarlarda yapılan her işlemin log kaydının tutulduğu ve böylelikle hangi personelin hangi anda hangi işlemi yaptığının kayıt altında alındığı, personelin yalnızca kendi aidiyet numarasına için tanımlanmış telefon numaralarını dinleyebildiği, yapılan dinleme işlemi bitince bir imha tutanağı düzenlendiği ve hedef telefon numarasının dinlemeye kapatıldığı belirtilmiştir.

Komisyon Heyeti son olarak, Daire Başkanlığının Sistem Yönetimi Bölümünü ziyaret etmiş ve ilgili bölümün yetkililerinden bilgi almıştır. Bölüm yetkilileri tarafından yapılan sunumda; ülke genelindeki sistemin sorunsuz çalışabilmesine imkan sağlayan teknik cihazların nasıl çalıştığı, sistem sayesinde illerdeki birimlerdeki faaliyetlerin koordinasyonun sağlandığı ve olası sorunların anında giderilebildiği ayrıca sistemde yer alan bilgilerin on gün içerisinde geri getirilemeyecek şekilde silindiği ifade edilmiştir.

Komisyon üyeleri, ziyaret süresince yapılan sunumlar sırasında Daire Başkanlığı yetkililerine sorular yöneltmişler ve bu sorular ilgili kısımların yetkilileri tarafından cevaplandırılmıştır. Ayrıca 21 Şubat 2013 tarihli Komisyon toplantısında Daire Başkanlığı yetkililerine yöneltilen sorulara ilişkin cevaplar yazılı olarak Komisyon üyelerine dağıtılmıştır.

1.4.2.2 14 Mart 2013 Tarihli Çalışma Ziyaretleri

Komisyon, 14 Mart 2013 tarihinde Başbakanlık Milli İstihbarat Teşkilatı Müsteşarlığı ile Telekomünikasyon İletişim Başkanlığına çalışma ziyaretleri düzenlemiştir. Söz konusu ziyaretlere; Komisyon Başkanı Tokat Milletvekili Zeyid ASLAN, Komisyon Başkanvekili Yozgat Milletvekili Yusuf BAŞER, Komisyon Sözcüsü Bartın Milletvekili Yılmaz TUNÇ, Komisyon üyeleri Balıkesir Milletvekili Namık HAVUTÇA, Bolu Milletvekili Ali ERCOŞKUN, Denizli Milletvekili Bilal UÇAR, Denizli Milletvekili İlhan CİHANER, Elazığ Milletvekili Enver ERDEM, Elazığ Milletvekili Şuay ALPAY, İstanbul Milletvekili Şirin ÜNAL, İzmir Milletvekili Erdal AKSÜNGER, İzmir Milletvekili Hamza DAĞ, Kırklareli Milletvekili Mehmet Siyam KESİMOĞLU, Şırnak Milletvekili Hasip KAPLAN ve Bağımsız İstanbul Milletvekili İhsan BARUTÇU ile Yasama Uzmanı Cemil ZEMHERİ ve Yasama Uzman Yardımcısı İlhan YÜCEL katılmıştır.

1.4.2.2.1 Millî İstihbarat Teşkilatı Ziyareti

Millî İstihbarat Teşkilatına yapılan çalışma ziyaretinde Elektronik - Teknik İstihbarat Daire Başkanı tarafından Komisyon Heyetine sunum yapılmıştır. Söz konusu sunumda; Komisyon üyeleri Millî İstihbarat Teşkilatının telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, kayda alınması ve teknik araçlarla yapılan izleme faaliyetleri, dinleme ve izleme cihazlarının çeşitleri ile nasıl kullanılabilecekleri ve Millî İstihbarat Teşkilatı tarafından yurt içinde ve dışında tespit edilen cihazlar hakkında bilgilendirilmiştir.

Ziyaret kapsamında ayrıca Millî İstihbarat Teşkilatı Müsteşarı Dr. Hakan Fidan, Komisyon Heyetine konuya ilişkin değerlendirmelerini kısaca aktarmış ve Komisyon üyelerinin sorularını cevaplandırmıştır.

1.4.2.2.2 Telekomünikasyon İletişim Başkanlığı Ziyareti

Komisyon Heyeti, çalışma ziyareti kapsamında öncelikle Telekomünikasyon İletişim Başkanlığı Başkanvekili Dr. Osman Nihat ŞEN ve beraberindeki yetkililerden Kurum ve Kurumun telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, kayda alınması ilişkin faaliyetleri hakkında brifing almış ve buradaki yetkililere sorular yönelmiştir.

Yapılan sunumun ardından Komisyon Heyeti, Başkanlığın ilgili birimlerini sırasıyla yerinde görerek yetkililerden bilgi almışlardır. Ziyaretin bu bölümünde Başkanlık yetkililerince; Kurumun teknik kapasitesi, sistem güvenliğinin nasıl sağlandığı, bütün sistemlere ve odalara giriş için ayrı ayrı yetkilendirilmiş personel bulunduğu, GSM şirketleri ve Emniyet, Jandarma ve MİT ile olan elektronik ağ bağlantılarının kriptolu olduğu, Kuruma gelen kararların hukuki incelemeye tabi tutulduğu, bu incelemeler sonrasında kararlarda eksik unsur tespit edilirse itiraz edildiği ancak CMK gereği itiraz edilse bile kararların yerine getirildiği, bu kararlar kapsamında hedef seslerin kaydedilip ilgili birimlere gönderildiği, karar süresi bittikten on gün sonra ilgili kayıtların silindiği ve bu işlemlerde kullanılan hard disklerin disk imha makinesince imha edildiği ifade edilmiştir.

1.4.2.3 Teknik Alt Komisyonca Gerçekleştirilen Ziyaretler

Teknik Alt Komisyon; ilk ikisi İstanbul’da ve sonuncusu Ankara’da olmak üzere, araştırma alanıyla ilgili hususlarda ilgili kurumların uzmanlarından bilgi almak ve mahallinde incelemelerde bulunmak üzere üç adet çalışma ziyareti gerçekleştirmiştir.

1.4.2.3.1 İstanbul Çalışma Ziyareti

Teknik Alt Komisyon ilk ziyaretini haberleşme özgürlüğü ve özel hayatın gizliliği ile ilgili teknolojik gelişmeleri ve ihlallere karşı alınabilecek önlemleri araştırmak üzere İstanbul’da gerçekleştirmiştir. Bu çerçevede, cep telefonu operatörlerinin teknoloji merkezleri, TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi, İstanbul Emniyet Müdürlüğü MOBESE Merkezi ziyaret edilmiş ve yetkililerden bilgi alınarak yerinde inceleme yapılmıştır. 10-11 Nisan 2013 tarihlerinde gerçekleştirilen ziyaretlere Alt Komisyon Başkanı İstanbul Milletvekili Mihrimah Belma SATIR, Alt Komisyon Üyesi İstanbul Milletvekili Şirin ÜNAL, Alt Komisyon Üyesi İzmir Milletvekili Hamza Dağ, Alt Komisyon Üyesi İzmir Milletvekili Erdal AKSÜNGER, Alt Komisyon Üyesi Denizli Milletvekili İlhan CİHANER, Alt Komisyon Üyesi Elazığ Milletvekili Enver ERDEM ve İstanbul Bağımsız Milletvekili İhsan BARUTÇU’nun yanı sıra; Yasama Uzman Yardımcısı İlhan YÜCEL (Türkiye Büyük Millet Meclisi) , Komiser Mevlüt AKGÜL (Emniyet Genel Müdürlüğü), Elektrik-Elektronik Mühendisi Muzaffer ÇALIŞKAN (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı), İletişim Uzmanı Ömer SAYILIR (Telekomünikasyon İletişim Başkanlığı), Uzman Araştırmacı Yavuz ÖZTÜRK (TÜBİTAK) ve Uzman Araştırmacı Dr. Mehmet Sabır KİRAZ (TÜBİTAK) katılmıştır.

1.4.2.3.1.1 Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Gebze Yerleşkesi Ziyareti

İstanbul Milletvekili Mihrimah Belma SATIR başkanlığındaki Alt Komisyon Heyeti, İstanbul programı kapsamında ilk olarak 10.04.2013 günü TÜBİTAK Gebze Yerleşkesini ziyaret etmiştir. Alt Komisyon Heyeti öncelikle TÜBİTAK Başkan Yardımcısı ve TÜBİTAK BİLGEM Başkanı Dr. Hasan PALAZ ve beraberindeki yetkililerden kurum ve yürüttüğü projeler hakkında brifing almış ve buradaki yetkililere araştırma alanı ile ilgili sorular yöneltilmiştir. Daha sonra Siber Güvenlik ve Ulusal Elektronik ve Kriptoloji Araştırma Enstitülerine bağlı bazı laboratuvarlar yerinde incelenerek hâlihazırda yürütülmekte olan çalışmalar hakkında ilgililerden bilgi alınmıştır.

1.4.2.3.1.2 TURKCELL Teknoloji Merkezi Ziyareti

TÜBİTAK Gebze Yerleşkesi sınırları içerisinde bulunan TURKCELL Teknoloji Merkezini ziyaret eden Alt Komisyon Heyeti, Kurumsal Stratejiler ve Regülasyondan Sorumlu Genel Müdür Yardımcısı Dr. Tayfun ÇATALTEPE'nin sunumunun ardından özel hayatın gizliliği ile ilgili hukuki ve teknik konulardaki sorularını şirket yetkililerine iletmışlerdir.

1.4.2.3.1.3 İstanbul Emniyet Müdürlüğü MOBESE Merkezi Ziyareti

Alt Komisyon Heyeti, İstanbul Emniyet Müdür Yardımcısı Hüseyin IŞILDAK ve beraberindeki yetkililerden MOBESE sisteminin alt yapısı ve işleyişi konusunda bilgi aldıktan sonra MOBESE sisteminin işleyişini yerinde incelemiştir.

1.4.2.3.1.4 AVEA Teknoloji Merkezi Ziyareti

Teknolojiden Sorumlu Genel Müdür Yardımcısı Dr. Coşkun ŞAHİN ve beraberindeki şirket yetkilileri tarafından şirket yapısı, AR-GE faaliyetleri ve projeler hakkında bilgilendirilen Alt Komisyon Üyeleri, daha sonra Komisyonun araştırma konusu dâhilinde teknik ve hukuki içerikli sorularını yönelterek, şirketin bizzat yürüttüğü ve destek verdiği AR-GE projelerini incelemiş ve bu projeler hakkında bilgi almışlardır.

1.4.2.3.1.5 VODAFONE Teknoloji Merkezi Ziyareti

Teknik Alt Komisyon, İstanbul Çalışma Ziyareti kapsamında son olarak VODAFONE Teknoloji Merkezi'ni ziyaret etmiştir. İcra Kurulu Başkan Yardımcısı Selçuk KARAÇAY ve beraberindeki yetkililerce kurumsal yapı ve faaliyetler hakkında bilgilendirilen Heyet, daha sonra yetkililere sorularını yöneltmiş ve ziyaret programını böylece sonlandırmıştır.

1.4.2.3.2 ANKAMALL Alışveriş Merkezi Güvenlik Sistem Odası Ziyareti

Teknik Alt Komisyon, ikinci çalışma ziyaretini haberleşme özgürlüğü ve özel hayatın gizliliği çerçevesinde, kamusal alanlarda özel güvenlik kameralarının kullanımı konusunda bilgi almak ve konuyla ilgili sorularını sormak üzere ANKAMALL Alışveriş Merkezi'ne gerçekleştirmiştir. 24.04.2013 tarihinde gerçekleştirilen ziyarete Alt Komisyon Başkanı İstanbul Milletvekili Mihrimah Belma SATIR, Alt Komisyon Üyesi İstanbul Milletvekili Şirin ÜNAL, Alt Komisyon Üyesi İzmir Milletvekili Hamza DAĞ, Alt

Komisyon Üyesi Bolu Milletvekili Ali ERCOŞKUN, Alt Komisyon Üyesi İzmir Milletvekili Erdal AKSÜNGER, Alt Komisyon Üyesi Denizli Milletvekili İlhan CİHANER ve Alt Komisyon Üyesi Elazığ Milletvekili Enver ERDEM'in yanı sıra; Yasama Uzman Yardımcısı İlhan YÜCEL (Türkiye Büyük Millet Meclisi) , Komiser Mevlüt AKGÜL (Emniyet Genel Müdürlüğü), Elektrik-Elektronik Mühendisi Muzaffer ÇALIŞKAN (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı) ve İletişim Uzmanı Ömer SAYILIR (TİB) katılmıştır.

ANKAMALL Müdürü Buğra KÖSE ve beraberindeki yetkililerce güvenlik sistemi ve kameraları hakkında bilgilendirilen Heyet, sistem odasındaki teknik ekipmanı yerinde incelemiş ve yetkililere sistemle ilgili yasal/teknik altyapı ve uygulamalarla ilgili sorular yönelterek çalışmalarını nihayete erdirmiştir.

1.5 Komisyona İntikal Eden Bilgi ve Belgeler

Komisyonumuz, kurulduğu tarihten itibaren çeşitli kurum, kuruluş, üniversite, sivil toplum örgütü ve alanında uzman kişilerden araştırma konusu ile ilgili hususlarda bilgi talep etmiş ve Komisyon raporunun hazırlanması sürecinde ilgililerce gönderilen dokümanlardan yararlanılmıştır.

Komisyonumuza, kuruluş tarihinden itibaren dilekçe, bilgi notu, öneri, yazılı cevap, görevlendirme ve görevlendirme onayı içerikli toplam 49 adet belge ulaşmıştır. Bu belgelerden 26 tanesi şahıslardan gelen talepler, öneri ve bilgi notlarından oluşmaktadır. Bunun yanında çeşitli kurum ve kuruluşlardan (Ekonomi Bakanlığı, Başbakanlık MİT Müsteşarlığı, İçişleri Bakanlığı Mülkiye Teftiş Kurulu Başkanlığı, İçişleri Bakanlığı Emniyet Genel Müdürlüğü, İstanbul Emniyet Müdürlüğü, Bilgi Teknolojileri ve İletişim Kurumu, Telekomünikasyon İletişim Başkanlığı, TÜRKSAT, TÜRKTRUST, AVEA, VODAFONE, TURKCELL) bilgi ve öneri içerikli 13 adet belge Komisyonumuza ulaşmış ve değerlendirilmiştir.

İKİNCİ BÖLÜM

ÖZEL HAYATIN GİZLİLİĞİ VE HABERLEŞME ÖZGÜRLÜĞÜ

2.1 Özel Hayatın Gizliliği ve Korunması

2.1.1 Genel Olarak

Özel hayat kavramı sözlük anlamı olarak bir kişinin kendisine özgü yaşamı, sadece kendisini ilgilendiren tutum ve davranışları¹ şeklinde tarif edilse de bu konuda öğretide ve yargı kararlarında kesin ve net bir tanım bulunmamaktadır.² Bununla birlikte özel hayatın gizliliği ve korunması hakkı hem Anayasamızda hem de Avrupa İnsan Hakları Sözleşmesinde bir temel hak olarak tanınmış ve güvence altına alınmıştır.

Anayasamızda Özel Hayatın Gizliliği ve Korunması başlığı altında Özel Hayatın Gizliliği (m. 20), konut dokunulmazlığı (m. 21) ve haberleşme hürriyeti (m. 22) olmak üzere üç temel kişisel hak yer almaktadır. Özel hayatın gizliliği ve korunması kapsamında değerlendirilen bu haklar kişiyi devlete ve topluma karşı koruyan negatif statü haklardır. Dolayısıyla Devlet, koruma görevinin dışında bu haklara dokunmamalıdır.³

2.1.2 Özel Hayatın Gizliliği

Toplumda yaşayan bireylerin kendilerini güvende hissedebilmeleri, diğer bireylerle sağlıklı ilişkiler kurabilmeleri ve kişiliklerini geliştirebilmeleri için özel hayatın gizliliğinin kişilere ve devlete karşı koruma altına alınması gerekmektedir.⁴

Bu anlamda Türk hukuk sistemine bakıldığında geçmiş anayasalarda özel hayatın korunmasına dair özel hayatın gizliliği ve korunması hakkının içeriğini oluşturacak bir kısım hak ve özgürlüklerin ifade edildiği görülmekle birlikte, “Özel Hayatın Korunması”

¹ Türk Dil Kurumu, Güncel Türkçe Sözlük, <http://tdkterim.gov.tr/bts/22.04.2013>; Yılmaz Ejder Hukuk Sözlüğü, Yetkin Yayınları, 2001 Ankara, s. 692.

² Üzeltürk Sultan, 1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı, İstanbul 2004, s. 3; Danişman Ahmet, Ceza Hukuku Açısından Özel Hayatın Korunması, Selçuk Üniversitesi Yayınları, Konya 1991, s. 7 vd; Akyürek Güçlü, Özel Hayatın Gizliliğini İhlal Suçu (TCK m. 134), Birinci Baskı, Ankara 2011, s. 42; Özbek Veli Özer, TCK İzmir Şerhi Yeni Türk Ceza Kanunun Anlamı, C. 2, Ankara 2008, s. 942; Sezer Yasin/Ipek Ali İhsan/Parlak Engin, Adli ve Önleme Amaçlı İletişimin Denetlenmesi, Gizli Soruşturmacı, Teknik Araçlarla İzleme, Seçkin Yayınevi, Eylül 2012, s. 15.

³ Gözler Kemal, Türk Anayasa Hukuku Dersleri, Ekin Kitabevi Yayınları, 9. Bası, Bursa, 2010, s. 111; Tanör Bülent/Yüzbaşıoğlu Necmi, 1982 Anayasasına Göre Türk Anayasa Hukuku, İstanbul, 2004, s. 169.

⁴ Kaymaz Seydi, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Seçkin Yayıncılık, 1. Baskı, Ankara, 2009, s. 70.

hakkı açık bir şekilde ilk defa 1961 Anayasası'nın 15'inci maddesinde düzenlenmiştir. "Özel hayatın gizliliği" başlıklı söz konusu maddede şu şekildedir:

"(Değişik madde: 20.09.1971 – 1488) Özel hayatın, gizliliğine dokunulamaz. Adli kavuşturmanın gerektirdiği istisnalar saklıdır.

Kanunun açıkça gösterdiği hallerde, usûlüne göre verilmiş hâkim kararı olmadıkça; milli güvenlik veya kamu düzeni bakımından sakınca bulunan hallerde de kanunla yetkili kılınan merciin emri bulunmadıkça kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz."

1982 Anayasası'nda ise, özel hayatın gizliliği 20'nci maddede düzenlenmiştir. Buna göre, *"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz"*. Söz konusu maddenin gerekçesinde de *"Bu madde ile kişinin özel hayatı korunmaktadır. Kişinin özel hayatı ferdi, özel hayat ve ayrı bir kavram ve bir bütün teşkil eden aile hayatından oluştuğu için her ikisi birlikte ifade edilmiştir. Bu anlamda, özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Bu cümleden olarak, mesela basın hürriyeti sınırlandırılabilir, yani kişinin özel hayatı gazete sayfalarında hikâye edilmeyecektir. Söz konusu gizliliğin korunması, ikinci olarak kişinin üstünün, özel kâğıtlarının ve eşyasının aranmaması ile sağlanacaktır"*⁵ denilmiştir.

Anayasa'da düzenlenmiş olan özel hayatın gizliliği hakkı dokunulmaz vazgeçilmez, devredilemez bir hak ve özgürlüktür. Düzenlemeden de anlaşılacağı üzere bu hak kişiye hem devlete karşı hem de diğer kişilere karşı koruma sağlamaktadır.⁶

Anayasa Mahkemesinin ifadesiyle *"özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Orada cereyan edenlerin yalnız kendisi veya kendisinin bilmesini istediği kimseler tarafından bilinmesini istemek hakkı, kişinin temel haklarından biridir. Bu niteliği sebebiyledir ki, özel hayatın gizliliğine dokunulmaması, insan haklarına ilişkin beyanname ve sözleşmelerde korunması istenilmiş, ayrıca tüm demokratik ülke mevzuatında açıkça belirlenen istisnalar dışında bu hak devlet organlarına, topluma ve diğer kişilere karşı korunmuş tur. insanın mutluluğu için büyük önemi olan özel hayata saygı gösterilmesi hakkı onun kişiliği için temel bir hak olup yeteri kadar korunmadığı takdirde kişilerin ve dolayısıyla toplumun*

⁵ Akad Mehmet/Dinçkol Abdullah, 1982 Anayasası, Madde Gerekçeleri ve Maddelerle İlgili Anayasa Mahkemesi Kararları, Alkım Yayınevi, İstanbul, 1998, s. 104.

⁶ Kaymaz, s. 76.

*kendini huzurlu hissedip güven içinde yaşaması mümkün değildir. Bu nedenlerle söz konusu gizliliği çeşitli biçimde ihlal eylemleri suç sayılarak ceza yaptırımlarına bağlanmıştır”.*⁷

Anayasa’nın 20’nci maddesinin ikinci fıkrasında özel hayata müdahalede hâkim kararını şart koşturmakla birlikte, gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış mercilerin emri ile bu hakka müdahale etmeye cevaz verilmiştir.

Kişilerin özel hayat ve aile hayatlarının korunması hakkı uluslararası sözleşmelerde de düzenlenmiş ve güvence altına alınmıştır.

İnsan Hakları Evrensel Bildirgesi’nin 12’nci maddesinde *Hiç kimsenin mahremiyetine, ailesine, evine ya da yazışmalarına keyfi bir şekilde karışamayacağı* düzenlenmiştir. Avrupa İnsan Hakları Sözleşmesi’nin 8’inci maddesinin birinci fıkrasında *"Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesini isteme hakkına sahiptir"* denilmektedir.

AİHM kararlarında her olayda kullanılacak kalıplaşmış bir tanım ve sınırlandırma yapılmayarak, değişik kararlarda özel hayatın içeriğine nelerin girdiği ortaya konulmaya çalışılmıştır.⁸

Diğer haklarda olduğu gibi özel hayatın gizliliği hakkı da sınırsız bir hak niteliğinde değildir. Bazı hallerde bu haklara müdahale edilebilmektedir⁹. Bu özel hayatın gizliliğinin hangi hallerde sınırlanabileceği bu hakkın düzenlendiği Anayasa’nın 20’nci maddede belirtilmiştir. 2001 yılında değişikliğe uğrayan maddede sınırlama nedenleri şu şekilde düzenlenmiştir: *“millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar”* (Ay m. 20).

⁷ Anayasa Mahkemesi, Tarih 31.03.1987, Esas 1986/24, Karar 1987/8 Numaralı Kararı, (www.anayasa.gov.tr: 10.12.2010)

⁸ Sezer/İpek/Parlak, s. 19.

⁹ Anayasa Mahkemesi, Tarih 31.03.1987, Esas 1986/24, Karar 1987/8 Numaralı Kararı, (www.anayasa.gov.tr: 10.12.2010)

Özel hayat kişinin sadece evinde, işyerinde ve sosyal faaliyetlerindeki davranışları ile sınırlı değildir. Kişisel verilerin korunması da özel hayatın gizliliği içerisinde değerlendirilmektedir.¹⁰ Nitekim 2010 yılında yapılan Anayasa değişikliği ile “Herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip” olduğu; “Bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı” hükme bağlanmıştır.

2.1.3 Haberleşme Özgürlüğü

Anayasa’ımızda “Özel Hayatın Gizliliği ve Korunması” başlığı altında düzenlenen haklardan bir diğeri haberleşme özgürlüğüdür. Özel hayatın gizliliği hakkı ile yakın ilişki içerisinde olan haberleşme özgürlüğü gerek 1961 Anayasası’nda gerekse 1982 Anayasası’nda koruma altına alınmış bireysel temel hak ve özgürlüklerdendir.¹¹ Haberleşme özgürlüğü aynı zamanda uluslararası sözleşmeler ve bildirgelerde de koruma altına alınmış bir değerdir.

Haberleşme özgürlüğünün korunması, özel hayatın korunmasının bir görünümü olarak klasik özgürlüklerden olup, hem yazılı olarak gerçekleştirilen iletişimi hem de telekomünikasyon yoluyla kurulan iletişimi kapsamaktadır.

Haberleşme özgürlüğü, Anayasa’nın temel haklar ve ödevler bölüm başlığı altında 22’nci maddesinde düzenlenmiştir. Buna göre, “Herkes haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır” (m. 22).

Madde metninden anlaşılacağı üzere Anayasa öncelikle haberleşme özgürlüğü hakkını kabul etmekte sonra da özel haberleşmenin gizliliğini koruma altına almaktadır. Bu anlamda özel haberleşmeyi, iletişimde bulunan kişilerin gizli kalmasını istediği ve beklediği, iletişim kuran kişiler dışında herhangi bir kimsenin bu bilgilere ulaşmayacağına dair mantıklı ve makul sebeplerinin bulunduğu iletişim olarak tanımlanabilir.¹²

Anayasa’nın 22’nci maddesinin gerekçesinde, “Burada söz konusu olan haberleşme, kişilerin kendi aralarında PTT araçları aracılığıyla serbestçe haberleşebilmesidir. Bu husus dahi özel hayatın bir unsurunu teşkil etmektedir; bu sıfatla haberleşmenin de gizliliğini korumak gerekir. ” denilmiş ise de günümüz itibarıyla kişisel haberleşmenin PTT araçları ile sınırlı olduğunu söylemek mümkün değildir. Teknoloji ve

¹⁰ Sezer/İpek/Parlak, s. 20; Kalabalık Halil, İnsan Hakları Hukuku, Seçkin Kitabevi, Ankara 2009, s.199.

¹¹ Taşkın Mustafa, Adli ve Önleme Amaçlı İletişimin Denetlenmesi, Seçkin Yayınevi, Ankara 2011, 27.

¹² Kaymaz, s. 80.

internetin yaygınlaşmasıyla birlikte haberleşme araç ve yöntemlerinin oldukça gelişmiş ve çeşitlenmiştir. Bu durum karşısında artık haberleşmeyi PTT araçlarıyla sınırlı tutmak mümkün değildir.

Haberleşme özgürlüğü uluslararası alanda İnsan Hakları Evrensel Bildirgesinin 12’nci, Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşmenin 17’nci ve Avrupa İnsan Hakları Sözleşmesinin 8’inci maddesinde koruma altına alınmıştır.¹³

AİHS’nin 8’inci maddesinde özel hayatın gizliliği ve korunması kapsamında düzenlenen haklardan birisi de haberleşme özgürlüğüdür. Sözleşme, özel yazışma ve haberleşmelerin gizliliğinin korunmasını öngörmektedir. Sözleşme bakımından mektuplara el konulması ve açılması veya telefon konuşmalarının dinlenilmesi veya kaydolunması yanında, haberleşmenin engellenmesi de haberleşme hürriyetini ihlal eder.¹⁴

Sözleşmenin 8’inci maddesinin ikinci fıkrasında bazı durumlarda kamu otoritelerine haberleşme hürriyetine müdahale ve sınırlama imkânı verilmiştir. Maddeye göre, *“Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak şartıyla söz konusu olabilir”*.

Haberleşme hürriyetinin sınırlanması konusunda 1982 Anayasası da AİHS’e paralel bir düzenleme getirmiştir. Anayasa’nın 22’nci maddesinin 2001 yılında yapılan değişikliği halinde, *“Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak”* haberleşme hürriyetinin sınırlanabileceği öngörülmüştür.

Haberleşme hürriyetinin sınırlanmasına karar verme yetkisi mahkemeye aittir. Kural olarak *“usulüne göre verilmiş hâkim kararı”* olmadıkça bu özgürlüğe müdahale edilemez. Ancak, gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri ile haberleşmenin engellenmesi ve gizliliğine dokunulması mümkündür. 2001 yılında yapılan değişiklikle yetkili merciin kararının yirmi dört saat içinde görevli hâkimin onayına sunulacağı; hâkimin kararını kırk sekiz saat içinde açıklayacağı; aksi halde, karar kendiliğinden kalkacağı hükme bağlanmıştır.

¹³ Taşkın, s. 27.

¹⁴ Sezer/İpek/Parlak, s. 30.

2.1.4 Özel Hayatın Korunması

Anayasal güvenceye bağlanan özel hayatın gizliliği hakkının ihlal edilmesi Türk Ceza Kanununda birçok maddede yaptırıma bağlanmıştır. Haberleşme hürriyetinin korunmasına yönelik olan TCK'nın 124'üncü maddesinde¹⁵, kişiler arası haberleşmenin hukuka aykırı olarak engellenmesi suç sayılarak müeyyideye tabi tutulmuştur. Bu madde kapsamında 3 ayrı suç düzenlenmektedir. Maddenin birinci fıkrasında “*kişiler arasındaki haberleşmenin engellenmesi*”, ikinci fıkrasında “*kamu kurumları arasındaki haberleşmenin engellenmesi*”, üçüncü fıkrasında ise, “*basın yayın organının yayınının engellenmesi*” ayrı ayrı düzenlenmiştir.¹⁶

Haberleşme hürriyetinin korunmasına yönelik olarak TCK'da düzenlenen bir diğer suç haberleşmenin gizliliğini ihlal suçudur. Bu suçun düzenlendiği 132'nci madde 2.7.2012 tarih ve 5362 sayılı “Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun”un 79'uncu maddesi ile değişikliğe uğratılmış ve cezalar artırılmıştır. “Haberleşmenin gizliliğini ihlal” başlıklı maddenin değişik hali şu şekildedir:

“(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. (Ek cümle: 2/7/2012-6352/79 md.) İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

TCK'nın “Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması”

¹⁵ TCK'nın “Haberleşmenin Engellenmesi” Başlıklı 124. Maddesi:

“(1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adli para cezasına hükmolunur.

(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi halinde, ikinci fıkra hükmüne göre cezaya hükmolunur.”

¹⁶ Gökçen Ahmet, Ceza Muhakemesi Hukukunda Basit Elkoyma ve Postada Elkoyma, DEÜHF Döner Sermaye İşletme Yayınları No: 49, Ankara 1994, s. 36

başlıklı 133'üncü maddesinde kişiler arasındaki aleni olmayan konuşmaların tarafların rızası olmadan dinlenmesi ve kayda alınması ayrı bir suç olarak düzenlenmiştir. Bu madde de 5362 sayılı Kanunun 80'inci maddesi ile değişikliğe uğratılmış ve cezalar artırılmıştır. Maddenin değişik hali şu şekildedir:

“(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.

(3) (Değişik: 2/7/2012-6352/80 md.) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adli para cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

Özel hayatın gizliliği hakkının ihlal edilmesi TCK'nın 134'üncü maddesinde suç olarak düzenlenmiştir. “Özel Hayatın Gizliliğini İhlâl” başlıklı madde şu şekildedir:

“(1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.

(2) (Değişik: 2/7/2012-6352/81 md.) Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

Maddeye göre, kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılacaktır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde ise verilecek ceza bir kat artırılacaktır.

Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa edilmesi veya ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması hali de suç olarak tanımlanmış ve bu fiili gerçekleştirenlere iki yıldan beş yıla kadar hapis cezası öngörülmüştür.

Kişisel verilerin kaydedilmesi, verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi de TCK'nın 135 ve 136'ncı maddelerinde suç olarak düzenlenmiştir. Yine Kanunun 137'nci maddesinde de tüm bu suçları kapsayacak şekilde bu suçların nitelikli hallerinin neler olacağı belirtilmiştir. Buna göre, özel hayatın gizliliğine karşı işlenen suçların kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek veya sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halleri suçun nitelikli halleridir ve bu durumda verilecek ceza yarı oranında artırılacaktır.

Ayrıca TCK'nın takip eden maddelerinde hukuka aykırı olarak kişisel verilerin kayıt edilmesi ve bu verilerin başkasına verilmesi, yayılması, kanundaki süreler geçmiş olmasına rağmen kişisel verilerin silinmemesi suç olarak düzenlenmiştir (TCK 135, 136, 138 md).¹⁷ Kişisel veriden ne anlaşılması gerektiği TCK'nın 135'inci maddesinin gerekçesinde, gerçek kişiyle ilgili her türlü bilgi şeklinde tarif edilmiştir.

Buraya kadar açıklanan ceza hukuku yaptırımları yanında ihlaller özel hukukta da bazı yaptırımlarla karşılaşılabilecektir. Türk Medeni Kanunu ve Borçlar Kanununda özel hayatın gizliliğinin ihlaline ilişkin doğrudan bir düzenleme mevcut değildir. Ancak, TCK anlamında suç teşkil eden bu fiiller, özel hukuk bakımından da haksız fiil teşkil edeceğinden cezai sorumluluk yanında hukuksal sorumluluğu da gerektirecektir. Dolayısıyla özel hayatın gizliliğinin ihlalleri mağdurlara özel hukuk anlamında tazminat davası açma hakkı da tanımaktadır.¹⁸

2.1.5 İletişimin Denetlenmesini Gerektiren Sebepler

Teknoloji, ulaşım, iletişim, ekonomik aktiviteler gibi birçok alanda meydana gelen hızlanma ve çeşitlenme kendisini suç dünyasında da göstermiş ve suçun küresel bir boyut

¹⁷ TCK'nın "Kişisel Verilerin Kaydedilmesi" Başlıklı 135'nci maddesi:

"(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırkı 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."

"Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme" Başlıklı 136'nci maddesi:

"(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır."

"Nitelikli Haller" Başlıklı 137'nci maddesi:

"(1) Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle,

işlenmesi halinde, verilecek ceza yarı oranında artırılır."

"Verileri Yok Etmeme" Başlıklı 138'inci maddesi:

"(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir."

¹⁸ Kaymaz, s. 92.

kazanmasına, suçla ilgili problemlerin büyümesine ve evrenselleşmesine neden olmuştur.¹⁹

İnsanlık günümüzde eskiye nazaran çok daha karmaşık ve çok yapıli terörist ve organize suç örgütleri ile karşı karşıya bulunmaktadır. Her geçen gün de büyüme gösteren bu suç örgütleriyle mücadele demokratik toplumlar için en önemli vazifelerden biri haline gelmiştir.²⁰

Bu vazifenin yerine getirilmesi sırasında başarıya ulaşılabilmesi için geleneksel güvenlik yapılanmaları çoğu zaman yeterli olmamaktadır. Bu noktada suçla mücadelede kullanılan klasik yöntemlerin güçlendirilmesi ve bunlara ek olarak yeni bazı tedbirlerin hayata geçirilmesi zorunlu hale gelmiştir. Bu bağlamda iletişimin denetlenmesi, bu yeni tedbirlerden birisi olarak karşımıza çıkmaktadır.²¹

Zira son yıllarda klasik ceza muhakemesi tedbirleri ile bu nitelikte suç ve suçlularla etkin mücadele mümkün olamamaktadır. Suçlular, özellikle örgütlü olarak hareket eden gruplar, bilişim alanındaki teknolojik imkânları faaliyetleri sırasında oldukça sık kullanmaktadırlar. Bu nedenle güvenlik görevlilerinin de suçun önlenmesi ve aydınlatılması amacıyla çağa uygun yöntemleri profesyonelce kullanmaları gerekmektedir. Buna paralel olarak teknolojik gelişmelere uygun suçla ve suçlulukla etkin bir mücadele yürütülebilmesine elverişli ceza muhakemesi tedbirlerinin uygulamaya konulması gerekmektedir. Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri de bunlardan birisi olarak ortaya çıkmıştır.²²

Bugün gelinen noktada da ülkemizde çok sayıda suçun delillerinin bulunmasında ve şüphelilerin yakalanmasında iletişimin denetlenmesi tedbirinin kullanıldığı görülmektedir.

2.2 Mukayeseli Hukukta İletişimin Denetlenmesi

2.2.1 Genel olarak

Avrupa ülkelerinde yıllardan beri suçla ve özellikle de örgütlü suçlarla mücadelede telefon ve benzeri telekomünikasyon araçlarının dinleme yöntemi yaygın olarak kullanılmaktadır.²³

Özellikle 11 Eylül 2001 tarihinde ABD’de meydana gelen terör olayından sonra

¹⁹ Güvel Enver Alper, Organize Suç Ekonomisi ve Hukuk Uygulaması, Ankara 2004, s. 86.

²⁰ Polat Ahmet, Fransa’da Terörizme Karşı Mücadele, Polis Dergisi, Yıl 11, Sayı 46, Ekim-Kasım-Aralık 2005, s. 204.

²¹ Taşkın, s. 28

²² Keklik Ramazan, Ceza Yargılamasında İletişimin Denetlenmesi, Adalet Dergisi, Sayı 25, s.1.

²³ Taşkın, s. 37

Avrupa Birliđinin ve ABD'nin istihbarata olan yaklaşımı deđiřmiř bu alanda yeni d zenlemelere gidilmiřtir.

Avrupa Birliđi  lkelerinde ađır su larla m cadelede istihbari bir teknik olarak telefonların dinlenilmesi genellikle standart olarak uygulanmaktadır.

Avrupa İnsan Hakları Mahkemesi de telefonların gizlice dinlenmesini, b y k su lar ya da ter rizmle m cadele gibi hallerle sınırlı olmak  zere kabul etmektedir.

Avrupa Parlamentosunun 2001/2098(1 INI)²⁴ sayılı raporunda; devletlerin, ulusal g venliđin sađlanması amacı ile dinleme faaliyetlerini y r t lebilmelerinin kabul edilebilir olduđunu vurgulamıřtır.²⁵

Avrupa Birliđi  yesi  lkelerin, ceza muhakemesi kanunlarında, kovuřturma organlarına telekom nikasyon yoluyla yapılan iletiřimin denetlenmesine olanak sađlayan d zenlemeler ve deđiřiklikler yaptıđı g r lmektedir. Bu y ntemin kullanılmasının kiři hak ve h rriyetlerine m dahale sayıldıđı i in yasal temelde sıkı řartlara bađlanmıřtır. İstisnaları olmakla birlikte bu yolla elde edilen bilgiler genel olarak delil sayılmamakta ve kullanılamamaktadır. Bu bilgilerle bařka delillere ulařılmakta ve mahkemelere bu deliller sunulmaktadır.²⁶

2.2.2 Almanya

Federal Almanya Anayasası'nın 10'uncu maddesinde, yazıřma gizliliđi ile posta, telgraf ve telefonla yapılan iletiřimin gizliliđi koruma altına alınmıřtır. Ayrıca bu dokunulmazlıklara ancak bir kanunla sınırlama getirilebileceđi, bu kanunun da hakkın  z ne dokunamayacađı h kme bađlanmak suretiyle haberleřme gizliliđinin temel bir hak olduđu belirtilmiřtir.²⁷

Almanya'da teknik dinleme, "G10" adlı kanun ile d zenlenmiřtir. Teknik dinlemenin kullanılabileceđi su lar, Alman Ceza Muhakemeleri Usul  Kanunu'nun 108. maddesinde tek tek sayılmak suretiyle listelenmiřtir. Bu su lar; bir su  organizasyonu  yesi olmak, cinayet, para ile ilgili su lar, soygun, gasp, illegal uyuřturucu ve silah ticareti,

²⁴ <http://www.europarl.europa.eu> (E. 2. 11.09.2007)

²⁵ 5397 sayılı Kanunun Genel Gerekeři.

²⁶ Tařkın, s. 37.

²⁷ Erdem Mustafa Ruhan/ zbek Veli  zer, 4422 Sayılı  ıkar Ama lı Su   rg tleriyle M cadele Kanunu  er evesinde Uzakla Haberleřmenin Denetlenmesi, Prof. Dr. Seyfullah Edis'e Armađan, İzmir 2000, s. 259; S z er Adem, T rkiye'de ve Karřılařtırmalı Hukukta Telefon Telefaks Faks ve Benzeri Ara larla Yapılan  zel Haberleřmenin Bir Ceza Yargılaması  nlemi Olarak Denetlenmesi, İstanbul  niversitesi Hukuk Fak ltesi Mecmuası, Yıl 1997, Sayı 3, Cilt LV, s. 88.

terörizm, vatana ihanet ve casusluk suçlarıdır.²⁸

Alman Ceza Muhakemesi Kanunu'nun 100a-1 hükmüne göre, bir kimsenin bu maddede sayılan suçları işlediğine veya işlemeye teşebbüs ettiğine dair belirli bir vakıya dayalı somut şüphe sebebi var ise ve olayın veya sanığın bulunduğu yerin başka türlü araştırılarak ortaya çıkarılması imkânsız ise veya çok zor olacaksa, bu kimsenin telefon görüşmelerinin polis tarafından dinlenmesine ve kaydedilmesine karar verilebilmektedir.²⁹ Bu tedbir bir suç işlenmesinden sonra uygulanabilen adli amaçlı bir tedbirdir.³⁰

Tedbire karar verme yetkisi hâkimdedir, ancak hâkime erişilemediği acil durumlarda savcı, 3 güne kadar dinleme kararı verme yetkisine sahiptir. Bu durumlarda savcı tarafından verilen iletişimin denetlenmesi kararı 3 gün içinde hâkim tarafından onaylanmalıdır. Aksi halde dinlemeye son verilecektir. Hâkim tarafından verilen ilk dinleme kararı en fazla 3 ay olabilmekte, koşulların gerçekleşmesi halinde ise, bu süre 3 ay daha uzatılabilmektedir.³¹

Alman hukukunda da ülkemizde olduğu gibi teknik dinlemeye son çare olması durumunda başvurulabilmektedir.

Almanya'da milletvekillerinin anayasadan kaynaklanan dokunulmazlıkları kapsamında iletişimlerinin denetlenmesinin tamamen yasak olduğu kabul edilmektedir.³²

İletişimin denetlenmesi tedbiri sırasında elde edilecek tesadüfi deliller sadece katalog suçlarla ilgili olması durumunda delil olarak kullanılabilir, katalog haricindeki suçlarla ilgili olması durumunda ise kullanılamamaktadır.³³

Alman kanunlarına göre iletişimin denetlenmesi tedbirinin sona ermesi halinde ilgililere haber verilmesi gerekmektedir.³⁴

Ayrıca Almanya'da buraya kadar açıklanan adli iletişimin denetlenmesi tedbiri yanında istihbarat örgütleri tarafından önleyici amaçlı iletişimin denetlenmesi tedbirine de

²⁸ Yenisey Feridun, Çıkar Amaçlı Örgüt Suçlarındaki Araştırmalar, Hukuk Kurultayı 2000, Cilt 2, Ankara, 119; NUHOĞLU Ayşe, Adli Amaçlı Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi ile Teknik Araçlarla İzleme Tedbirine Konu Olan Suçlar, Yargı Dünyası, Sayı 128, Ağustos 2006, s. 10; Erdem/Özbek, s. 256.

²⁹ Erdem/Özbek, S. 279; Sözüer, S. 89.

³⁰ Sözüer, S. 89.

³¹ Yenisey, S. 119; Sözüer, S. 90.

³² Erdem/Özbek, S. 272.

³³ Sözüer, s. 91.

³⁴ Erdem/Özbek, s. 288.

başvurulabilmektedir.³⁵

2.2.3 Fransa

Haberleşmenin gizliliğinin korunmasına yönelik olarak Fransa Anayasası'nda açık bir düzenleme bulunmamaktadır. Ancak kişisel özgürlük hakkı yazılı olmayan bir anayasal hak olarak kabul edilmektedir.³⁶

Fransa'da iletişimin denetlenmesi adli denetleme ve idari denetleme olmak üzere ikiye ayrılmıştır. Adli denetleme bir suç soruşturması için kullanılırken, idari denetleme terör ve ağır organize suçların önlenmesi amacıyla kullanılmaktadır.³⁷

Fransa'da iletişimin denetlenmesi sıkı koşullara bağlanmış bir tedbirdir. Fransız Ceza Muhakemesi Kanununun 100 ilâ 100-7 maddeleri arasında adli amaçlı iletişimin denetlenmesi düzenlenmiştir. Bu maddeler gereğince telekomünikasyon yoluyla yapılan iletişimin dinlenmesi, saptanması ve kaydedilmesi işlemleri yapılabilmektedir.³⁸

Adli amaçlı iletişimin denetlenmesi kararı, sadece soruşturma hâkimi tarafından 2 yıl ve daha fazla hapis cezası öngörülen suç veya kabahatler için verilebilmektedir.³⁹ Hazırlık soruşturması sırasında savcı ya da polis suçüstü halinde dahi iletişimin denetlenmesi kararı verememektedir.

Adli amaçlı iletişimin denetlenmesinde Fransa'da da son çare ilkesi benimsenmiştir. Buna göre iletişimin denetlenmesi kararı verilebilmesi için başka şekilde delil elde edilme olasılığının bulunmaması gerekmektedir. Buna ek olarak suç işlendiğine dair kuvvetli belirtiler bulunması da gerekmektedir.⁴⁰

İletişimin denetlenmesi kararı en fazla 4 ay süre için verilebilmekte ve aynı usulle 12 aya kadar uzatılabilmektedir.⁴¹

Meclis başkanına bilgi verilmedikçe hiç bir halde bir milletvekili ya da senatörün hattı için iletişimin denetlenmesi tedbiri uygulanamamaktadır.⁴²

Sanığın, müdafii ile kurduğu iletişim koruma altındadır ve denetlenmesi belirli

³⁵ Sözüer, s. 89.

³⁶ Erdem/Özbek, s. 259.

³⁷ Sözüer, s. 97; Taşkın, s. 47.

³⁸ Taşkın, s. 48.

³⁹ Sözüer, s. 95; Taşkın, s. 48.

⁴⁰ Taşkın, s. 48.

⁴¹ Sözüer, s. 96.

⁴² Taşkın, s. 49.

şartlara bağlanmıştır. Bu korumadan müdafilerin yanında hekimler, eczacılar gibi meslek mensupları da yararlanır.⁴³

Hâkimler bakımından da bir denetleme yasağı mevcuttur. Buna göre, Birinci başkan veya Yargılama Kurulu Başsavcısı bilgilendirilmeden hiç bir hâkimin evi ve bürosunun iletişimi denetlenememektedir. Bununla birlikte tanıklıktan çekinme hakkı sahiplerinin, şüpheli veya sanıkla gerçekleştirdikleri iletişimin denetlenmeyeceğine dair düzenleme bulunmamaktadır.⁴⁴

Fransa’da iletişimin adli amaçlı denetlenmesi kadar önleme amaçlı denetlenmesi de sıkı kurallara bağlanmıştır. Önleme amaçlı iletişimin denetlenmesi 1991 yılında çıkartılan 91-646 sayılı Kanunla düzenlenmiştir. Bu Kanunun 3’üncü maddesine göre, “*milli güvenliği, Fransa’nın bilimsel ve ekonomik varlığının (potansiyelinin) temel unsurlarını korumak, terörizmi, örgütlü suçluluğu ve 10 Ocak 1936 tarihli Kanunla ilga edilmiş olan özel savaş gruplarının ve milislerin yeniden teşkili ve muhafazası hakkındaki çabaları ortaya çıkarmak amacı ile telekomünikasyon vasıtası ile yapılan haberleşmelerle müdahaleye (girmeye) istisnai olarak ve 4. maddenin belirlediği koşullarla izin verilebilir*”. Önleme dinlemesine karar verilme usulünün hükme bağlandığı söz konusu Kanunun 4’üncü maddesine göre önleme dinlemesi başbakan veya onun tarafından özel yetki verilmiş olan iki kişiden birisinin yazılı ve gerekçeli kararıyla mümkün olmaktadır. Görevlendirmeye bu yetkinin genellikle içişleri bakanına verildiği görülmektedir. Önleme dinlemesi sonunda elde edilen bilgiler yargılama aşamasında delil olarak kullanılamaz.

Fransa’da önleme dinlemesi kararı en fazla 4 ay için verilebilmektedir. Ancak aynı koşulların bulunması ve gerekli olması durumunda bu süre uzatılabilmektedir.⁴⁵

Önleme dinlemesi sonunda elde edilen bilgiler yargılama aşamasında delil olarak kullanılamamaktadır. Ancak önleyici dinleme yapıldığı sırada bir suçu işlendiğine dair delil elde edilmesi halinde, bu dinleme adli dinlemeye dönüştürülebilmektedir. Bu şekilde önleyici dinlemelerin yarısına yakınında suç işlendiğine dair delil ortaya çıkması nedeniyle adli dinlemeye dönüştürülmüştür.

Fransa’da önleme dinlemelerinin kanuna uygun bir şekilde ve tek elden yürütülmesini sağlamakla görevli bir Güvenlik Dinlemeleri Milli Kontrol Komisyonu (Commission Nationale de Contrôle des Interceptions de Sécurité -CNCİS-) kurulmuştur.

⁴³ Sözüer, s. 96; Taşkın, s. 50.

⁴⁴ Taşkın, s. 50.

⁴⁵ Taşkın, s. 51

Bağımsız bir idari otorite statüsünde çalışmakta olan Komisyonun başkanı, Danıştay ikinci başkanı ve Yargıtay birinci başkanınca birlikte meydana getirilen ve dört ismi içeren bir listeden Cumhurbaşkanı tarafından seçilmektedir. Başkanının görev süresi 6 yıl olan Komisyon Meclisin seçtiği bir üye ile senatonun seçtiği bir üye de yer almaktadır. Komisyonun diğer görevlileri başkan tarafından atanmaktadır. Bu Komisyonun üyeleri hükümet içinde başka bir görev alamamaktadırlar ve başkan da dâhil görevleri sırasında öğrendikleri bilgiler bakımından gizlilik ilkesine uygun davranmak zorundadırlar. Komisyon başvuru üzerine yapılmakta olan bir dilemenin kanuna uygun olup olmadığını her zaman denetleyebileceği gibi resen de böyle bir denetime girişebilmektedir. Komisyon her yıl yürütülen faaliyetler ve bunların sonuçları hakkında bir rapor hazırlamakta ve Başbakan'a sunmaktadır. Bu raporların yayınlanarak kamuoyunun bilgilendirilmesi de mümkündür.⁴⁶

2.2.4 İngiltere

İngiltere’de iletişimin denetlenmesi 25.07.1985 tarihli Haberleşmeye Müdahale Kanunu (Interception of Communications Act) ile düzenlenmiştir.⁴⁷

Haberleşmenin denetlenmesi kararı milli güvenliğin sağlanması, ağır suçların önlenmesi ve araştırılması ile Birleşik Krallığın mali değerlerinin korunması amaçlarıyla verilebilmektedir.⁴⁸

İngiltere’de bu tedbire karar verilebilmesi için en az 3 yıl hürriyeti bağlayıcı ceza gerektiren bir suçun söz konusu olması gerekmektedir. Ayrıca çok sayıda kişinin ortak bir amaç etrafında birleşerek işledikleri suçlar da ağır suç sayılmakta ve iletişimin denetlenmesi tedbiri uygulanabilmektedir.⁴⁹

Karar verme yetkisi İngiltere ve Galler’de İçişleri Bakanına aittir. Diğer ülkelerin tersine İngiltere’de iletişimin denetlenmesi kararı verme yetkisi idari mercilere verilmiştir.⁵⁰

Tedbir kararı verilebilmesi için suç işlendiğine ilişkin özel bir şüphe derecesi aranmamıştır. Suç işlendiğinin ispatlanması için zorunlu olması ve başka yollarla bu

⁴⁶ Taşkın, s. 52,53.

⁴⁷ Sözüer, s. 92.

⁴⁸ Sözüer, s. 93.

⁴⁹ Sözüer, s. 93.

⁵⁰ Sözüer, s. 93. Erdem/Özbek, s. 284.

bilgilerin elde edilmesinin çok zor olması durumunda bu tedbir uygulanabilecektir.⁵¹

Kanunda belirtilen şartlar dışında iletişimin denetlenmesi suç olarak tanımlanmıştır. Ayrıca bu şekilde elde edilen bilgiler de mahkemelerde delil olarak kullanılamamaktadır.

İletişimin denetlenmesi kararları kural olarak 2 ay için verilebilmektedir. Bu süre gerektiğinde birer aylık sürelerle uzatılabilmektedir. Milli güvenlik ve ülkenin düzeni ile ilgili konularda 6 aylık uzatma da mümkündür. Ayrıca acil durumlarda güvenlik kuvvetlerinin 2 günlük dinleme yetkisi bulunmaktadır.⁵²

Sanığın müdafisinin veya tanıklıktan çekinme hakkı olanların şüpheli veya sanıkla kurdukları iletişimin denetlenmeyeceğine dair bir sınırlama bulunmamaktadır.⁵³

İngiltere’de milletvekillerinin iletişimlerinin denetlenemeyeceği kanunla hüküm altına alınmıştır.⁵⁴

İletişimin denetlenmesine ilişkin olarak yürütülen işlemler, karşılaşılan sorunlar, gerçekleştirilen denetleme sayısı gibi bilgiler kurulmuş olan komisyon tarafından her yıl rapor halinde başbakana sunulmaktadır. Ayrıca bu raporun daha sınırlı hali parlamentoya da sunulmaktadır.⁵⁵

2.2.5 Avusturya

Avusturya’da haberleşmenin gizliliğinin korunması Anayasa’da hüküm altına alınmıştır.⁵⁶

Özel haberleşmelerin bir ceza yargılaması tedbiriyle denetlenmesinin esas ve usulleri Avusturya Ceza Usul Kanununa 1974’te eklenen 149a, 149b ve 414a maddelerinde düzenlenmiştir. Bu hükümlere göre, iletişimin denetlenmesi tedbirine, işlenmiş bir suçun aydınlatılması ve bir kaçağın veya sanık statüsünde birisinin yerinin tespiti amacıyla başvurulabilmektedir. Avusturya’da sadece adli amaçlı iletişimin denetlenmesi mümkün olup, önleme amaçlı olarak iletişimin denetlenmesine başvurulamamaktadır.⁵⁷

Avusturya Ceza Usul Kanununa göre en az 1 yıl ve daha üzeri hapis cezası gerektiren kasıtlı suçlarla ilgili olarak iletişimin denetlenmesi kararı verilebilmektedir.

⁵¹ Sözüer, s. 93. Erdem/Özbek, s. 276.

⁵² Taşkın, s. 54.

⁵³ Sözüer, s. 93. Erdem/Özbek, s. 270.

⁵⁴ Taşkın, s. 55.

⁵⁵ Erdem/Özbek, s. 289.

⁵⁶ Erdem/Özbek, s. 259.

⁵⁷ Sözüer, s. 100.

Ancak ilgilinin rızasının olması halinde 6 ay ve üzeri hapis cezası gerektiren kasıtlı suçlar için bu tedbire başvurulabilmektedir.⁵⁸

İletişimin denetlenmesi Tedbirine karar verilebilmesi için tutuklama tedbirinde olduğu gibi “kuvvetli suç şüphesinin” varlığı gerekmektedir.⁵⁹

Telefon dinlemeye kural olarak Avusturya yüksek mahkemesinin bir dairesi olan üç hâkimden oluşan bir kurul tarafından karar verilmektedir. Denetleme talebi savcıdan ön soruşturmayı yürüten hâkime gönderilmekte, hâkimin kurula ilettiği talebin uygun bulunması halinde tedbire hükmedilmektedir. Gecikmesinde sakınca bulunan hallerde soruşturma hâkimi tarafından da karar verilebilmekte ancak bu durumda karar en kısa sürede kurulun onayın sunulması gerekmektedir. Kurulun bu kararı onaylamaması durumunda yapılan tespitlerin ve kayıtların imhası gerekmektedir.⁶⁰

Avusturya’da avukatların müdafilerin, noterlerin ve mali müşavirlerin özel haberleşme araçları, denetlenemez. Ancak sanık yakınları ve hekimler için bu şekilde bir kısıtlamaya yer verilmemiştir.⁶¹

İletişimin denetlenmesi tedbirinin uygulanmasının sona ermesi halinde tedbire muhatap olan kişinin müdafisine konuyla ilgili bilgi verilmesi gerekmektedir.⁶²

2.2.6 İtalya

İtalya’da iletişimin denetlenmesi Ceza Yargılama Yöntem Yasasının 226’ncı maddesinde sınırlı olarak sayılmış bulunan uyuşturucu madde, silah ve patlayıcı madde kaçakçılığı, telefonun suç işleme aracı olarak kullanıldığı suçlar (hakaret tehdit gibi) ile cezasının alt sınırı 5 yıldan fazla hapis cezası gerektiren suçlar için kabul edilmiştir.⁶³

Soruşturma aşamasında iletişimin denetlenmesi tedbirine başvurulabilmesi için savcının talebi ve hâkim kararı gerekmektedir. Ancak acele hallerde savcı da iletişimin denetlenmesine karar verebilmektedir. Bu durumda savcının verdiği kararın 24 saat içerisinde hâkim onayına sunulması ve hakim de 48 saat içinde karar vermesi gerekmektedir.

Tedbire karar verilebilmesi için suça dair kuvvetli belirtiler bulunmalı ve iletişimin

⁵⁸ Nuhoğlu, s. 10.

⁵⁹ Sözüer, s. 101; Erdem/Özbek, s. 276.

⁶⁰ Sözüer, s. 101; Erdem/Özbek, s. 284.

⁶¹ Sözüer, s. 101.

⁶² Erdem/Özbek, s. 288.

⁶³ Nuhoğlu, s. 10; Sözüer, s. 101.

denetlenmesinin zorunlu olması gerekmektedir.⁶⁴

İletişimin denetlenmesi kararı en fazla 15 gün için verilebilmektedir. Ancak gerekli görülmesi halinde hâkim kararıyla her defasında aynı süreyle uzatılmasına karar verilebilmektedir.

Ağustos 1992 tarihinde yapılan yasa değişikliği ile organize suçlar bakımından iletişimin denetlenmesi tedbirine başvurmak için aranan şartlar biraz daha kolaylaştırılmıştır.⁶⁵

İtalyan hukukunda önleme amaçlı iletişimin denetlenmesi tedbirine de yer verilmiştir. Buna göre devlete karşı suçlar, adam öldürme, yağma, organize suçlar, adam kaçırma suçları bakımından önleme amaçlı iletişimin denetlenmesi mümkündür. İçişleri bakanı, emniyet müdürleri, Carabini komutanları, maliye ve polisler savcıya başvurarak telefon dinleme talebinde bulunabilirler.

Önleme amaçlı iletişimin denetlenmesi sonucu elde edilen kayıtlar ceza yargılamasında delil olarak kullanılamamaktadır.⁶⁶

2.3 Türk Hukukunda İletişimin Denetlenmesi

2.3.1 Tarihsel Gelişim

2.3.1.1 1961 ve 1982 Anayasaları

Haberleşme hürriyeti, 1961 Anayasası'nın "II. Özel Hayatın Korunması" üst başlığı altında "C Haberleşme Hürriyeti" başlıklı 17'nci maddesinde düzenlenmiştir. Düzenlemeye göre;

"Herkes, haberleşme hürriyetine sahiptir.

Haberleşmenin gizliliği esastır. Kanunun gösterdiği hallerde, hakim tarafından kanuna uygun olarak verilmiş bir karar olmadıkça, bu gizliliğe dokunulamaz."

Metinden de anlaşılacağı üzere maddenin birinci fıkrasında haberleşme özgürlüğü koruma altına alınmaktadır.

Maddenin ikinci fıkrasında ise, hangi hallerde ve hangi koşullarla bu özgürlüğün sınırlandırılacağı hükme bağlanmıştır. Buna göre haberleşme özgürlüğü sadece hâkim kararıyla sınırlandırılabilir. 1982 Anayasası'nda bulunan gecikmesinde sakınca

⁶⁴ Sözüer, s. 107; Taşkın, s. 58.

⁶⁵ Taşkın, s. 56.

⁶⁶ Sözüer, s. 108.

bulunan halde yetkili merciin emriyle bu sınırlandırılması ilkesi 1961 Anayasası’nda kabul edilmemiştir.

Haberleşme özgürlüğü, 1982 Anayasası’nın “IV. Özel Hayatın Gizliliği ve Korunması” üst başlığı ve “C. Haberleşme Hürriyeti” kenar başlığı altında 22’nci maddesinde düzenlenmiştir. 1961 Anayasası’nda olduğu gibi 1982 Anayasası’nda da haberleşme özgürlüğü, özel hayat kapsamında koruma altına alınmıştır. 1982 Anayasası’nda “Özel Hayatın Gizliliği ve Korunması” başlığı altında “Özel Hayatın Gizliliği” (m. 20), “Konut Dokunulmazlığı” (m. 21) ve “Haberleşme Hürriyeti” (m. 22) olmak üzere üç temel kişisel hak yer almaktadır.

2.3.1.2 1412 Sayılı Ceza Muhakemeleri Usulü Kanunu

4422 sayılı Kanun yürürlüğe girinceye kadar mevzuatımızda doğrudan ve açıkça adli ve önleme amaçlı iletişimin denetlenmesini düzenleyen bir hüküm bulunmamaktaydı.⁶⁷ Bu boşluk CMUK’un arama ve elkoymaya ilişkin hükümlerinin kıyas yoluyla uygulanması yoluyla doldurulmuş ve telekomünikasyon yoluyla yapılan iletişimin denetlenmesi mümkün kılınmıştı.⁶⁸ Ayrıca CMUK’un 91’inci maddesinde,

“Maznuna gönderilen mektuplar vesair mersule ve telgrafların posta ve telgrafhanede zaptı caizdir.

Maznun tarafından veya ona hitaben gönderildiği bazı hallerden anlaşılan ve tahkikat noktai nazarından münderecatının ehemmiyeti haiz olduğu tayin edilen mektuplar vesair mersule ve telgrafların dahi bu yerlerde zaptı caizdir.”

Şeklinde düzenlenmiş olan maddede geçen “vesair mersule” deyimini, kıyas yoluyla telefonları da kapsayacak şekilde yorumlanarak iletişimin denetlenmesi sağlanmakta idi.⁶⁹

2.3.1.3 2559 Sayılı Polis Vazife ve Salahiyet Kanunu

İletişimin denetlenmesi konusunda 2559 sayılı kanunun ilk halinde de bir düzenleme mevcut değildi. Ancak maddenin 1985 yılında değiştirilen ek 7’nci maddesi geniş yorumlanmak suretiyle önleyici kolluk hizmetleri için istihbarat faaliyetlerinde

⁶⁷ Ünver/Hakeri, s. 188.

⁶⁸ Kunter Nurullah/Yenisey Feridun/Nuhoğlu Ayşe, Muhakeme Dalı Olarak Ceza Muhakemesi Hukuku; Beta Yayınları; 15. Bası; İstanbul 2006, s. 697.

⁶⁹ Ersoy Yüksel, Özel Telefon İşletmelerinin Dinleme ve Bilgi Verme Sorunları, Prof. Dr. Çetin Özek Armağanı, İstanbul 2004, s. 317; Taşkın, s. 63.

bulunma yetkisine dayanak sağlanmaktaydı.⁷⁰ 2559 sayılı Kanunun 16.6.1985 tarih ve 3233 sayılı Kanunla değiştirilmiş ek 7'nci maddesi şu şekildedir:

“Polis, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayiş sağlamak üzere, ülke seviyesinde istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla işbirliği yapar.”

2.3.1.4 2803 Sayılı Jandarma Teşkilat Görev ve Yetkileri Kanunu

2559 sayılı kanun için yapılan açıklamalar 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu için de geçerli diyebiliriz. Zira 2559 sayılı Kanunun 25'inci maddesinde *“Polis teşkilatı bulunmayan yerlerde il, ilçe ve bucak jandarma komutanları ile jandarma karakol komutanları bu kanunda yazılı vazifeleri yapar ve yetkileri kullanır”* hükmü uyarınca polise verilen istihbarat toplama görev ve yetkisinin jandarma tarafından da kullanılabileceği kabul edilmekte idi.

Ayrıca 2803 sayılı Kanunun 7'nci maddesinde de *“suç işlenmesini önlemek için gerekli tedbirleri almak ve uygulamak”* şeklinde jandarmanın görevlerini düzenleyen madde de geniş yorumlanmakta idi.⁷¹

2.3.1.5 2937 Sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu

İletişimin denetlenmesi konusunda açık bir hüküm 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda da yer almamaktaydı. Söz konusu Kanunun 4'üncü maddesinde MİT'in görevleri sayılmıştır.⁷² Maddede geçen görevler

⁷⁰ Ersoy, s. 331; Erdem/Özbek, s. 258.

⁷¹ Taşkın, s. 63.

⁷² 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun “Milli İstihbarat Teşkilatının görevleri” başlıklı 4. maddesi:

“Milli İstihbarat Teşkilatının görevleri şunlardır;

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 Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak.

b) Devletin milli güvenlik siyasetiyle ilgili planların hazırlanması ve yürütülmesinde; Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamak.

c) Kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için Milli Güvenlik Kurulu ve Başbakana tekliflerde bulunmak.

d) Kamu kurum ve kuruluşlarının istihbarat ve istihbarata karşı koyma faaliyetlerine teknik konularda

arasında istihbarat toplama ve ilgili birimlere iletme de yer almaktadır. Buna dayanılarak belirli bir süre iletişimin önleyici amaçlı olarak denetlenmesi tedbirine başvurulmuştur.

2.3.1.6 4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu

Haberleşmenin denetlenmesi yoluyla delil elde edilmesi konusunda Türk hukuk sisteminde ilk açık düzenlemeye 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanununda⁷³ yer verilmiştir. Buna karşın adli ve önleyici amaçlı iletişimin denetlenmesi ayrımı yeterli ve açık şekilde belirtilmemiş olmasına karşın bir süre bu Kanunun 2'nci maddesine⁷⁴ dayanılarak önleme amaçlı iletişimin denetlenmesine başvurulmuştur.

2.3.2 Adli Amaçlı İletişimin Denetlenmesi

2.3.2.1 Genel Olarak

İletişim, kişilerin birbirleriyle ve toplumla ilişki kurma, haber düşünce ve konuları

müşavirlik yapmak ve koordinasyonun sağlanmasında yardımcı olmak.

e) Genelkurmay Başkanlığınca Silahlı Kuvvetler için lüzum görülecek haber ve istihbaratı, yapılacak protokole göre Genelkurmay Başkanlığına ulaştırmak.

f) Milli Güvenlik Kurulunda belirlenecek diğer görevleri yapmak.

g) İstihbarata karşı koymak.

Milli İstihbarat Teşkilatına bu görevler dışında görev verilemez ve bu teşkilat Devletin güvenliği ile ilgili istihbarat hizmetlerinden başka hizmet istikametlerine yöneltilemez. Milli İstihbarat Teşkilatı birimlerinin görev, yetki ve sorumlulukları Başbakanca onaylanacak bir yönetmelikte belirtilir.”

⁷³ Kabul tarihi: 30/07/1999, Yayımlandığı R.G. Tarih.: 01/08/1999, Sayı: 23773.

⁷⁴ 4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunun “İletişimin Dinlenmesi Veya Tespiti” Başlıklı 2. Maddesi:

“Bu Kanunda öngörülen suçları işleme veya bunlara iştirak yahut işlendikten sonra faillere her ne suretle olursa olsun yardım veya aracılık veya yataklık etme kuşkusuna altında bulunan kimselerin kullandıkları telefon, faks ve bilgisayar gibi kablolu, kablosuz veya diğer elektromanyetik sistemlerle veya tek yönlü sistemlerle alınan veya iletilen sinyalleri, yazıları, resimleri, görüntü veya sesleri ve diğer nitelikteki bilgileri dinlenebilir veya tespit edilebilir. Tespit edilenler mühürlenerek yetkililerce zapta bağlanır.

İletişimin dinlenmesine veya tespitine ilişkin kararlar, ancak kuvvetli belirtilerin varlığı halinde verilebilir. Başka bir tedbir ile failin belirlenmesi, ele geçirilmesi veya suç delillerinin elde edilmesi mümkün ise, iletişimin dinlenmesine veya tespitine karar verilemez.

Resmi veya özel her türlü iletişim kuruluşlarının tuttuıkları, iletişimin içeriği dışında kalan kayıtlar hakkında da yukarıdaki hükümler uygulanır.

Dinleme veya tespiti veya kayıtların incelenmesine hakim karar verir. Gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı da bu hususlarda yetkilidir. Hakim kararı olmaksızın yapılan bu gibi işlemlerin yirmidört saat içinde hakim kararına bağlanması şarttır. Sürenin dolması veya hakim tarafından aksine karar verilmesi halinde tedbir Cumhuriyet savcısı tarafından derhal kaldırılır.

Dinleme ve tespit kararları en çok üç ay için verilebilir, bu süre en çok iki defa üçer aydan fazla olmamak üzere uzatılabilir.

İletişimin dinlenmesi ve tespiti sırasında bu Kanunda öngörülen suçların işlendiğine ilişkin şüphe ortadan kalkarsa, tedbir Cumhuriyet savcısının tarafından kaldırılır. Bu gibi hallerde tedbir uygulaması sonucu elde edilen veriler, Cumhuriyet savcısının denetimi altında derhal ve nihayet on gün içinde yok edilir ve durum bir tutanakla belirlenir.

Cumhuriyet savcısı veya görevlendireceği kolluk mensubu, iletişim kurum ve kuruluşlarında görevli veya böyle bir hizmeti vermeye yetkili olanlardan, dinleme ve kayda alma işlemlerinin yapılmasını ve bu amaçla cihazların kurulmasını istediğinde, bu istem derhal yerine getirilir ve işlemin başladığı ve bitirildiği tarih ve saat bir tutanakla saptanır.”

öğrenme ve yayma işlemidir.⁷⁵

İletişimin denetlenmesi ise, araya bir vasıta sokulmak suretiyle her türlü haberleşmenin gizlice dinlenmesi, buradan elde edilen bilgilerin kaydedilmesi ve değerlendirilmesi olarak ifade edilmektedir.⁷⁶

Mevzuatımızda ise iletişimin denetlenmesi kavramı CMK'nın 135'inci maddesinde tespit etme, dinleme, kayda alma ve sinyal bilgilerini değerlendirilme olarak ifade edilmiştir. 14.01.2007 tarihli “Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin” 5'inci vd. maddelerinde de denetleme yerine tespit, dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesi ifadelerinin tümünün birlikte kullanıldığı görülmektedir.

Yukarıda yer verilen açıklamalardan da anlaşılacağı üzere kanun koyucu İletişimin denetlenmesin 4 türü olduğunu kabul etmektedir. Bunlar; iletişimin tespiti, iletişimin dinlenilmesi, iletişimin kaydedilmesi ve iletişimin sinyal bilgilerinin değerlendirilmesi işlemlerdir. Ayrıca bunlara ek olarak mobil telefonun yerinin tespiti işleminden de bahsedebiliriz.⁷⁷

2.3.2.2 İletişimin Tespiti

İletişimin tespiti, sanık veya şüphelinin telekomünikasyon yoluyla kimler ile iletişim kurduğunun belirlenmesi olarak tarif edilebilir. Diğer bir ifadeyle iletişimin tespitinde iletişimin içeriğinin öğrenilmesi değil belli bir telefon numarasından kimlerin, ne zaman, nereden arandığı, konuşmanın ne kadar süreyle yapıldığı, elektronik posta yoluyla kimlerle iletişim kurulduğu hususlarının belirlenmesidir.⁷⁸

Nitekim iletişimin tespiti 14.01.2007 tarihli Yönetmeliğin “Tanımlar” başlıklı 4'üncü maddesinin “f” bendinde *“İletişimin içeriğine müdahale etmeden, iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri”* olarak tanımlanmıştır.

İletişimin tespiti kavramı uygulamada HTS (Historical Traffic Search), geçmişe yönelik olarak telefon trafiğinin araştırılması olarak adlandırılmakta ve dinleme işleminin

⁷⁵ Aycı Emrullah, İletişim Özgürlüğü ve Özel Hayatın Gizliliği, Polis Dergisi, Yıl 11, Sayı 45, Temmuz-Ağustos-Eylül, 2005, s. 13.

⁷⁶ Kaymaz, s. 34 vd.

⁷⁷ Taşkın, s. 82.

⁷⁸ Kaymaz, s. 113.

aksine geçmişe yönelik telefon kayıtları bilgilerini içermektedir.⁷⁹

İletişimin tespitinin uygulanabilmesi açısından Kanun Koyucu CMK'nın 135'inci maddesinde sayılan katalog suçların söz konusu olmasını aramamaktadır. Dolayısıyla bu katalog suçlarla sınırlı olmaksızın her türlü suç için bu tedbire başvurulabilecektir.

CMK'nın 135'inci maddesinin altıncı fıkrasında *“Bu madde kapsamında dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümler ancak aşağıda sayılan suçlarla ilgili olarak uygulanabilir”* denildikten sonra katalog suçlar sayılmıştır. Maddede sayılan işlemler arasında iletişimin tespiti sayılmadığından, tespit işlemi için katalog suç şartı aranmayacaktır. Bu husus yerleşmiş Yargıtay kararlarınca da vurgulanmıştır.⁸⁰

2.3.2.3 İletişimin Dinlenmesi ve Kaydedilmesi

Telekomünikasyon yoluyla yapılan iletişimin dinlenmesi, her türlü haberleşmenin, araya bir vasıta sokulmak suretiyle gizlice dinlenmesi, iletişimin kaydedilmesi de buradan elde edilen bilgilerin kaydedilmesi ve değerlendirilmesi olarak tanımlanabilir.⁸¹ Telekomünikasyon araçları teknolojinin gelişmesiyle oldukça çeşitlenmesine rağmen CMK'da hangi iletişim araçları veya türlerinin iletişim kapsamına gireceği konusunda bir sınırlamaya gidilmemiştir. Bu durumda telefon, faks, bilgisayar, kablolu veya kablosuz araçların tamamı telekomünikasyon araçlarına örnek verilebilirse de teknolojinin gelişmesiyle birlikte bu örnekleri çoğaltmak mümkündür.⁸²

İletişimin dinlenmesi ve kayda alınması 14.01.2007 tarihli Yönetmeliğin *“Tanımlar”* başlıklı 4'üncü maddesinde *“Telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmaların dinlenmesi ve kayda alınması ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemler”* şeklinde tanımlanmıştır.

Bu dinleme işlemi sonucunda elde edilecek konuşmaların ispat aracı olarak kullanılabilmesi için kaydedilmesi gerekmektedir. Bu durum 14.01.2007 tarihli Yönetmelikte iletişimin dinlenmesinin, iletişimin kayda alınması suretiyle yapılacağı şeklinde ifade edilmiştir.

CMK'nın 135'inci maddesi gereğince iletişimin dinlenmesi ve kayda alınmasına

⁷⁹ Taşkın, s. 83.

⁸⁰ Yargıtay 5. Ceza Dairesi, 2005/14969 Esas, 2005/20489 Karar sayılı kararı (Karar için bkz. Taşkın, s. 84)

⁸¹ Taşkın, s. 84

⁸² Şen Ersan, Türk Hukuku'nda Telefon Dinleme-Gizli Soruşturmacı-X Muhabir, Seçkin Yayınevi, Ankara 2008, s. 47.

sadece katalog suçlar için başvurulabilecektir.

2.3.2.4 Sinyal Bilgilerinin Değerlendirilmesi

CMK'nın 135'inci maddesinin ilk halinde sinyal bilgilerinin değerlendirilmesi tedbiri yer almazken, 5353 sayılı Kanunla yapılan değişiklikle maddeye dahil edilmiştir.

Sinyal bilgileri, bir şebekede haberleşmenin iletimi veya faturalanması amacıyla işlenen her türlü veriyi ifade etmektedir. Sinyal bilgilerinin değerlendirilmesi ise, bu verilerden fatura, yazılım ve mekanik bilgilerin bir sanal havuza alınarak ikinci bir işleminden geçirildikten sonra farklı bir amaç için değerlendirilmesi ve işlenmesidir. Burada işlenmekten kastedilen iletişimin içeriğine müdahale değildir.⁸³

14.01.2007 tarihli Yönetmelikte sinyal bilgisinin, *“Bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi,”* ifade edeceği sinyal bilgilerinin değerlendirilmesi kavramının ise, *“İletişimin içeriğine müdahale niteliğinde olmayıp yetkili makamdan alınan karar kapsamında sinyal bilgilerinin iletişim sistemleri üzerinde bıraktığı izlerin tespit edilerek, bunlardan anlamlandırılan sonuçlar çıkarmak üzere gerçekleştirilen değerlendirme işlemlerini,”* ifade edeceği belirtilmiştir.

CMK'nın 135'inci maddesine göre sinyal bilgilerinin değerlendirilmesi tedbirine de sadece katalog suçlar açısından başvurulabilecektir.

2.3.2.5 Mobil Telefonun Yerinin Tespiti

İletişimin denetlenmesi işlemlerinden birisi de CMK 135'inci maddenin dördüncü fıkrasında düzenlenmiş olan mobil telefonun yerinin tespiti tedbidir. Bu tedbire delil elde edilmesi için değil, şüpheli veya sanığın yakalanması amacıyla başvurulmaktadır ve sadece yer tespiti yapılmaktadır.⁸⁴

CMK'nın 135'inci maddesinin dördüncü fıkrasının 5353 sayılı Kanunla değişik halinde artık şüpheliye ulaşmak için sadece şüphelinin ya da sanığın değil herhangi bir mobil telefonun yerinin tespiti yapılabilecektir.

Mobil telefonun yerinin tespiti tedbirine karar verilebilmesi için CMK'nın 135'inci maddesinde sayılan katalog suçlardan birisinin söz konusu olmasına gerek yoktur. Diğer bir ifadeyle bu tedbire her hangi bir suç bakımından şüpheli veya sanığın yakalanması

⁸³ Şahin Cumhuriyet, Ceza Muhakemesi Şerhi, Seçkin Yayınevi, Ankara 2006, s. 381; Şen, s. 47; Kaymaz, s. 125; Taşkın, s. 86.

⁸⁴ Kaymaz, s. 129.

amacıyla başvurulabilecektir.⁸⁵

2.3.2.6 İletişimin Denetlenmesinin Koşulları

Yukarıda iletişimin denetlenmesinden hangi tedbirlerin anlaşılması gerektiği ayrıntılı bir şekilde anlatılmıştı. Buradan da anlaşılacağı üzere, iletişimin denetlenmesi kapsamı içerisinde farklı hukuki statüye sahip tedbirler yer almaktadır. Bu tedbirlerden iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi tedbirleri kişi hak ve özgürlüklerine daha fazla müdahale ettiğinden uygulanması sıkı şekil şartlarına bağlanmıştır. Diğer taraftan bu tedbirlere göre daha az müdahale içeren tedbirler olan iletişimin tespiti, mobil telefonun yerinin tespitine karar verilmesinin koşulları ise diğer tedbirler kadar ağır değildir.

2.3.2.6.1 İletişimin Dinlenmesi, Kayda Alınması ve Sinyal Bilgilerinin Değerlendirilmesi Bakımından Koşullar

CMK'nın 135'inci maddesinin birinci fıkrasına göre; *“Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Cumhuriyet savcısı kararını derhâl hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir Cumhuriyet savcısı tarafından derhâl kaldırılır.”*

Ceza Muhakemesi Kanununda öngörülen telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, gizli soruşturmacı ve teknik araçlarla izleme tedbirlerine ilişkin talepte bulunulması, kararların alınması ve uygulanmasında uyulacak usul ve esasların belirlendiği 14.01.2007 tarihli Yönetmeliğin 5'inci maddesinin birinci fıkrasında ise, *“Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir; bu Yönetmeliğin 8 inci maddesinde belirtilen bir suç dolayısıyla yapılan soruşturma ve kovuşturmalarda da dinlenebilir, kayda alınabilir veya sinyal bilgileri değerlendirilebilir.”*

⁸⁵ Özbek, s. 424; Şahin, s. 379; Ünver Yener/Hakeri Hakan, Sorularla Ceza Muhakemesi Hukuku, Türkiye Barolar Birliği, Ankara 2006, s. 172; Taşkın, s. 88.

denilmektedir.

Bu yasal düzenlemelerden bu tedbirlerin belli kişilere, belli suçlar için, kuvvetli suç şüphesi olması halinde, başka yolla delil elde edilememesi durumunda belli mercilerin kararıyla, belirli sürelerle uygulanabileceği anlaşılmaktadır.

Aşağıda ayrıntılı bir şekilde açıklayacağımız koşullardan birisinin bulunmaması durumunda elde edilen delil “hukuka aykırı delil” niteliği taşıyacağından ceza muhakemesinde kullanılamayacak dolayısıyla hükme esas alınamayacaktır.⁸⁶

2.3.2.6.1.1 Tedbirin Uygulanacağı Kişi

Söz konusu tedbirlerin düzenlenmiş olduğu CMK’nın 135’inci maddesinin birinci fıkrasında “*şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir.*” denilmek suretiyle bu tedbirlerin sadece şüpheli veya sanık hakkında uygulanabileceği açıkça belirtilmiştir. Ancak şüpheli veya sanıkla görüşmeler yapan üçüncü kişilerin iletişimlerinin dolaylı olarak dinlenmesi ve kaydedilmesi söz konusu olabilir.⁸⁷

Bu tedbirlerin sadece şüpheli ve sanıklar için uygulanabileceği hükme bağlandığına göre, tedbirin uygulanacağı kişi hakkında ya bir soruşturma başlatılmış ya da kovuşturma başlamış bulunması gerekmektedir. Aksi halde ortada bir şüpheli veya sanık bulunmayacağından tedbirin uygulanması yoluna da gidilemeyecektir.⁸⁸

CMK’nın 135’inci maddesinin ilk halinde sanıklar hakkında iletişimin denetlenmesi tedbirine başvurulabileceğine dair açık bir hüküm yokken, 5353 sayılı kanunla yapılan değişiklikle 135’inci maddenin ikinci ve dördüncü fıkralarında geçen “*şüphelinin*” ibaresi, “*şüpheli veya sanığın*” şeklinde değiştirilmiş ve sanıklar hakkında da bu tedbirin uygulanabileceğine dair açık bir hükme yer verilmiştir.

CMK’nın 2’nci maddesinde soruşturma, Kanuna göre yetkili mercilerce suç şüphesinin öğrenilmesinden iddianamenin kabulüne kadar geçen evre, şüpheli de bu evrede suç şüphesi altında bulunan kişi şeklinde tanımlanmıştır. Aynı maddeye göre kovuşturma iddianamenin kabulüyle başlayıp, hükmün kesinleşmesine kadar geçen evreyi kapsar ve sanık da kovuşturmanın başlamasından itibaren hükmün kesinleşmesine kadar, suç şüphesi altında bulunan kişidir.

⁸⁶ Şen, s. 51

⁸⁷ Özbek, s. 425; Taşkın, s. 91; Aksi görüş için bkz. Şen, s. 53.

⁸⁸ Kunter/Yenisey/Nuhoğlu, s. 720; Sezer/İpek/Parlak, s. 114.

CMK’da iletişimin denetlenmesinden bahsedilmekle birlikte, tedbirin konuluş amacını gerçekleştirmesini de engelleyeceğinden şüpheli veya sanığın sadece kendisine ait olan araçlarla yaptıkları iletişimin denetlenmesi gibi bir sınırlamaya gidilmemiştir. Dolayısıyla iletişimin denetlenmesi tedbiri, şüpheli veya sanığın adına kayıtlı olan iletişim araçları ile adına kayıtlı olmamakla birlikte şüpheli veya sanığın kullandığı iletişim araçları için uygulanabilecektir.⁸⁹ Uygulamada da şüpheli ve sanıkların kendi adlarına kayıtlı olmayan birçok iletişim aracını kullandıkları da sıkça görülmektedir.

CMK’nın 135’nci maddesinde “*şüpheli veya sanığın*” ibaresi kullanıldıktan sonra tedbirin uygulanacağı kişiler hakkında başka bir sınırlamaya gidilmemiştir. Dolayısıyla maddeden şüpheli veya sanık olması durumunda milletvekillerinin iletişimlerinin denetlenip denetlenemeyeceğine dair bir sınırlama çıkarılamayacaktır. Bu konuda asıl düzenleme Anayasa’nın 83’üncü maddesinde yapılmıştır. Ancak madde iki farklı şekilde yorumlanmaktadır. İlk görüşe göre; Anayasa’nın 83’üncü maddesi uyarınca, milletvekilleri hakkında soruşturma veya kovuşturma yapılabilmesi için Türkiye Büyük Millet Meclisinin kararı gerekmektedir. Bir milletvekili hakkında suç isnadında bulunulması halinde Cumhuriyet savcısı soruşturma yapabilmek için, TBMM Başkanlığından söz konusu milletvekilinin dokunulmazlığının kaldırılmasını isteyecektir. TBMM’de aleni olarak yürütecek dokunulmazlığın kaldırılması süreci sonunda müspet karar alınması halinde soruşturma açılabileceği için dinleme de bu safhadan sonra yapılabilecektir. Bunun istinası Anayasa’nın 83’üncü maddesinde “*Ağır cezayı gerektiren suçüstü hali ve seçimden önce soruşturmasına başlanılmış olmak kaydıyla Anayasanın 14 üncü maddesindeki durumlar bu hükmün dışındadır.*” şeklinde belirtilmiştir.⁹⁰

İkinci görüşe göre; Anayasa’nın 83’üncü maddesinin ikinci fıkrasında, “*seçimden önce veya sonra bir suç işlediği ileri sürülen bir milletvekili, Meclis’in kararı olmadıkça tutulamaz, sorguya çekilemez, tutuklanamaz ve yargılanamaz*” denilmektedir. Buradan yola çıkılarak Meclis kararı olmadıkça milletvekillerinin tutuklanması sorguya çekilmesi ve yargılanması mümkün değilse de, milletvekilleri hakkında soruşturma yapılmasına ve bu arada delil elde edilmesi amacıyla milletvekilinin özgürlüğünü ve hareket yeteneğini kısıtlamayan koruma tedbirlerine başvurulmasına bir engel bulunmadığı sonucuna da

⁸⁹ “... Hakim tarafından iletişimin tespiti tedbiri, şüpheli veya sanık tarafından kullanılan telefonlar hakkında uygulanabilir.” Yargıtay 4. Ceza Dairesi, 29.11.2006 Tarih, 2006/4669 Esas, 2006/17007 Karar numaralı kararı (Karar için bkz. Şen, s. 54).

⁹⁰ Meran Necati, Adli ve Öneme Amaçlı İletişimin Denetlenmesi Gizli Soruşturmacı Teknik Takip, Adalet Yayınevi, Ankara 2009, s. 91.

ulaşılabilmektedir.⁹¹

Kamu görevlilerinin işlemiş olduğu görevleriyle ilgili suçların soruşturmasının başlatılabilmesi için bazı istisna suçlar haricinde 4483 sayılı Kanun veya diğer özel kanunlar gereğince önceden izin alınması gerekmektedir. Ancak, izin verilme sürecinde şüpheli, soruşturmadan ve isnat edilecek suçtan haberdar olacağı için, izin sisteminin uygulanacağı soruşturmalarda bu tedbirin delil elde etmeye elverişli olamayacağı açıktır.

CMK'nın 135'inci maddesinde, sadece şüpheli veya sanığın iletişiminin denetlenmesi öngörülmüştür. Kural olarak şüpheli veya sanık dışında üçüncü bir kişinin iletişimi denetlenemez. Ancak 14.01.2007 tarihli Yönetmeliğin 10'uncu maddesinin dördüncü fıkrasına göre, *“Bir soruşturma sırasında delil toplama kapsamında, somut olayın özelliğine göre maddi gerçekliğin araştırılması ve adil bir yargılamanın yapılabilmesi için zorunlu olduğu takdirde, açık rızasının bulunması ve iletişim aracının kendisine ait olması şartıyla şikâyetçinin iletişiminin tespiti Cumhuriyet savcısının yazılı kararıyla Başkanlıktan istenir.”*

Burada dikkat edilmelidir ki Yönetmelik rıza ile sadece iletişimin tespiti yapılabileceğini hükme bağlamaktadır. Dolayısıyla rıza olsa dahi dinleme, kayda alma ve sinyal bilgilerinin denetlenmesi yoluna gidilemeyeceğidir.

2.3.2.6.1.2 Tedbirin Uygulanacağı Suç

İletişimin denetlenmesi tedbirinin uygulanabileceği suçların belirlenmesinde, ülkelere göre farklı yaklaşımların benimsendiği görülmektedir. Ülkemizde iletişimin denetlenmesi tedbirinin uygulanmasında suçların sınırlandırılması yöntemi tercih edilmiş ve bu suçlar CMK'nın 135'inci maddesinin altıncı fıkrasında katalog halinde sayılmıştır. Bu suçların bütünü incelendiğinde çıkar amaçlı ya da örgütlü suç olmasının aranmadığı, bireysel olarak işlenen suçlarla ilgili olarak da gerektiğinde bu tedbirlere başvurulabileceğinin benimsendiği görülmektedir.⁹²

İletişimin dinlenmesi, kaydedilmesi ile sinyal bilgilerinin değerlendirilmesi tedbirine karar verilebilmesi için CMK'nın 135'inci maddesinin altıncı fıkrasında sayılan katalog suçlar şunlardır:

⁹¹ Öztürk/Erdem, s. 634; Kaymaz, 206; Saydam Mehmet, Ceza Muhakemesi Kanununa Göre Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Oniki Levha Yayıncılık, İstanbul Ocak 2011, s. 130

⁹² Özbek, s. 424; Taşkın, s. 100.

a) Türk Ceza Kanununda yer alan;

1. Göçmen kaçakçılığı ve insan ticareti (Madde 79, 80),
2. Kasten öldürme (Madde 81, 82, 83),
3. İşkence (Madde 94, 95),
4. Cinsel saldırı (birinci fıkra hariç, Madde 102),
5. Çocukların cinsel istismarı (Madde 103),
6. Uyuşturucu veya uyarıcı Madde imal ve ticareti (Madde 188),
7. Parada sahtecilik (Madde 197),
8. Suç işlemek amacıyla örgüt kurma (iki, yedi ve sekizinci fıkralar hariç, Madde 220),
9. Fuhuş (Madde 227, fıkra 3),
10. İhaleye fesat karıştırma (Madde 235),
11. Rüşvet (Madde 252),
12. Suçtan kaynaklanan malvarlığı değerlerini aklama (Madde 282),
13. Silahlı örgüt (Madde 314) veya bu örgütlere silah sağlama (Madde 315),
14. Devlet Sırlarına Karşı Suçlar ve Casusluk (Madde 328, 329, 330, 331, 333, 334, 335, 336, 337) suçları.

b) Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (Madde 12) suçları.

c) Bankalar Kanununun 22’nci maddesinin (3) ve (4) numaralı fıkralarında tanımlanan zimmet suçu,

d) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar.

e) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74’üncü maddelerinde tanımlanan suçlardır.

Yukarıda sayılan suçlar haricinde bir suçun söz konusu olması durumunda iletişimin denetlenmesi tedbiri uygulanamayacaktır. Bu suçlardan dolayı bir tedbirin uygulanmasına başlandıktan sonra suç vasfının değişerek katalog harici bir suç

dönüşmesi halinde de tedbire derhal son verilmesi gerekecektir.

Vasfı değişikliği sonunda, yeni suçun katalog dâhilinde bir suça dönüşmesi halinde dahi tedbire derhal son verilip, yeni suça göre iletişimin denetlenmesi koşullarının tekrar değerlendirilmesi gerekmektedir.⁹³

CMK’da teşebbüs aşamasında kalmış suçlar için de bu tedbirin uygulanıp uygulanamayacağı konusunda açık bir düzenlemeye gidilmemiş ise de teşebbüsün suçun özel görünüş şeklini oluşturduğundan bu tedbire teşebbüs aşamasında kalan suçlar bakımından da başvurulabilecektir.⁹⁴

CMK’nın 135’inci maddesinde sayılan katalog suçların birden fazla kişi tarafından iştirak halinde işlenmesi durumunda müşterek failler veya suça azmettirme veya yardım etme şeklinde iştirak eden şeriklerden her biri için iletişimin denetlenmesi tedbirinin uygulanması mümkündür.⁹⁵

2.3.2.6.1.3 Tedbirin Uygulanacağı Şüphe Derecesi

Şüphe, zihnin çeşitli alternatifler arasında seçme yapma konusunda tereddüt etmesi, hangi seçeneğin doğru olduğunu kestirememesi halidir.⁹⁶

Ceza muhakemesinde şüphe, “basit şüphe” ve “yoğun şüphe” olmak üzere ikiye ayrılır. Yoğun şüphe de kendi içinde “yeterli şüphe” ve “kuvvetli şüphe olmak üzere ikiye ayrılır. Basit şüphe, fiilin suç olduğu ve soruşturulabilir nitelik arz ettiği haldir. Yeterli şüphe, eldeki delillere göre yapılacak muhakeme sonunda sanığın mahkûm olması ihtimalinin beraat etme ihtimaline göre daha kuvvetli olması halidir. Kuvvetli şüphe ise, mevcut delillere göre yapılacak muhakeme sonunda mahkûm olma ihtimalinin kuvvetle muhtemel olması halidir.⁹⁷

CMK’nın 135’inci maddesinde iletişimin denetlenmesi kararı verilebilmesi için, katalog suçlardan birisinin işlendiğine ilişkin “kuvvetli şüphe sebepleri”nin varlığı zorunlu kılınmıştır.

⁹³ Ünver/Hakeri, s. 238; Taşkın, s. 104.

⁹⁴ Öztürk Bahri/Erdem Mustafa Ruhan, uygulamalı ceza muhakemesi hukuku, Seçkin Yayınevi, 11. Bası Ankara 2007, s. 608; Taşkın, s. 105; Kaymaz, s. 149.

⁹⁵ Kaymaz, s. 150.

⁹⁶ Develioğlu Ferit, Osmanlıca–Türkçe Ansiklopedik Lügat, 15. Baskı, Ankara 1998, s. 402; Öztürk/Erdem, s. 494.

⁹⁷ Öztürk/Erdem, s. 494; Taşkın, s. 108.

2.3.2.6.1.4 Başka Yolla Delil Elde Edilememesi (Son Çare)

CMK'nın 135'inci maddesine göre iletişimin denetlenmesi tedbirinin uygulanabilmesi için kişi hak ve özgürlüklerine daha az sınırlama getirecek başka tedbirlerle failin belirlenmesi veya suç delillerinin elde edilmesinin mümkün olmaması gerekmektedir. Aksi halde iletişimin denetlenmesine karar verilemeyecektir.⁹⁸

Başka suretle delil elde edilmesi imkânının bulunmaması hâli 14.01.2007 tarihli Yönetmelikte, *“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,”* şeklinde ifade edilmiştir.

Başka suretle delil elde edilemeyeceğinin deneyerek ispatlanmasına gerek yoktur. Bu tedbirlere başvurulsa dahi sonuç alınamayacağı konusunda bir beklentinin varlığı yeterlidir.⁹⁹

2.3.2.6.1.5 Talep ve Karar

Soruşturma aşamasında iletişimin denetlenmesi tedbirinin uygulanmasına Cumhuriyet savcısının istemi üzerine karar verilebilir. Kovuşturma aşamasında hâkim veya mahkeme gerek savcının talebi üzerine ve gerekse resen bu tedbire karar verebilir. Bu evrede iletişimin denetlenmesine karar verilebilmesi için Cumhuriyet savcısının talepte bulunması şart değildir.¹⁰⁰

CMK'nın 135'inci maddesine göre iletişimin denetlenmesi tedbirine kural olarak ancak hâkim kararıyla başvurulabilir. CMK'nın 162'nci maddesi gereğince bu kararı vermeye yetkili ve görevli hâkim, soruşturmanın yapıldığı yerdeki sulh ceza hâkimidir.¹⁰¹

Bu kararın yazılı verilmesi gerekmektedir.¹⁰²

Kural olarak iletişimin denetlenmesi kararını hâkim verecekse de gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı da iletişimin denetlenmesine karar verebilecektir. Gecikmesinde sakınca bulun halden ne anlaşılması gerektiği

⁹⁸ Kaymaz, s. 223.

⁹⁹ Taşkın, s. 113.

¹⁰⁰ Kovuşturma aşamasında bu tedbire karar verilemeyeceğine dair görüş için bkz. Taşkın, s. 105 vd.

¹⁰¹ CMK Madde 162- *“(1) Cumhuriyet savcısı, ancak hâkim tarafından yapılabilecek olan bir soruşturma işlemine gerek görürse, istemlerini bu işlemin yapılacağı yerin sulh ceza hâkimine bildirir. Sulh ceza hâkimi istenilen işlem hakkında, kanuna uygun olup olmadığını inceleyerek karar verir ve gereğini yerine getirir.”*

¹⁰² Kunter/Yenisey/Nuhoğlu, s. 711; Öztürk/Erdem, s. 607.

“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 Yönetmeliğin” 3’üncü maddesinde “*Gecikmesinde sakınca bulunan hâl: Derhal işlem yapılmadığı takdirde suçun iz, eser, emare ve delillerinin kaybolması veya şüphelinin kaçması veya kimliğinin saptanamaması olasılığının ortaya çıkması hâlini,*” şeklinde açıklanmıştır.

Cumhuriyet savcısının gecikmesinde sakınca bulunan hâlde vereceği iletişimin denetlenmesi kararlarının yazılı olması, gerekçeli olması ve gerekçede gecikmesinde sakınca bulunan halin varlığının somut olgularla açıklanması gerekmektedir.¹⁰³

CMK’nın 135’inci maddesinin birinci fıkrasına göre Cumhuriyet savcısının gecikmesinde sakınca bulunan hallerde verdiği iletişimin denetlenmesine ilişkin kararlar, değerlendirilmek üzere derhal hâkim onayına sunulacaktır.

Cumhuriyet Başsavcılığınca gönderilen talep yazısı hâkim tarafından saat belirtilerek havale yapılacaktır ve CMK’nın 135’inci maddesinin birinci fıkrasında belirtildiği üzere havale saatinden itibaren 24 saat içerisinde talep konusunda karar verilecektir.¹⁰⁴

Hakim tarafından Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde CMK’nın 135’inci maddesinin birinci fıkrasının son cümlesi gereğince tedbir Cumhuriyet savcısı tarafından derhâl kaldırılacaktır. Bu durumda yapılmış iletişimin denetlenmesi işlemleri mevcut olması durumunda bu kayıtlar savcı denetiminde en geç 10 gün içerisinde yok edilecektir.¹⁰⁵

2.3.2.6.1.6 Süre

İletişimin denetlenmesi kararı en çok üç ay için verilebilir ve bu süre, bir defalığına uzatılabilir. Ek süre, ilk kararda verilen tedbir süresinden fazla olamaz. Ancak, örgüt faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi halinde, hâkim bir aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir (CMK m. 135/3). Dolayısıyla diğer suçlarda tedbir en fazla 6 ay sürebilecekken, örgütlü suçlarda belli bir süre sınırı olmaksızın bu tedbire başvurulabilecektir.¹⁰⁶

¹⁰³ Şen, s. 64;

¹⁰⁴ Sezer/İpek/Parlak, s. 129.

¹⁰⁵ Şen, s. 67

¹⁰⁶ Şen, s. 73

Tedbire belirli bir süreyle karar verilmiş olması, bu sürenin sonuna kadar tedbirin uygulanabileceği anlamına gelmez. Henüz süre sona ermeden, tedbirin uygulanmasına ilişkin koşullardan birisi ortadan kalkmış ise, tedbirin uygulanmasına derhal son verilmesi gerekir.¹⁰⁷

2.3.2.6.1.7 İletişimin Denetlenmesi Tedbirine Son Verilmesi

İletişimin denetlenmesi tedbirine karar verilmesi temel hak ve özgürlüklere yaptığı müdahale nedeniyle sıkı şekil şartlarına bağlanmıştır. Bu şartların tedbire karar verildikten sonra ortadan kalkması durumunda tedbir kararına da son verilmesi gerekmektedir. Dolayısıyla katalog suçlar söz konusu olduğundan bahisle başlanan tedbire suçun katalog suçlardan olmadığına anlaşılmaması halinde derhal son verilmesi gerekmektedir.¹⁰⁸

İletişimin tespiti kararı belirli süre için verilebileceğinden dolayı bu sürenin sona ermesiyle birlikte tedbir de kendiliğinden sona ermiş olacaktır.

Soruşturma veya kovuşturma sırasında tedbire karar verilmesini gerektiren şüphenin ortadan kalkmasıyla da tedbire son verilmesi gerekmektedir. Şüpheli veya sanığın suç işlemediğinin anlaşılmaması durumunda artık tedbire devam edilmemesi gerekmektedir. Bununla beraber tedbirin devam ettiği sırada toplanan delillerden suçun işlendiği konusunda kesin kanaat getirilmesi durumunda da artık tedbire devam edilmemesi gerekmektedir.

Bununla beraber CMK'nın "Kararların Yerine Getirilmesi, İletişim İçeriklerinin Yok Edilmesi" başlıklı 137'nci maddesine göre iletişimin denetlenmesi tedbirine şu iki halde son verilecektir:

- Şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da
- 135'inci maddenin birinci fıkrasına göre hâkim onayının alınamaması halinde.

Yukarıda sayılan hallerde tedbire Cumhuriyet savcısı tarafından derhâl son verilecektir.

Bu durumda, denetleme tedbiri sonucunda elde edilen kayıtlar savcılık makamının denetimi altında en geç on gün içinde ortadan kaldırılarak, bu husus bir tutanakla kayıt altına alınacaktır (CMK m. 137/3). Bu şekilde tespit ve dinlemeye ilişkin kayıtların yok edilmesi halinde soruşturma evresinin bitiminden itibaren, en geç on beş gün içinde,

¹⁰⁷ Taşkın, s. 131.

¹⁰⁸ Kaymaz, s. 334.

Cumhuriyet Başsavcılığı tarafından tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgisine yazılı olarak bilgi verilecektir (CMK m. 137/4).

CMK'nın 137'nci maddesinde tedbire son verilecek iki durumdan bahsedilmesine rağmen tedbire son verme sadece bu iki nedenle sınırlı değildir. Tedbirin uygulanmasına devam edilmesini gereksiz kılacak bir durumun ortaya çıkması halinde de tedbire son verilecektir. Örneğin iletişimin denetlenmesi sırasında soruşturma konusu suçun maddede, sayılan katalog suçlardan olmadığına anlaşılmaması halinde tedbire derhal son verilmelidir.¹⁰⁹

Ayrıca ifade alma, arama, elkoyma ve benzeri klasik koruma tedbirleriyle delil elde edilmesi imkânının doğması durumunda, failin bulunduğu yer başka yollarla öğrenildiğinde, suç işleme şüphesi ortadan kalktığında veya iletişimin denetlenmesi yoluyla delil elde edilmesi imkânı kalmadığında tedbire derhal son verilmesi gerekir.¹¹⁰

Bununla birlikte, iletişimin denetlenmesi tedbirinin amacına ulaşması halinde de tedbirin uygulanmasına son verilmelidir.

Görüldüğü üzere Tedbirin uygulanmasına son verilmesi kararı kişi hak ve özgürlükleri bakımından lehe bir durum olduğundan, tedbire hâkim karar verdiği halde son vermek için hâkimden ayrıca bir karar alınması gerekmemektedir.¹¹¹ Bu konuda karar verme yetkisi savcılık makamına bırakılmıştır.¹¹²

2.3.2.6.2 İletişimin Tespiti Bakımından Koşullar

İletişimin tespiti, belli bir telefon numarasından kimlerin ne zaman arandığı, konuşmanın ne kadar süreyle yapıldığı, elektronik posta yoluyla kimlerle iletişim kurulduğu hususlarının belirlenmesidir. 14.01.2007 tarihli Yönetmelikte ise iletişimin tespiti, *“iletişimin içeriğine müdahale etmeden, iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri”* şeklinde tanımlanmıştır. İletişimin tespiti kavramı uygulamada HTS olarak adlandırılmakta ve geçmişe yönelik olarak telefon trafiği araştırılmaktadır.

Sadece abone ismi, abone adresi, abone kimlik bilgileri, abone sözleşmesi ve buna

¹⁰⁹ Şahin, s. 385; Taşkın, s. 151.

¹¹⁰ Şen, s. 81.

¹¹¹ Kunter/Yenisay/Nuhoğlu, s. 714.

¹¹² Şen, s. 81.

dair belgeler, telefon numarası, IMEI numara sorgusu ve eşleştirmesi, IP sorgusu bilgileri, sim kart bilgileri ve eşleştirilmesi, imsi bilgileri, PUK numarası bilgisi, kontör kartları bilgisi ve eşleştirilmesi, Roaming bilgisi, telefonun açık olup olmadığı bilgileri iletişimin tespiti kapsamında değildir. Bu bilgilere savcı CMK'nın 332'nci maddesindeki yetkileri kapsamında ulaşabilecektir.¹¹³

İletişimin tespiti, CMK'nın 135'inci maddesinde sayılan katalog suçlarla sınırlı olmaksızın her türlü suç için kullanılabilir.¹¹⁴ İletişimin denetlenmesinden farklı olarak bu tedbirle şüpheli ve sanık yanında şikâyetçinin de iletişiminin tespiti yapılabilir.

Tedbire başvurabilmek için iletişimin tespiti tedbirinde olduğu gibi kuvvetli şüphe sebebi ve başka yolla delil elde edilememesi gerekmektedir. Bununla beraber tedbire karar verecek merci de aynıdır.¹¹⁵

2.3.2.6.3 Mobil Telefonun Yerinin Tespiti Bakımından Koşullar

CMK'nın 135'inci maddesinde yer verilen iletişimin denetlenmesi işlemlerinden birisi de mobil telefonun yerinin tespit edilmesidir. Bu tedbire şüpheli ve sanık için başvurulabilmekle beraber bunlar dışında diğer kişilerin de mobil telefonlarının yeri tespit edilebilir.

Mobil telefonun yerinin tespitine ilişkin kararlar bakımından 135'inci maddedeki katalog suç sınırlaması bulunmamaktadır. Her türlü suçla ilgili mobil telefonun yerinin tespitine karar verilebilir.¹¹⁶

Mobil telefonun yerinin tespiti bakımından kuvvetli şüphe koşulu ve başka yollarla delil elde edilememesi koşulu aranmamaktadır.

Mobil telefonun yerinin tespitine kural olarak hâkim karar verebilir. Ancak gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı da bu tedbire karar verebilir.¹¹⁷

¹¹³ Taşkın, s. 137.

¹¹⁴ Şahin, s. 379.

¹¹⁵ Taşkın, s. 135 vd.

¹¹⁶ Şahin, s. 379.

¹¹⁷ Taşkın, s. 140; Öztürk/Erdem karar verme yetkisinin kural olarak hakim ve gecikmesinde sakınca bulunan hallerde cumhuriyet savcısı ile sınırlı tutulmasını yapılacak işlemin rutin bir işlem olması nedeniyle eleştirmektedir. Bkz. Öztürk/Erdem, s. 607.

CMK’nın 135’inci maddesinin dördüncü fıkrasına göre tespit işlemi en çok üç ay için yapılabilir ve bu süre, bir defa daha uzatılabilir. Madde de diğer tedbirlerde olduğu gibi örgüt faaliyeti çerçevesinde işlenen suçlarla ilgili olarak defalarca uzatma imkânı bu tedbirde tanınmamıştır.

2.3.2.7 İletişimin Denetlenmesi Yasası

CMK’nın 135’inci maddesinin yedinci fıkrasında “*Bu Maddede belirlenen esas ve usuller dışında hiç kimse, bir başkasının telekomünikasyon yoluyla iletişimini dinleyemez ve kayda alamaz.*” düzenlemesi yer almaktadır. Bu hükümle kanun koyucu Adli amaçlarla iletişimin dinlenmesi ve kayda alınmasında CMK’nın 135’inci vd. maddelerinde yer alan sıkı koşullara uyularak yapılabileceğini hükme bağlamıştır.

Bu genel yasak haricinde CMK iki kesim açısından daha yasak getirilmektedir. Bunlardan birincisi, tanıklıktan çekinme hakkı olanlar (CMK m. 135/2); ikincisi ise müdafii olarak atananlardır (CMK m. 136).

2.3.2.7.1 Müdafii ile Gerçekleştirilen İletişimin Denetlenmesine İlişkin Yasak

CMK’nın “Tanımlar” başlıklı 2’nci maddesinde müdafii “*Şüpheli veya sanığın ceza muhakemesinde savunmasını yapan avukatı*” olarak tarif edilmektedir. Şüpheli ya da sanığın savunmasının özgürce yapılabilmesi için, müdafilere bazı imtiyazlar tanınmıştır. CMK’nın 46’ncı maddesinde mesleki uğraşı nedeniyle öğrendiği bilgiler bakımından tanıklık yapmaktan çekinebileceği hükme bağlanmıştır. CMK’nın 126’ncı maddesinde 46’ncı madde kapsamında tanıklıktan çekinme hakkı olanlarla, şüpheli veya sanık arasındaki mektup ve belgelere elkonulamayacağı belirtilmiştir. CMK’nın 130’uncu maddesinde avukat bürolarında arama, elkoyma ve postada elkoyma bakımından bazı sınırlamalar getirilmiştir. CMK’nın 154’üncü maddesinde şüpheli veya sanığın vekâletname aranmaksızın müdafii ile her zaman ve konuşulanları başkalarının duyamayacağı bir ortamda görüşebileceği ve bu kişilerin müdafii ile yazışmalarının denetime tâbi tutulamayacağı hüküm altına alınmıştır.

Bu düzenlemelere paralel olarak CMK’nın 136’ncı maddesinde “*şüpheli veya sanığa yüklenen suç dolayısıyla müdafinin bürosu, konutu ve yerleşim yerindeki telekomünikasyon araçları hakkında, 135’inci madde hükmü uygulanamaz*” düzenlemesine gidilmiştir. Bu düzenleme ile avukatın bazı hallerde iletişimlerinin denetlenmesine ilişkin olarak bir yasak getirilmiştir. Ancak bu yasak sadece müdafiliğini yaptığı suçla sınırlıdır ve

sadece müdafinin bürosu, konutu ve işyerinde bulunan telekomünikasyon araçları bakımından geçerlidir.¹¹⁸

2.3.2.7.2 Tanıklıktan Çekinme Hakkı Sahipleri ile Gerçekleştirilen İletişimin Denetlenmesine İlişkin Yasak

CMK'nın 135'inci maddesinde tanıklıktan çekinme hakkı sahiplerinin de iletişimlerinin denetlenmesi konusunda bazı yasaklar getirmiştir. Maddeye göre *“Şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda alınamaz. Kayda alma gerçekleştirildikten sonra bu durumun anlaşılması hâlinde, alınan kayıtlar derhâl yok edilir.”* Bu düzenlemenin dayanağı, Anayasa'nın 38'inci maddesinin beşinci fıkrasında yer alan *“Hiç kimse kendisini ve kanunda gösterilen yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlanamaz.”* hükmüdür.¹¹⁹

Yakınlık dolayısıyla tanıklıktan çekinebilecek kişiler, CMK'nın 45'inci maddesinin birinci fıkrasında,

“Aşağıdaki kimseler tanıklıktan çekinebilir:

- a) Şüpheli veya sanığın nişanlısı.*
- b) Evlilik bağı kalmasa bile şüpheli veya sanığın eşi.*
- c) Şüpheli veya sanığın kan hısımlığından veya kayın hısımlığından üstsoy veya altsoyu.*
- d) Şüpheli veya sanığın üçüncü derece dahil kan veya ikinci derece dahil kayın hısımları.*
- e) Şüpheli veya sanıkla aralarında evlâtlık bağı bulunanlar.”*

şeklinde sayılmıştır.

Meslek ve sürekli uğraşları sebebiyle tanıklıktan çekinebilecek kişiler ise CMK'nın 46'ncı maddesinin birinci fıkrasında,

“(1) Meslekleri ve sürekli uğraşları sebebiyle tanıklıktan çekinebilecekler ile çekinme konu ve koşulları şunlardır:

- a) Avukatlar veya stajyerleri veya yardımcılarının, bu sıfatları dolayısıyla veya yükledikleri yargı görevi sebebiyle öğrendikleri bilgiler.*

¹¹⁸ Taşkın, s. 165.

¹¹⁹ Taşkın, s. 170.

b) Hekimler, diř hekimleri, eczacılar, ebeler ve bunların yardımcıları ve diğerk bütün tıp meslek veya sanatları mensuplarının, bu sıfatları dolayısıyla hastaları ve bunların yakınları hakkında öğrendikleri bilgiler.

c) Malf işlerde görevlendirilmiş müşavirler ve noterlerin bu sıfatları dolayısıyla hizmet verdikleri kişiler hakkında öğrendikleri bilgiler.”

şeklinde sayılmıştır.

Ancak aynı maddenin ikinci fıkrasında “Yukarıdaki fıkranın (a) bendinde belirtilenler dışında kalan kişiler, ilgilinin rızasının varlığı halinde, tanıklıktan çekinemez.” denilmek suretiyle sanık ya da şüphelinin onayıyla tanıklık yapmak zorunda olan kimseler sayılmıştır. Bu tür durumlarda, bu kimselerle sanığın konuşmaları dinlenebilecektir.¹²⁰

5187 sayılı Basın Kanununun 12’nci maddesinde ise, “Sürelı yayın sahibi, sorumlu müdür ve eser sahibi, bilgi ve belge dahil her türlü haber kaynaklarını açıklamaya ve bu konuda tanıklık yapmaya zorlanamaz.” düzenlemesine yer verilmiştir.

CMK’nın 135’inci maddesinin ikinci fıkrasına göre şüpheli veya sanık ile tanıklıktan çekinebilecek kişiler arasında kurulan iletişim kayda alınamayacaktır. Şayet tanıklıktan çekilme ilişkisi bilinemediğı için kayıt yapılmışsa bu kayıtlar derhal imha edilmelidir.¹²¹

İletişimin denetlenmesi tedbirinin uygulanması sırasında, şüpheli veya sanığın kullandığı belirlenen telefon, dinlemeye alınmakta ve yapılan konuşmalar kaydedilmektedir. Şüpheli veya sanık kiminle görüşürse görüşsün kayıt devam etmektedir. Şüpheli veya sanığın iletişim kurduğu kişilerin tanıklıktan çekinme hakkı olan kişiler olup olmadığı, bu aşamada belirlenememektedir. Bu nedenle yapılan kaydın, tanıklıktan çekinme hakkı sahipleri ile kurulan iletişime ait olduğunun sonradan anlaşılması halinde, bu kayıtların delil olarak kullanılmasının önlenmesi amacıyla imha edilme zorunluluğı getirilmiştir.¹²²

Ancak tanıklıktan çekinme hakkı olan kişilerin suç işleme şüphesi altında bulunmaları durumunda 135’inci maddede belirtilen yasal şartlar da varsa iletişimin denetlenmesi tedbirlerine başvurulabilecektir.

¹²⁰ Sezer/İpek/Parlak, s. 144.

¹²¹ Şen, s. 86.

¹²² Taşkın, s. 170.

2.3.2.8 Tesadüfen Elde Edilen Deliller

CMK'nın 138'inci maddesinin ikinci fıkrasında telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında tesadüfen elde edilen delillerin durumu düzenlenmiştir.

Maddeye göre, *“Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ve ancak, 135 inci Maddenin altıncı fıkrasında sayılan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir.”*

Aynı konu 14.01.2007 tarihli Yönetmeliğin 14'üncü maddesinde de *“Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ve ancak, bu Yönetmeliğin 8 inci maddesinde belirtilen suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilirse bu delil muhafaza altına alınır ve durum Cumhuriyet başsavcılığına derhâl bildirilir.”* şeklinde düzenlenmiştir.

Bu düzenlemelerden de anlaşılacağı üzere tesadüfen ele geçen delil, yapılan soruşturma ile ilgisi bulunmayan ve soruşturma yapılırken bir başka suçun işlendiğini gösteren ve soruşturma yapılırken ele geçirilen delillerdir.¹²³

— Şüpheli veya sanık hakkında uygulanan tedbire konu olan suçtan başka, ancak bir başka katalog suç işlediğine dair bilgiler elde edilirse, bu bilgiler de delil olarak kullanılabilir. Örneğin, uyuşturucu ticareti suçu ile ilgili şüpheli hakkında dinleme kararı alınmış ve yapılan dinlemede sırasında şüphelinin bir adam öldürdüğüne ilişkin bilgi ve bulgu elde edilmişse, bu kayıtlar Cumhuriyet savcısına verilecektir. Bu şekilde elde edilen tesadüfî bilgiler delil olarak kullanılabilir.¹²⁴

— Şüpheli veya sanık hakkında uygulanan tedbir sırasında üçüncü kişilerle ilgili elde edilen tesadüfî deliller, katalog suçlardan birine ait olmak kaydıyla delil olarak kullanılabilir. Bu durumda da yeni suçun soruşturmasına kendiliğinden başlanamaz ve dinlemeye aynı soruşturma üzerinden devam edilemez. Bu durumda yapılması gereken bu delilin muhafaza altına alınıp, durumun Cumhuriyet Savcılığına derhâl bildirilmesidir. Örneğin bir şüpheli uyuşturucu ticareti suçundan dinlemeye başlandığı sırada şüpheliyle telefonla görüşen üçüncü kişilerden birisinin de 135'inci maddede sayılan katalog

¹²³ Erdem, s. 107; Taşkın, s. 184.

¹²⁴ Taşkın, s. 187; bkz. Yargıtay Ceza Genel Kurulu, 2006/5.MD-154 Esas, 2007/145 Karar sayılı Kararı.

suçlardan insan ticareti suçunu işlediğine dair bilgi elde edilmesi durumunda bu kayıt muhafaza altına alınıp soruşturma başlatıp başlatmama kararını vermek üzere derhal Cumhuriyet Savcılığına bildirilecektir. Artık bu yeni suç için iletişimin denetlenmesi tedbirine başvurup vurmamak da açılması durumunda bu yeni soruşturmada değerlendirilecektir.

— İletişimin denetlenmesi sırasında katalog dışında kalan suçlardan birisine ilişkin delil elde edilmesi durumunda ise, CMK’nın “...135 inci Maddenin altıncı fıkrasında sayılan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilirse...” şeklindeki açık hükmü uyarınca, bu delillerin kullanılması mümkün değildir. Yargıtay Ceza Genel Kurulu da bir kararında katalog harici suçlarla ilgili olarak elde edilen delillerin kullanılamayacağı hükmüne bağlanmıştır.¹²⁵

2.3.2.9 Hukuka Aykırı İletişimin Denetlenmesi ve Yaptırımı

İletişimin denetlenmesinin koşulları CMK’nın 135’inci maddesinde ayrıntılı bir şekilde düzenlenmiştir. Bu maddenin son fıkrasında ise, “*Bu maddede belirlenen esas ve usuller dışında hiç kimse, bir başkasının telekomünikasyon yoluyla iletişimini dinleyemez ve kayda alamaz.*” hükmüne yer verilmiştir. Bu hüküm karşısında kamu görevlileri veya özel kişilerin kanuna aykırı olarak bir başkasının iletişimini denetlemesi kanuna aykırılık teşkil edecek ve aynı zamanda suç oluşturacaktır. Bu şekilde bir eylemin ne gibi yaptırımlarla karşılaşacağına aşağıda değinilecektir.

2.3.2.9.1 Ceza Yaptırımı

İletişimin denetlenmesine ilişkin olarak kanunlarda hükme bağlanan koşullara aykırı olarak bir kişinin iletişimin denetlenmesi halinde bu tarz eylemleri gerçekleştirenler TCK’nın 132, 133 ve 134’üncü maddeleri uyarınca cezalandırılacaktır. Ayrıca koşullarının bulunması halinde bu eylemler “Kişisel Verilerin Kaydedilmesi”, “Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme” veya “Verileri Yok Etmeme” suçlarını da oluşturabilecektir.

¹²⁵ Yargıtay Ceza Genel Kurulu, 2006/4.MD–122 Esas, 2006/162 Karar sayılı Kararı. Söz konusu olayda, hakim kararı ile çete kurma suçundan telefonu dinlenen bir kişinin, bir başka çete üyesi ile görüşmesi sırasında, bir hakimi arkadaşlarını tahliye edeceğine ilişkin bir konuşma geçmektedir. Telefon konuşmasında belirtildiği gibi sözü edilen kişi belirtilen tarihte tahliye edilmiştir. Ancak tahliye ile ilgili koşullar tam men kanunlara uygundur. Bu telefon konuşması üzerine tahliyeye karar veren hakim hakkında görevi köttüye kullanmak suçundan soruşturma açılmıştır. Ceza Genel Kurulu olayda tesadüfen elde edilen delil olduğunu, elde edilen delilin hakkında dinleme kararı verilmeyen bir kişiyle ilgili olduğu bu delilin katalog haricinde kalan bir suçla ilgili olduğu gerekçesiyle hukuka aykırı delil sayılarak buna göre işlem yapılamayacağına hükmetmiştir. (bkz. Taşkın, s. 190)

TCK'nın 132'nci maddesinde haberleşmenin gizliliğini ihlâl suçu düzenlenmektedir. Buna göre,

“(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. (Ek cümle: 2/7/2012–6352/79 md.) İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

TCK'nın 133'üncü maddesinde kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu düzenlenmektedir. Düzenlemeye göre,

“(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.

(3) (Değişik: 2/7/2012–6352/80 md.) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adli para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

TCK'nın 134'üncü maddesinde ise özel hayatın gizliliğini ihlâl suçu düzenlenmiştir. Bu düzenleme 132'nci ve 133'üncü maddelere girmeyen eylemleri de kapsamı içine alan torba bir düzenlemedir. Bu maddeye göre,

“(1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.

(2) (Değişik: 2/7/2012–6352/81 md.) Kişilerin özel hayatına ilişkin görüntü veya

sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”

Kanunda yazılı bulunan usule uymaksızın iletişimi denetleyen veya son verilmesi gerekirken son vermeyen kimseler, bu suçlar dolayısıyla cezalandırabileceklerdir. Üçüncü kişilerin de kişiler arasında gerçekleştirilen iletişimi bir şekilde kaydetmesi de TCK anlamında suç oluşturacaktır.¹²⁶

Ayrıca dinleme sırasında elde edilen verilerin kanuna göre imha edilmesi gereken durumlarda sürelerin geçmiş olmasına karşın bunların imha edilmemesi de TCK’nın 138’inci madde kapsamında suç oluşturacaktır. Söz konusu suç TCK’nın 18’inci maddesinde *“Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir.”* şeklinde düzenlenmiştir.

2.3.2.9.2 Hukuk Yaptırımı

CMK’nın 141 ila 144’üncü maddeleri arasında koruma tedbirlerinin uygulanması esnasında sanık veya şüphelinin maruz kalabileceği zararlara ilişkin olarak tazminat yükümlülüğü düzenlenmiştir. İletişimin denetlenmesi de bir koruma tedbiri olmasına rağmen tazminatı düzenleyen maddelerde bu tedbir nedeniyle uğranılan zararın tazmini düzenlenmemiştir.¹²⁷ Dolayısıyla bu tedbir için tazminat istenmesi CMK kapsamında mümkün değildir. Bu tedbirin uygulanması sebebiyle oluşacak zararlar ancak tazminat hukukunun genel hükümleri çerçevesinde mümkün olacaktır.

İletişimin denetlenmesi tedbirinin, uygulanan kişide manevi veya maddi bir zarar meydana getirmesi mümkündür. Bu durumda kanunda belirtilen koşullara aykırı olarak bir başkasının iletişimini denetleyen kişi hakkında ayrıca tazminat davası açılması ve uğranılan zararın giderilmesi istenebilecektir. Bu dava hukuk davası usulüne uygun olarak sulh veya asliye hukuk mahkemelerinde açılabilir. Tedbirin yasal koşullara uygun olarak gerçekleştirilmesi durumunda, kural olarak bu zararları tazmin yükümlülüğü ortaya çıkmayacaktır. Hakkında tedbir uygulanan kişi hakkında kovuşturmayla yer olmadığı veya beraat kararı verilmesi tek başına tedbirin hukuka aykırı şekilde uygulandığı sonucunu

¹²⁶ Taşkın, s. 202.

¹²⁷ Şen, s. 108; Ünver/Hakeri, s. 184.

doğurmaz.¹²⁸

2.3.2.9.3 Disiplin Yaptırımı

Kanunda belirtilen koşullara aykırı olarak bir başkasının iletişimini denetleyen kişinin kamu görevlisi olması durumunda bu kişi hakkında ayrıca disiplin soruşturması açılması ve disiplin yaptırımı uygulanması mümkündür. Bu durumda oluşan suçla ilgili olarak ceza soruşturması yapılması yanında buna doğrudan veya dolaylı olarak yol açan devlet memurları hakkında disiplin soruşturması yapılacak ve şartları oluşması durumunda da disiplin cezası verilebilecektir. Nitekim 657 sayılı Devlet Memurları Kanununun 131'inci maddesinde aynı olaydan dolayı ceza mahkemesinde memur hakkında kovuşturmaya başlanmış olmasının disiplin soruşturmasını geciktirmeyeceği, keza kişinin olay dolayısıyla mahkûm olup olmamasının disiplin cezası verilmesine engel olmayacağı açıkça düzenlenmiştir.¹²⁹

2.3.3 Önleme Amaçlı İletişimin Denetlenmesi

Dünya üzerinde gelişmiş ülkelere bakıldığında hemen hemen hepsinde, anayasal düzeni ve kamu güvenliğini etkileme potansiyeline sahip bazı ağır suçların işlenmesinin önlenmesi amacıyla kolluk kuvvetlerine önleme ya da istihbari amaçlı olarak iletişimin denetlenmesi yetkisi verildiği görülmektedir.¹³⁰

Önleme dinlemesi ile adli amaçlı dinleme birbirinden oldukça farklı kavramlardır. Önleme dinlemesinde, henüz ortada bir suçun işlendiği iddiası bulunmamakta olup, işlenebilme veya sonuçları ağır olabilecek nitelikteki suçlara geçiş yapılabilme ihtimalinin bulunması söz konusudur.¹³¹

Hukukumuzda önleme amaçlı iletişimin denetlenmesine dair 4422 sayılı Kanuna kadar herhangi bir düzenleme bulunmadığı görülmektedir. Dolayısıyla bu dönemde önleme amaçlı denetleme yasal dayanaktan yoksundu. 4422 sayılı Kanunla konu ilk kez açıkça düzenlenmiştir.¹³² Ancak 4422 sayılı Kanunda düzenlenen iletişimin denetlenmesi, aslında

¹²⁸ Taşkın, s. 202.

¹²⁹ Taşkın, s. 203.

¹³⁰ Yenisey, s. 118; Şen, s. 32.

¹³¹ Şen, s. 36.

¹³² Aksi görüş için bkz. Şen, s. 32, "Uygulamada 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu kapsamında istihbarat amaçlı iletişimin denetlenmesi yapılmaya çalışılmakla birlikte, 4422 sayılı Kanunun 2. maddesi adli maksatlı dinleme ve kayda almaya imkan tanıdığı halde, bu Kanunda önleme amaçlı dinleme ve kayda alma yönünde düzenleme öngörülmemiştir. Bu sebeple, 4422 sayılı Kanunun yürürlükte olduğu dönemde, varsa yapılan önleme amaçlı dinleme ve tespitler hukuka aykırıdır." (Şen, s. 32).

daha çok adli iletişimin denetlenmesi niteliğinde olmasına rağmen, düzenlemedeki esneklik nedeniyle, önleme amaçlı olarak da bu hükümlere dayanılarak iletişimin denetlenmesi tedbirleri uygulanabilmektedir.¹³³

CMK'nın yürürlüğe girmesi ile birlikte 4422 sayılı Kanun yürürlükten kaldırılmıştır. Adli amaçlı iletişimin denetlenmesi CMK kapsamında düzenlenmiştir. Bu durum önleme amaçlı denetleme bakımından yasal bir boşluk oluşmuştur. Bu boşluğun doldurulması amacıyla da 5397 sayılı Kanun yürürlüğe girmiş ve önleme amaçlı iletişimin denetlenmesi daha ayrıntılı olarak düzenlenmiştir.

5397 sayılı "Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun"¹³⁴ ile birlikte;

¹³³ Taşkın, s. 205.

¹³⁴ 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun:

"Madde 1 – 4.7.1934 tarihli ve 2559 sayılı Polis Vazife ve Selahiyet Kanununun ek 7 nci maddesine aşağıdaki fıkralar eklenmiştir.

Birinci fıkra da belirtilen görevlerin yerine getirilmesine yönelik olarak, 4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç, 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmidört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç yirmidört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.

Yetkili ve görevli hâkim, talepte bulunan kolluk biriminin bulunduğu yer itibarıyla yetkili olan ve 5271 sayılı Kanunun 250 nci maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemesinin üyesidir.

Kararda ve yazılı emirde, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tesbite imkân veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenler belirtilir. Kararlar, en fazla üç ay için verilebilir; bu süre aynı usulle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilir. Ancak, terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir.

Uygulanan tedbirin sona ermesi halinde, dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir. Durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.

İstihbarat faaliyetlerinde, bu maddede belirtilen suçların önlenmesi amacıyla ve hâkim kararı alınmak koşuluyla, teknik araçlarla izleme yapılabilir. Ayrıca, kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların ihtiyaç duyulan bilgi ve belgelerinden yararlanabilmek için gerekçesini de göstermek suretiyle yazılı talepte bulunulabilir. Bu kurum ve kuruluşların kanuni sebeplerle veya ticari sır gerekçesiyle bu bilgi ve belgeleri vermeleri halinde ancak hâkim kararı ile bu bilgi ve belgelerden yararlanılabilir.

Bu madde hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtlar, birinci fıkra da belirtilen amaçlar dışında kullanılamaz. Elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik ilkesi geçerlidir. Bu fıkra hükümlerine aykırı hareket edenler hakkında, görev sırasında veya görevden dolayı işlenmiş olsa bile Cumhuriyet savcılarınınca doğrudan soruşturma yapılır.

Hâkim kararları ve yazılı emirler, Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanlığı görevlilerince yerine getirilir. İşlemin başladığı ve bitirdiği tarih ve saat ile işlemi yapanın kimliği bir tutanakla saptanır.

Bu maddede yer alan faaliyetlerin denetimi, sıralı kurum amirleri, Emniyet Genel Müdürlüğü ve ilgili bakanlığın teftiş elemanları ve Başbakanın özel olarak yetkilendireceği kişi veya komisyon tarafından yapılır. Bu maddede belirtilen işlemler ile 5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak dinlemeler, Telekomünikasyon Kurumu bünyesinde, Kurum başkanına doğrudan bağlı "Telekomünikasyon İletişim Başkanlığı" adıyla kurulan tek bir merkezden yürütülür. Oluşturulan bu Başkanlık bir başkan ile teknik, hukuk ve idari olmak üzere üç uzmandan oluşur. Bu Başkanlıkta Millî İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığının ilgili birimlerinden birer temsilci bulundurulur. Verilen

görevleri yerine getirmek üzere yeteri kadar da personel istihdam edilir. Telekomünikasyon İletişim Başkanı, Telekomünikasyon Kurumu Başkanının teklifi üzerine Başbakan tarafından atanır. Telekomünikasyon İletişim Başkanı, Kurul üyelerinin sahip olduğu özlük haklarına sahiptir. Ulaştırma Bakanlığı bu merkezle ilgili alt yapıyı hazırlamakla yükümlüdür. Bu merkezin kuruluş giderleri Telekomünikasyon Kurumu gelirlerinden karşılanır. Bu merkezin kuruluşu ile ilgili her türlü mal ve hizmet alımları ile yapım işleri, ceza ve ihalelerden yasaklama işleri hariç 4734 sayılı Kamu İhale Kanunu ve 4735 sayılı Kamu İhale Sözleşmeleri Kanunu hükümlerinden muaftır.

Bu maddede belirlenen usul ve esaslara aykırı dinlemeler hukuken geçerli sayılmaz ve bu şekilde dinleme yapanlar hakkında 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu hükümlerine göre işlem yapılır.

Bu maddenin uygulanmasına ilişkin esas ve usuller Adalet, İçişleri ve Ulaştırma bakanlıklarının görüşü alınarak Başbakanlık tarafından üç ay içinde çıkarılacak yönetmelikle düzenlenir.

Madde 2 - 10.3.1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununa aşağıdaki ek madde eklenmiştir.

Ek Madde 5 - Jandarma, bu Kanunun 7 nci maddesinin (a) bendine ilişkin görevleri yerine getirmek için öncelikli ve koruyucu tedbirleri almak üzere, sadece kendi sorumluluk alanında 4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç, 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Jandarma Genel Komutanı veya istihbarat başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişimi tespit edebilir, dinleyebilir, sinyal bilgilerini değerlendirebilir, kayda alabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmidört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç yirmidört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir. Bu işlemler, 4.7.1934 tarihli ve 2559 sayılı Polis Vazife ve Selahiyyet Kanununun ek 7 nci maddesinin onuncu fıkrası hükmüne göre kurulan merkez tarafından yürütülür. 5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak dinlemeler de bu merkez üzerinden yapılır.

Yetkili ve görevli hâkim, talepte bulunan kolluk biriminin bulunduğu yer itibarıyla yetkili olan ve 5271 sayılı Kanunun 250 nci maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemesinin üyesidir.

Kararda ve yazılı emirde, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespitte imkân veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenler belirtilir. Kararlar, en fazla üç ay için verilebilir; bu süre aynı usulle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilir. Ancak, terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir.

Uygulanan tedbirin sona ermesi halinde, dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.

Bu maddede belirtilen suçların önlenmesi amacıyla ve hâkim kararı alınmak koşuluyla, teknik araçlarla izleme yapılabilir. Ayrıca, kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların ihtiyaç duyulan bilgi ve belgelerinden yararlanabilmek için gerekçesini de göstermek suretiyle yazılı talepte bulunulabilir. Bu kurum ve kuruluşların kanuni sebeplerle veya ticari sır gerekçesiyle bu bilgi ve belgeleri vermemekle ilgili olarak hâkim kararı ile bu bilgi ve belgelerden yararlanılabilir.

Bu madde hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtlar, birinci fıkrada belirtilen amaçlar dışında kullanılamaz. Elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik ilkesi geçerlidir. Bu fıkra hükümlerine aykırı hareket edenler hakkında, görev sırasında veya görevinden dolayı işlenmiş olsa bile Cumhuriyet savcılarınca doğrudan soruşturma yapılır.

Hâkim kararları ve yazılı emirler, Jandarma Genel Komutanlığı İstihbarat Başkanlığı görevlilerince yerine getirilir. İşlemin başladığı ve bitirildiği tarih ve saat ile işlemi yapanın kimliği bir tutanakla saptanır.

Bu maddede yer alan faaliyetlerin denetimi, sıralı kurum amirleri, Jandarma Genel Komutanlığı ve ilgili bakanlığın teftiş elemanları ve Başbakanın özel olarak yetkilendireceği kişi veya komisyon tarafından yapılır. Bu maddede belirlenen usul ve esaslara aykırı dinlemeler hukuken geçerli sayılmaz ve bu şekilde dinleme yapanlar hakkında 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu hükümlerine göre işlem yapılır.

Bu maddenin uygulanmasına ilişkin esas ve usuller, Adalet, İçişleri ve Ulaştırma bakanlıklarının görüşü alınarak Başbakanlık tarafından üç ay içinde çıkarılacak yönetmelikle düzenlenir.

Madde 3 - 1.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 6 ncı maddesinin birinci fıkrası aşağıdaki şekilde değiştirilmiş ve maddeye bu fıkradan sonra gelmek üzere aşağıdaki fıkralar eklenmiştir.

Millî İstihbarat Teşkilatı;

a) Bakanlıklar ve diğer kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların yöneticileri ve istihbarat hizmetlerinden sorumlu kişileri ile istihbaratın tevcihi, istihsalı ve istihbarata karşı koyma

2559 sayılı “Polis Vazife ve Salahiyet Kanunu”nun ek 7’nci maddesine fıkralar eklenerek, 2803 sayılı “Jandarma Teşkilatı Görev ve Yetkileri Kanunu”na ek 5’inci maddesi

konularında doğrudan ilişki kurabilir, uygun koordinasyon yöntemlerini uygulayabilir.

b) Bakanlıklar ve diğer kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından kendi görev sahasına giren konularda yararlanabilmek, bunlarla irtibat kurabilmek, bilgi ve belge almak için gerekçesini de göstermek suretiyle yazılı talepte bulunabilir.

Bu Kanunun 4 üncü maddesinde sayılan görevlerin yerine getirilmesi amacıyla Anayasanın 2 nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, hâkim kararı veya gecikmesinde sakınca bulunan hallerde MİT Müsteşarı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmidört saat içinde yetkili ve görevli hâkimin onayına sunulur. Hâkim, kararını en geç yirmidört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir. Bu işlemler, 4.7.1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyet Kanununun ek 7 nci maddesinin onuncu fıkrası hükmüne göre kurulan merkez tarafından yürütülür. 4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 135 inci maddesi kapsamında yapılacak dinlemeler de bu merkez üzerinden yapılır.

Yetkili ve görevli hâkim, talepte bulunan birimin bulunduğu yer itibarıyla yetkili olan ve 5271 sayılı Kanunun 250 nci maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemesinin üyesidir.

Kararda ve yazılı emirde, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespiti imkân veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenler belirtilir. Kararlar, en fazla üç ay için verilebilir; bu süre aynı usulle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilir. Ancak, terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir.

Uygulanan tedbirin sona ermesi halinde, dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.

Bu madde hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtlar, bu Kanunda belirtilen amaçlar dışında kullanılamaz. Elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik ilkesi geçerlidir. Bu madde hükümlerine aykırı hareket edenler hakkında, görev sırasında veya görevden dolayı işlenmiş olsa bile Cumhuriyet savcılarında doğrudan soruşturma yapılır.

Hâkim kararları ve yazılı emirler, MİT Müsteşarlığı görevlilerine yerine getirilir. İşlemin başladığı ve bitirildiği tarih ve saat ile işlemi yapanın kimliği bir tutanakla saptanır.

Bu maddede yer alan faaliyetlerin denetimi, sıralı kurum amirleri, Başbakanlık teftiş elemanları ve Başbakanlık özel olarak yetkilendireceği kişi veya komisyon tarafından yapılır.

Bu maddede belirlenen usul ve esaslara aykırı dinlemeler hukukun geçerli sayılmaz ve bu şekilde dinleme yapanlar hakkında 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu hükümlerine göre işlem yapılır.

Bu maddenin uygulanmasına ilişkin esas ve usuller Adalet, İçişleri ve Ulaştırma bakanlıkları ile MİT Müsteşarlığının görüşü alınmak suretiyle Başbakanlık tarafından üç ay içinde çıkarılacak yönetmelikle düzenlenir.

Geçici Madde 1- 2559 sayılı Kanunun ek 7 nci maddesinde düzenlenen merkez, en geç altı ay içinde kurulur. Merkez kuruluncaya kadar 2559 sayılı Kanunun ek 7 nci maddesi, 2803 sayılı Kanunun ek 5 inci maddesi ve 2937 sayılı Kanunun 6 ncı maddesi hükümleri uyarınca verilen iletişimin dinlenmesi, tespiti, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına dair karar veya yazılı emirler, telekomünikasyon hizmeti veren kurum ve kuruluşlar tarafından derhal yerine getirilir; ilgili istihbarat kurumlarının mevcut sistemlerinin kullanılmasına devam olunur.

Geçici Madde 2 - (Ek madde: 01/02/2006-5453 S.K./1.mad)

2559 sayılı Kanunun ek 7 nci maddesinde düzenlenen merkez, en geç altı ay içinde kurulur. Merkez kuruluncaya kadar 2559 sayılı Kanunun ek 7 nci maddesi, 2803 sayılı Kanunun ek 5 inci maddesi ve 2937 sayılı Kanunun 6 ncı maddesi hükümleri uyarınca verilen iletişimin dinlenmesi, tespiti, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına dair karar veya yazılı emirler, telekomünikasyon hizmeti veren kurum ve kuruluşlar tarafından derhal yerine getirilir; ilgili istihbarat kurumlarının mevcut sistemlerinin kullanılmasına devam olunur.

Madde 4 - Bu Kanun yayımı tarihinde yürürlüğe girer.

Madde 5 - Bu Kanun hükümlerini Bakanlar Kurulu yürütür.”

eklenerek ve 2937 sayılı “Devlet istihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu”nun 6’ncı maddesinin birinci fıkrası değiştirilip, maddeye bu fıkradan sonra gelmek üzere fıkralar eklenmek suretiyle önleme maksatlı dinleme, tespit ve kayda almaya ilişkin düzenlemeler getirilmiştir.

5397 sayılı Kanuna göre; Emniyet, Milli İstihbarat Teşkilatı ve Jandarma Teşkilatı kanundan doğan görevlerini yerine getirmeleri sürecinde bu kanunlarında belirtilen suçların önlenmesi amacıyla iletişimin denetlenmesi tedbirine başvurabileceklerdir¹³⁵.

5397 sayılı Kanunla getirilen düzenlemede dört tür iletişimin denetlenmesi işlemi sayılmaktadır. Bunlar iletişimin tespiti, iletişimin dinlenilmesi, iletişimin kaydedilmesi ve iletişimin sinyal bilgilerinin değerlendirilmesi işlemleridir.

Bununla birlikte Kanunda önleme amaçlı iletişimin denetlenmesi tedbirleri arasında mobil telefonun yerinin tespiti tedbirine yer verilmemiştir.

2.3.3.1 İletişimin Denetlenmesinin Koşulları

Yukarıda ayrıntılı bir şekilde değinilen adli amaçlı iletişimin denetlenmesinde, denetleme türlerine göre, zorunlu olan koşullarda bazı farklılıklar söz konusuydu. Bu nedenle de tedbirler arasında bir ayrıma gidilmişti. Önleme amaçlı iletişimin denetlenmesinde ise, denetleme türlerinin hepsi için aynı koşullar öngörülmüş olup istisnası bulunmamaktadır. Bu nedenle önleme amaçlı iletişimin denetlenmesi tedbirlerinin tümü için koşullar tek başlık altında değerlendirilecektir.

2.3.3.1.1 Tedbirin Uygulanacağı Kişi

Önleme amaçlı iletişimin denetlenmesinde ortada işlenmiş bir suç olmadığı için şüpheli veya sanık statüsünde kimse de bulunmamaktadır. Bu nedenle tedbir için kişi bakımından bir belirleme ya da sınırlama yoluna gidilmemiş, işlenmesinin önlenmesi amaçlanan suç bakımından bir kriter oluşturulmuştur. Dolayısıyla da kanunda sayılan suçların önlenmesi amacıyla teorik olarak herkesin iletişimi denetlenebilecektir.¹³⁶

Kanunda bir kişi sınırlaması bulunmadığına göre milletvekili, hâkim veya savcı, vali veya kaymakam, asker veya sivil sıfat veya görevi ne olursa olsun herkes hakkında bu tedbir uygulanabilecektir. Bu aşamada henüz bir soruşturma başlatılmadığından

¹³⁵ Centel Nur/Zafer Hamide, Ceza Muhakemesi Hukuku, 7. Baskı, İstanbul 2010, s. 397; Sezer/İpek/Parlak, s. 194.

¹³⁶ Taşkın, s. 214.

soruşturma izni prosedürü ile bu tedbirin uygulandığının idari amirlerce haberdar olunması da mümkün değildir.

2.3.3.1.2 Tedbirin Uygulanması Suretiyle İşlenmesinin Önlenmesi Amaçlanan Suç

Ülkemizde adli amaçlı denetlemede olduğu gibi önleme amaçlı iletişimin denetlenmesi tedbirinin uygulanması bakımından da önlenmesi amaçlanan suçların sınırlandırılması yöntemi tercih edilmiştir. Sadece belirli nitelikteki suçlarla ilgili olarak iletişimin denetlenmesi tedbirine başvurulabilecektir.¹³⁷

Buna göre polis önleme amaçlı iletişimin denetlenmesi tedbirine casusluk suçları haricindeki 3713 sayılı “Terörle Mücadele Kanunu”nun 10/h maddesinde sayılan suçların önlenmesi amacı ile başvurulabilecektir.

3.7.2005 tarih ve 5397 sayılı “Bazı kanunlarda Değişiklik Yapılmasına Dair Kanun”un 1’inci maddesinde: *“Birinci fıkrada belirtilen görevlerin yerine getirilmesine yönelik olarak, 4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç, 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla,”* bu tedbire başvurulabileceği hükmüne yer verilmiştir.

“Ceza Muhakemesi Kanunu”nun özel yetkili mahkemeleri düzenleyen 250, 251 ve 252’nci maddeleri 6352 sayılı “Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun”un 105’inci maddesiyle yürürlükten kaldırılmıştır. Bunun yerine TMK 10 ile yetkili mahkeme sistemi kurulmuştur. Bu nedenle de 6352 sayılı Kanunun geçici 2’nci maddesinin yedinci fıkrasında mevzuatta Ceza Muhakemesi Kanunu’nun 250’nci maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemelerine yapılmış olan atıfların “Terörle Mücadele Kanunu”nun 10’uncu maddesinin birinci fıkrasında belirtilen ağır ceza mahkemelerine yapılmış sayılacağı hükme bağlanmıştır.

Buna göre önleme amaçlı iletişimin denetlenmesi tedbirine başvurulabilecek suçlar 3713 sayılı “Terörle Mücadele Kanunu”nun 10/h maddesinde;

“Türk Ceza Kanununda yer alan;

a) Örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imâl ve ticareti

¹³⁷ Kunter/Yenisay/Nuhoğlu, s. 708,709.

suçu veya suçtan kaynaklanan malvarlığı değerini aklama suçu,

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

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

dolayısıyla açılan davalar,” şeklinde sayılmıştır.

5397 sayılı Kanunun 2’nci maddesinde jandarmanın önleyici amaçla iletişimin denetlenmesi yetkisi düzenlenmektedir. Burada ayrık bir duruma yer verilmediğinden polis yetkisi konusunda söylenenler jandarma için de geçerlidir.

Ancak jandarmanın yetki sınırlarından kaynaklanan önemli bir sınırlaması bulunmaktadır. 2803 sayılı “Jandarma Teşkilat, Görev ve Yetkileri Kanunu”nun 10’uncu maddesinde jandarmanın görev alanı “*Jandarmanın genel olarak görev ve sorumluluk alanı; Polis görev sahası dışı olup, bu alanlar il ve ilçe belediye hudutları haricinde kalan veya polis teşkilatı bulunmayan yerlerdir.*” şeklinde düzenlenmiştir. Buna göre jandarma, polisin görev sahası dışı ile polis teşkilatı bulunmayan yerlerde yukarıda sayılan suçların önlenmesi amacıyla iletişimin denetlenmesi tedbirini kullanabilecektir.

Milli istihbarat teşkilatı bakımından durum 5397 sayılı Kanunun 3’üncü maddesiyle “Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu”nun 6’ncı maddesine yeni fıkralar eklenmek suretiyle belirlenmiştir.

Buna göre “*Bu Kanunun 4 üncü maddesinde sayılan görevlerin yerine getirilmesi amacıyla Anayasanın 2 nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak*” iletişimin denetlenmesi tedbirine başvurulabilecektir. Bu düzenlemeye göre MİT bakımından önleyici amaçla iletişimin denetlenmesi kararı verilebilmesi için iki temel koşulun gerçekleşmesi gerekmektedir.

Bunlardan ilki; 2937 sayılı “Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu”nun 4’üncü maddesinde sayılan görevleri yerine getirmek amacının bulunmasıdır. Bu sayılan amaçların gerçekleştirilebilmesi için MİT koşullarına uygun ol-

mak kaydıyla bireylerin iletişimlerini denetleyebilecektir.¹³⁸

Söz konusu maddeye göre Milli İstihbarat Teşkilatının görevleri şunlardır;

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 Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak.

b) Devletin milli güvenlik siyasetiyle ilgili planların hazırlanması ve yürütülmesinde; Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamak.

c) Kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için Milli Güvenlik Kurulu ve Başbakana tekliflerde bulunmak.

d) Kamu kurum ve kuruluşlarının istihbarat ve istihbarata karşı koyma faaliyetlerine teknik konularda müşavirlik yapmak ve koordinasyonun sağlanmasında yardımcı olmak.

e) Genelkurmay Başkanlığınca Silahlı Kuvvetler için lüzum görülecek haber ve istihbaratı, yapılacak protokole göre Genelkurmay Başkanlığına ulaştırmak.

f) Milli Güvenlik Kurulunda belirlenecek diğer görevleri yapmak.

g) İstihbarata karşı koymak.

İkinci koşul ise, Anayasa'nın 2. maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde;

a) Devlet güvenliğinin, sağlanması,

b) Casusluk faaliyetlerinin ortaya çıkarılması,

c) Devlet sırrının ifşasının tespiti,

d) Terörist faaliyetlerin önlenmesi,

amacının gerçekleşmesidir.

Bu şekilde 5397 sayılı Kanunda yer alan suçların net olarak belirlenememesi ve

¹³⁸ Taşkın, s. 220.

sınırlarının çizilememesi, kanunların açıklığı öngörülebilirliği ilkesi bakımından önemli bir sorun oluşturmaktadır.¹³⁹

2.3.3.1.3 Tedbirin Uygulanacağı Evre ve Gerekli Olan Şüphe Derecesi

5397 sayılı Kanunla düzenlenen önleme amaçlı iletişimin denetlenmesi suçun işlenmesinden önceki aşamada uygulanabilecek bir tedbirdir. Bu tedbirin uygulanmasına karar verildiği sırada, henüz ortada işlenmiş bir suç bulunmamaktadır.

Suçun işlendiği andan daha önceki zaman dilimi içerisinde başvurulabileceği gibi kesin hükümden sonraki aşamada aynı kişinin yeni suçlar işlemesi söz konusu olabilecektse yeniden önleme amaçlı denetleme yoluna başvurulabilecektir. Diğer bir deyişle önleme amaçlı iletişimin denetlenmesi tedbirine sadece soruşturma ve kovuşturma evresinde değil bunun öncesinde ve sonrasında da başvurulabilir.

Kanunda önleme amaçlı iletişimin denetlenmesi kararı verilebilmesi için, işleneceği varsayılan ve önlenmesi amaçlanan suçla ilgili bir şüphe derecesinden söz edilmemiştir. Adli amaçlı iletişimin denetlenmesi ile önleme amaçlı iletişimin denetlenmesi müesseseleri bu noktada da birbirlerinden ayrılmaktadırlar.

5397 sayılı Kanun metninde şüphe kelimesine hiç yer verilmediğinden önleme amaçlı iletişimin denetlenmesi tedbirine karar verilebilmesi için istihbarat birimlerinin yaptıkları çalışmaları, elde ettikleri verileri, yaptıkları analizleri ve aldıkları ihbarları değerlendirmeleri ve bir tehlikenin meydana geleceğini hissetmeleri yeterli olacaktır.¹⁴⁰

2.3.3.1.4 Başka Yollarla Suç İşlenmesinin Önlenmesinin Mümkün Olması Halinde Dahi Tedbirin Uygulanabilmesi

Önleme amaçlı iletişimin denetlenmesinde adli amaçlı denetlemede olduğu gibi son çare olması zorunluluğu bulunmamaktadır.

Dolayısıyla söz konusu suçların işlenmesi başka yollarla önenebilecek olsa dahi, bu suçların işlenmesinin önlenmesi amacıyla iletişimin denetlenmesi yoluna gidilebilecektir.

Ancak burada “Orantılılık ilkesi”nin göz önünde bulundurularak, bireysel özgürlüklere daha az müdahale eden tedbirlerle sonuca gidilmesinin mümkün olması

¹³⁹ Taşkın, s. 221

¹⁴⁰ Taşkın, s. 223.

durumunda bunların tercih edilmesi daha yerinde olacaktır.

2.3.3.1.5 Talep ve Karar

Anayasa'nın “Haberleşme Hürriyeti” başlıklı 22'nci maddesinin ikinci fıkrası “*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; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakimın onayına sunulur. Hakim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.*” şeklinde düzenlenmiştir. Buna göre, haberleşme özgürlüğüne müdahale edebilmek için, mutlaka usulüne uygun olarak verilmiş bir hâkim kararı gerekmektedir.

5397 sayılı Kanunda da, önleme amaçlı olarak iletişimin denetlenmesi tedbirinden bahsedebilmek için mutlaka hâkim tarafından verilmiş bir karar bulunması gerektiği hükme bağlanmaktadır.

Ancak kanunda bu kuralın bir istisnasına da yer verilmektedir. Bu da gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri ile de haberleşme özgürlüğüne müdahale edilebileceği düzenlemesidir.

Yetkili mercilerin yazılı emri verebilmesi için öncelikle gecikmesinde sakınca bulunan hal söz konusu olması gerekmektedir.

Bu şartın gerçekleşmesi durumunda önleme amaçlı olarak iletişimin denetlenmesi tedbirine karar verebilecek yetkili idari merciler 5397 sayılı Kanunda şu şekilde sayılmaktadır:

- Polis bakımından Emniyet Genel Müdürü veya İstihbarat Daire Başkanı,
- Jandarma bakımından Jandarma Genel Komutanı veya İstihbarat Başkanı,
- MİT bakımından ise, MİT Müsteşarı veya Müsteşar Yardımcısıdır.

5397 sayılı Kanunda vali ve kaymakamlara bu yetki verilmediğinden söz konusu tedbire bu merciler karar veremeyeceklerdir.

Kanuna göre önleme amaçlı iletişimin denetlenmesine yönelik olarak emir verebilecek olan mercilerin bu emirleri yazılı olmak zorundadır.

Gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış idari merciin yazılı emri nihai bir karar değildir. 5397 sayılı Kanunda bu yazılı emrin 24 saat içinde yetkili ve görevli hâkim onayına sunulacağı hükme bağlanmıştır. Onaya sunma işlemi sonrasında hâkim, kararını en geç yirmi dört saat içinde verecektir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılacaktır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilip, durum bir tutanakla tespit olunacak ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilecektir.

Kararda ve yazılı emirde, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespiti imkân veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenlerin belirtilmesi gerekmektedir.

2.3.3.1.6 Süre

İletişimin önleyici amaçla denetlenmesine ilişkin kararlar, en fazla üç ay için verilebilir; bu süre aynı usulle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilir. Dolayısıyla hâkim aynı konu ile ilgili olarak en fazla üç kez uzatma kararı verebileceğinden aynı konuda aynı kişi için toplam en fazla 3 ay normal süre, 9 ay da uzatma süresi olmak üzere, toplam 12 ay için denetleme kararı verilebilmektedir.¹⁴¹

Ancak kanunda bu kurala iki istisna getirilmiştir. Bunlardan ilkinde göre; terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim her defasında üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilecektir. Dolayısıyla terör eylemlerinin önlenmesi amacıyla yapılacak denetlemelerde süre bakımından bir üst sınır bulunmamaktadır.

Bir diğer istisna da, MİT için casusluk suçları bakımından getirilmiştir. 5397 sayılı Kanununun ilk yürürlüğe girdiği tarihte olmayan bu istisna, 13.05.2007 tarih ve 5651 sayılı Kanun ile eklenmiştir. Buna göre casusluk faaliyetlerinin tespiti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim üç aydan fazla olmamak üzere sürenin müteaddit icralar uzatılmasına karar verebilecektir.

2.3.3.2 Elde Edilen Bilgilerin Niteliği ve Kullanılması

5397 sayılı Kanunda önleme amaçlı iletişimin denetlenmesi yetkisi verilen üç kurumla ilgili olarak da tedbirin uygulanma amaçları belirtilmiş ve elde edilen bilgilerin

¹⁴¹ Taşkın, s.235.

sadece bu amaçlarla kullanılması hükme bağlanmıştır. Buna göre polis bakımından bu bilgiler ancak “...Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayiş sağlamaya üzere...” ve CMK’nın 250’nci maddesinin 1. fıkrasının “a”, “b” ve “c” bentlerinde yazılı suçların islenmesinin önlenmesi amacıyla kullanılabilir.

Jandarma bakımından, 2803 sayılı Kanunun 7’nci maddesinin “a” bendinde belirtilen “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 korumalarını yapmak” ve CMK’nın 250’nci maddesinin birinci fıkrasının “a”, “b” ve “c” bentlerinde yazılı suçların işlenmesinin önlemek amacıyla kullanılabilir.

MİT bakımından ise, 2937 sayılı Kanunun 4’üncü maddesinde sayılan amaçlar için kullanılabilir.

5397 sayılı Kanunda her üç kurum için de “Bu madde hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtlar, birinci fıkrafta belirtilen amaçlar dışında kullanılamaz.” hükmüne yer verildiğinden elde edilen kayıtların belirlenen bu amaçlar dışında soruşturma veya kovuşturmada delil olarak kullanılması, Cumhuriyet savcısı tarafından bu bilgilere dayanarak kamu davası açılması, mahkemede bu bilgilere dayanarak mahkûmiyet hükmü kurulması mümkün değildir. Diğer bir ifadeyle bu tedbirin uygulanması suretiyle elde edilen bilgilerin delil niteliği bulunmamaktadır.¹⁴²

2.3.3.3 Keyfiliği Önleyici Güvenceler ve Hukuka Aykırılığın Yaptırımı

5397 sayılı Kanunda polis, jandarma ve MİT için geçerli olan “Bu maddede belirlenen usul ve esaslara aykırı dinlemeler hukuken geçerli sayılmaz ve bu şekilde dinleme yapanlar hakkında 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu hükümlerine göre işlem yapılır.” düzenlemesi yer almaktadır. Bu düzenleme gereğince iletişimin önleme amaçlı denetlenmesine ilişkin olarak 5397 sayılı Kanunda hükme bağlanan koşullara aykırı olarak bir kişinin iletişimin denetlenmesi halinde ilgililer, TCK hükümleri uyarınca cezalandırılacaktır.

Bu kişilerin fiilleri TCK’nın 132’nci maddesinde düzenlenmiş olan haberleşmenin gizliliğini ihlâl suçunu, TCK’nın 133’üncü maddesinde düzenlenmiş olan kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçunu, TCK’nın 134’üncü

¹⁴² Taşkın, s. 243.

maddesinde düzenlenmiş olan özel hayatın gizliliğini ihlâl suçunu oluşturabilecektir. Ayrıca sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmemeleri durumunda da TCK’nın 138’inci maddesinde düzenlenmiş olan “Verileri Yok Etmeme” suçu gündeme gelebilecektir.

Cezai yaptırımlar yanında bu hukuka aykırılıklar karşısında maddi veya manevi tazminat da talep edilebilecektir.

Kanunda belirtilen koşullara aykırı olarak bir başkasının iletişimini denetleyen görevli hakkında disiplin soruşturması açılması ve disiplin yaptırım uygulanması mümkündür.

ÜÇÜNCÜ BÖLÜM

İLETİŞİMİN DENETLENMESİ TEDBİRİNİN UYGULAMASI

3.1 İletişimin Denetlenmesi Tedbirinin Uygulaması

İletişimin denetlenmesi tedbirinin tatbiki sürecinde hâkim, Cumhuriyet savcısı, kolluk ve TİB görev almaktadır. Tedbirin uygulanmasına veya sonlandırılmasına hâkim ve Cumhuriyet savcısı tarafından karar verilir. Yapılan işlemler kolluk marifetiyle yapılır ve Cumhuriyet savcısının sorumluluğunda yürütülür. İletişimin denetlenmesi tedbirine ilişkin verilerin sağlanması gibi işlemler ise TİB üzerinden yürütülmektedir.

3.1.1 Kararı Yerine Getirecek Kişi ve Kurumlar

İletişimin denetlenmesine ilişkin kararın yerine getirilmesi CMK'nın 137'nci maddesinde hüküm altına alınmıştır. Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri Cumhuriyet savcılığı ve onun yardımcı organı olan kolluk tarafından yerine getirilmektedir.

5271 sayılı Ceza Muhakemesi Kanunu'nun 137'nci maddesinin birinci fıkrası uyarınca “Cumhuriyet savcısı veya görevlendireceği adli kolluk görevlisi telekomünikasyon hizmeti veren kurum ve kuruluşların yetkililerinden iletişimin tespiti, dinlenmesi veya kayda alınması işlemlerinin yapılmasını ve bu amaçla cihazların yerleştirilmesini yazılı olarak istediğinde bu istem derhal yerine getirilir” demektedir. Mülga 4422 sayılı ÇASÖMK'da bu kuruluşların kovuşturma organları ile iş birliğine gitmemesi durumunda bu kuruluşları iş birliğine zorlayıcı herhangi bir düzenlemeye yer verilmemiş iken CMK'nın 137'nci maddesi ile haberleşme hizmeti sunan kurumlar için bazı yükümlülükler getirilmiştir.

14.01.2007 tarihli Ceza Muhakemesi Kanunu'nda Öngörülen Telekomünikasyon Yolu ile Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirinin Uygulanmasına İlişkin Yönetmelik'in 11'inci maddesinde “işlem görevlileri” başlığı altında getirilen düzenleme ile Cumhuriyet savcısınca belirlenen adli kolluk görevlisi tarafından iletişimin dinlenmesi, kayda alınması, sinyal bilgilerinin değerlendirilmesi ve tespitiyle ilgili işlemlerin yerine getirilmesi amacıyla yeterli sayıda personel görevlendirileceği ve bu yönetmelik kapsamında yapılan işlemlerin ve yapıldığı yerlerin gizliliği, düzeni ve güvenliği ile kolluk görevlilerinin aidiyet numaralarının

belirlenmesine ve muhafazasına ilişkin esas ve usuller ile ilgili kolluğun merkez birimlerince düzenleneceği belirtilmiştir. Söz konusu bu düzenlemede bahsedilen adli kolluk görevlileri Emniyet, Jandarma ve MİT birimleridir. Emniyet Teşkilatında adli amaçlı iletişimin denetlenmesi tedbirini uygulayan birimler Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, Terörle Mücadele Daire Başkanlığı ve Siber Suçlarla Mücadele Daire Başkanlığıdır.

Önleme amaçlı iletişimin denetlenmesi işlemi, 2559 sayılı Polis Vazife ve Salahiyet Kanunu ek 7’nci maddesi, 2803 sayılı Jandarma Teşkilat Görev ve Yetkileri Kanunun ek 5’inci maddesi ve 2937 sayılı Millî İstihbarat Teşkilatı Kanunu 6’ncı maddesi çerçevesinde Emniyet, Jandarma ve MİT tarafından gerçekleştirilir.

14.01.2007 tarihli “Ceza Muhakemesi Kanunu’nda Öngörülen Telekomünikasyon Yolu ile Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirinin Uygulanmasına İlişkin Yönetmelik’in 9/2-a maddesine göre; iletişimin denetlenmesi tedbirini içeren karar Cumhuriyet savcısı tarafından ilgili adli kolluk birimine verildikten sonra, kolluk birimi bu karar doğrultusunda işlemleri yapacak kolluk personelinin aidiyet numarasını TİB’e bildirilir. Bu işlemten sonra bu kararla ilgili işlemler bildirilen aidiyet numarasına sahip personel tarafından yerine getirilir.

Söz konusu Yönetmelik’in 4/a maddesine göre; Aidiyet numarası: İletişimin denetlenmesi tedbirinin uygulanması işlemlerini yapmak üzere görevlendirilen adli kolluk personeline kimliğinin belirlenmesini sağlamak amacıyla sicil numaralarından farklı olarak kurumlarınca verilen numaradır. Yönetmelik’in 9/2-c maddesine göre, karar olmadan ve aidiyet numarası bildirilmeden TİB tarafından işlem başlatılmaz.

Yönetmelik’in 9/5 maddesine göre, iletişimin denetlenmesi işlemi denetleme tedbirine konu kararda belirtilen süre dolmadan önce sonlandırıldığında bu durum Cumhuriyet savcısı tarafından derhal TİB’e bildirilir. TİB’in kanuna aykırı kararlara karşı itiraz hakkı vardır.

3.1.2 Kararın Yerine Getirilmesi

TİB kurulmadan önce Cumhuriyet savcısı, kendi verdiği denetleme emrini veya hâkimin verdiği denetleme kararını özetleyerek, imzalayıp mühürler ve telekomünikasyon hizmeti veren kurumun adliye ile bağlantıyı kuran görevlisine gönderirdi. Bu yazıda,

CMK'nın 137'nci maddesinin birinci fıkrasına göre, iletişimin tespiti, dinlenmesi veya kayda alınması işlemlerinin yapılması için gerekli cihazların kurulması istenirdi.

TİB kurulduktan sonra 2005 tarihli Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmeliğin 14'üncü maddesinde 2009 yılında yapılan değişiklik ile birlikte kararların yerine getirilmesi şu şekilde anlatılmıştır;

"İletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi ile salt mobil telefonun yerinin tespitine ilişkin kararlar ve kararların içeriği, Cumhuriyet savcısınca işlemleri yerine getirmek üzere görevlendirilen kolluk görevlilerinin aidiyet numarası ile birlikte, Başkanlığın belirleyeceği şekilde elektronik ortamda ilgili kurumlar tarafından Başkanlığa gönderilir. İletişimin tespiti kararları ise, fiziki ortamda veya Başkanlığın belirleyeceği şekilde elektronik ortamda gönderilebilir. Kararlar ilgili kurum görevlileri ve Başkanlık tarafından yerine getirilir." Görüldüğü gibi, Yönetmelikte yapılan bu değişiklik neticesinde Cumhuriyet savcısının acele hallerde, önce sözle veya telefonla da emir vererek, yazılı karar veya emiri sonradan gönderilebilmesinin yolu kapatılmıştır.¹⁴³

İletişimin denetlenmesi tedbiri kapsamında elde edilecek deliller Cumhuriyet savcılığı veya adli kolluk görevlisi tarafından çözümü yapılarak metin haline getirilmektedir. Yabancı dildeki kayıtlar bir tercüman vasıtasıyla Türkçeye çevrilmektedir. Karşılaştırmalı hukukta kayıtların tutanağa aktarılması aşamasında ekleme ve çıkarma yapılması veya konuşmanın anlaşılmayan yerlerinin atlanması bakımından ortaya çıkabilecek anlam sapmalarının önüne geçebilmek için tedbirin ön denetimini yapmaya yetkili bağımsız bir hâkimlik kurumuna yer verilmesi gerekliliğinden söz edilmekte; öyle ki bazı ülkelerde elde edilen bilgileri inceleme yetkisi bulunan ancak hakkında tedbir uygulanan kişiye karşı susma yükümlülüğü altında olan ve ilgilinin haklarını gözetmekle görevli bir müdafilik kurumu meydana getirilmiştir.¹⁴⁴

¹⁴³ Yenisey Feridun, Nuhoglu Ayşe, "Global Hukuk Eğitim Programları (IGUL) Seminer Notları 2009-2010 Seminer Notları", İstanbul: Bahçeşehir Üniversitesi Hukuk Fakültesi IGUL Brimi, s. 71

¹⁴⁴ Turgutalp Mehmet Ali, "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi (5271 sayılı CMK'nın 135'inci maddesi)", Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Yüksek Lisans Programı, Yayınlanmamış Yüksek Lisans Tezi, Konya, 2011, s. 79

Raporumuzda uygulamada yer alan kolluk birimleri olan Emniyet, Jandarma ve MİT kurumları ayrı ayrı başlıklar halinde adli ve önleme amaçlı iletişimin denetlenmesi tedbiri bakımından ele alınacaktır.

Kurumlarımızı incelemeden önce “İletişimin Denetlenmesi” tedbirinin hangi tedbirleri içerdiğini anlamak için aşağıdaki tabloyu incelemekte fayda vardır.

Tablo 6- Adli Amaçlı İletişimin Denetlenmesi Türleri

	Amaç	Tedbirin Uygulanabileceği Suçlar	Tedbirin Uygulanabileceği Kişiler	Karar Mercii
İletişimin Dinlenmesi	Delil Elde Etmek	Katalog Suçlar	Şüpheli/Sanık	Hâkim veya Gecikmesinde Sakınca Bulunan hallerde Cumhuriyet Savcısı
Kayda Alınması	Delil Elde Etmek	Katalog Suçlar	Şüpheli/Sanık	Hâkim veya Gecikmesinde Sakınca Bulunan hallerde Cumhuriyet Savcısı
Sinyal Bilgilerinin Değerlendirilmesi	Delil Elde Etmek	Katalog Suçlar	Şüpheli/Sanık	Hâkim veya Gecikmesinde Sakınca Bulunan hallerde Cumhuriyet Savcısı
İletişimin Tespiti	Delil Elde Etmek	Tüm Suçlar	Şüpheli Sanık veya Müşteki (rızası halinde)	Cumhuriyet savcısı kararı ve hâkim onayı gerektirir. Ancak mağdur veya müştekinin rızası durumunda savcı kararı yeterlidir, hâkim onayı gerektirmez.
Mobil Telefonun Yerinin Tespiti	Şüpheli veya Sanığın Yakalanması	Tüm Suçlar	Şüpheli, Sanık, İlgili üçüncü Şahıs	Hâkim veya Gecikmesinde Sakınca Bulunan hallerde Cumhuriyet Savcısı (daha sonra Hâkim onayına ihtiyaç duyulmaz).

3.2 Emniyet Teşkilatı

İletişimin denetlenmesi tedbiri adli ve amaçlı iletişimin denetlenmesi tedbiri olarak ayrı ayrı anlatılacaktır.

3.2.1 Adli Amaçlı İletişimin Denetlenmesi

3.2.1.1 Uygulamada Dikkat Edilmesi Gerekenler

3.2.1.1.1 Gizlilik

İletişim denetlenmesi tedbiri gizlilik içerisinde yürütülür.¹⁴⁵ Aksi takdirde uygulanacak tedbirden soruşturma veya kovuşturma aşamasında etkili bir sonuç almak mümkün olmayacaktır.

İletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi ile ilgili alınan kararlar, yerine getirilmek üzere soruşturma ve kovuşturmanın yürütüldüğü yer dikkate alınarak Cumhuriyet savcısınca ilgili kolluk birimine gönderilir. Kolluk birimi, bu tedbirlere ilişkin karar ve işlemi yapmakla görevlendirilen kolluk personelinin aidiyet numarasını TİB’e bildirir ve işlemler aidiyet numaralı personel tarafından yerine getirilir.

Aidiyet numarası, iletişimin denetlenmesi tedbirlerinin uygulanması işlemlerini yapmak üzere görevlendirilen kolluk personeline kimliğinin belirlenmesini sağlamak amacıyla sicil numaralarından farklı olarak kurumlarınca verilen numaralardır.

Tedbirin uygulanması aşamasında gizlilik gereği ilgili birim dışındaki diğer birim amirlerinin ve hatta müdürlerinin dahi bilgilendirilmemesi gerekir.¹⁴⁶

3.2.1.1.2 İletişimin Denetlenmesi Kararı Alınması

İletişimin denetlenmesi tedbirine hâkim tarafından karar verilir, ancak gecikmesinde sakınca bulunan durumlarda Cumhuriyet Savcısı tarafından da karar verilebilir. Denetlenme tedbiri uygulanmasını bu makamlar şahsen isteyerek karar verebilecekleri gibi kolluktan gelen talep üzerine de karar alabilirler. İletişimin denetlenmesi kararı alınması talebini soruşturmayı yürüten ilin KOM, Asayiş veya Terör

¹⁴⁵ CMK m. 135/5.

¹⁴⁶ Ünver/ Hakeri, s.217.

Şubesinin ilgili bürosu tarafından ilgili savcılıktan veya mahkemeden talep edilir. Talepte tedbir kararından bulundurulması gereken hususlara dikkat edilir.

3.2.1.1.3 Kararın Merkez Birimlerine İletilmesi

İl birimlerince iletişimin denetlenmesine ilişkin alınan savcılık talimatları veya mahkeme kararları, Merkez Birimlerine iletilir. Alınan tedbir kararları Merkez Birimlerindeki Teknik Takip ve İzleme Şube Müdürlüğü görevlilerince TİB tarafından istenen formata uygun olarak sisteme girilir.

3.2.1.1.4 Tedbir Kararının TİB’e İletilmesi

İletişimin denetlenmesi tedbiri kararı alındıktan sonra, karar ve içeriği, görevlendirilen kolluk görevlisinin aidiyet numarasıyla birlikte elektronik ortamda TİB’e iletilir. Karar olmadan ve aidiyet numarası bildirilmeden TİB tarafından işlem başlatılmaz. Gecikmesinde sakınca bulunan hal durumunda Cumhuriyet savcısı tarafından alınan kararın yanı sıra daha sonra alınan hakim onayı da TİB’e iletilir. Karar TİB Hukuk Dairesi tarafından şekli açıdan incelenir.

TİB Hukuk Dairesi tarafından yapılan inceleme neticesinde karar TİB Teknik Dairesine iletilir. Kararların TİB tarafından Millî İstihbarat Teşkilatı Müsteşarlığına, Emniyet Genel Müdürlüğüne ve Jandarma Genel Komutanlığına aktarılması sağlanır.

Hem alınan karar, hem de yapılan işlemler tedbir uygulandığı sürece gizli tutulur. Karar verilirken hâkim tarafından gizlice verilir, tedbirin uygulanması sırasında da gizliliğe riayet edilir. Özellikle emniyet amirlerinin veya diğer kimselerin tedbire ilişkin olarak bilgilendirilmemesi gerekir. Bu noktada tek yetkili kimse hâkim veya savcıdır. Aksi takdirde TCK’nın 132 (haberleşmenin gizliliğini ihlal), 258 (göreve ilişkin sırrın açıklanması) veya 285’inci (gizliliğin ihlali) maddelerinden sorumluluk söz konusu olabilecektir.

Tablo 7- Adli Amaçlı İletişimin Denetlenmesinin Uygulanması Aşamaları

SUÇ ŞÜPHESİNİN TESPİTİ

Cumhuriyet Savcısının Soruşturma İznini Vermesi

Kuvvetli Şüphe Sebepleri Bulunması

Başka Suretle Delil Elde Edilememesi

Güvenlik Güçlerinin Tedbir Talebinde Bulunması

Savcı veya Hâkimin İletişimin Dinlenmesi veya Tespiti Kararı

Kararın Kolluğa Yazılı Olarak Tebliği

Kararın TİB'e Gönderilmesi ve Teknik Bağlantının Sağlanması

Dinleme ve Tespit İşlemi

Suçun İşlendiğine İlişkin Şüphenin Devamı

Suç İçeren Konuşmaları Çözümü veya Başka bir Veri Taşıyıcısına Aktarılması veya Her İki İşlemin Birlikte Yapılması

Davanın Açılması

Suçla İlişkin Bilgi İçeren Kayıtların C. Savcılığına Gönderilmesi

Yargılama

Süre Başlar ve Kesintisiz Devam Eder

İşlemin Başladığı ve Bittiği Saat Tutanakla Tespit Edilir.

Kolluk Tarafından Gizlilik Kurallarına Uygun Hazırlanmış Kayıt Odalarında, Kayda Alma Suretiyle Gerçekleştirilir. Kesintisiz Devam Edilir

Şüphenin Ortadan Kalkması

C. Savcısı Tarafından İşleme Son Verilmesi

Tüm Bilgilerin 10 Gün İçinde İmhası

Mahkûmiyet /Beraat

3.2.1.1.5 Verilerin Tutanağa Bağlanması

İletişimin denetlenmesine ilişkin her bir işlem tutanağa bağlanır.¹⁴⁷ Görevi yerine getirecek kolluk personeli tarafından hazırlanacak tutanakta işlemin başladığı ve bitirildiği tarih ve saat ile işlemi yapanın kimliği muhakkak yazılması gerekmektedir.

Tablo 8- Tutanak Örneği

İLETİŞİMİN DİNLENMESİ VE KAYDA ALINMASINA İLİŞKİN TUTANAK	
.....Mahkemesi hakimi/savcısı tarafından verilentarihli vesoruşturma sayılı iletişimin tespiti, dinlenmesi ve kayda alınması kararının uygulanması sonucunda adlı kişiye ait adlı kişinin kullandığı numaralı/ iletişim aracının tarihleri arasında yapılan dinlenmesi esnasında aşağıdaki konuşma/konuşmalar tespit edilmiştir.	
Kayıt Sıra No(*)	:
Tarih saat ve süre	:
Arayan ve Aranan İletişim Aracının Numaraları	:
Arayan ve Aranan Kişiler	:
Konuşma Dili/Lehçesi	:
Konuşmanın İçeriği	:
Bu iletişimin dinlenmesi sırasındadillerindeki konuşmalartarafından tercüme edilmiştir.	
Bu Tutanaktarihinde saat.....'da tanzim edilmiş ve tarafımızdan imzalanmıştır.	

Tutulan kayıtlar Savcı tarafından veya Savcılıkça görevlendirilen adli kolluk görevlisi tarafından çözülerek metin haline getirilir.¹⁴⁸ Yabancı dildeki kayıtlar tercüman aracılığıyla Türkçeye çevrilir.¹⁴⁹ Elde edilen kayıtların yazılı belgeler haline getirilmesi son derece önemlidir.

Tutanak tutulurken hiçbir bilginin atlanmadan aktarılmasına dikkat edilir.

Kişinin tanıklıktan çekinme hakkı sahipleriyle kurduğu iletişim kayıtları kayda alınmaz.

¹⁴⁷ CMK m.169/2.

¹⁴⁸ CMK m. 137/1.

¹⁴⁹ CMK m.137/2.

Bu işlemlerin uygulanmasında görev alan memurlar gerektiğinde tanık olarak dinlenmek üzere mahkemeye çağrılabilirler. Fakat tercihen hâkim takdirine kalmakla beraber gizli oturum yapılması talep edilir.

3.2.1.1.6 Verilerin Taşınması

Bilgi iletimi ve verilerin saklanıp korunma şekilleri gelişen teknolojiyle birlikte zamanla değişikliğe uğramaktadır. Bu süreçte yazılı belgeler kısmen yerini elektronik cihazlara bırakmıştır. Dinleme ve kayda alma işleminde kullanılan veri taşıyıcısındaki tüm veriler, Cumhuriyet savcısınca görevlendirilen adli kolluk personeline ayrı bir alt veri taşıyıcısına (CD, DVD vs.) nakledilir ve işlem ilgili tutanağa kaydedilir.¹⁵⁰

Yapılan dinleme ve kayıtlar yetkili personel tarafından çözülerek yazılı metin haline getirilir. Yazılı hale getirilemeyen, internet üzerinden gönderilen resim, tablo vb. gibi veriler resim haline getirilir.

Yabancı dildeki görüşmeler tercüman aracılığı ile Türkçeye çevrilir. Soruşturmanın gizliliğine zarar gelmemesi açısından çeviri yapacak kişinin güvenilirliğine dikkat edilmesi gerekmektedir. Ayrıca çeviri yapmadan önce Cumhuriyet savcısı tarafından görevlendirilmiş olması şarttır.

Dinleme ve kayda almaya ilişkin veri taşıyıcısına nakledilen tüm kayıtlar, görevlendirilen kolluk birimi personeline Cumhuriyet başsavcılığına sevk edilir. Kayıtlar ilgili soruşturma savcısının talimatı ile Adli Emanet Bürosuna teslim edilir ve alınan “Adli Emanet Fişi” soruşturma dosyasına eklenir.

3.2.1.1.7 İletişimin Denetlenmesinin Sonlandırılması

3.2.1.1.7.1 Tedbir Kararının Onanmaması Halinde Sonlandırma

Gecikmesinde sakınca bulunan hallerde Cumhuriyet Savcısı tarafından verilen kararın derhal hâkim onayına sunulmaması veya onaya sunulmasına rağmen hâkim tarafından savcının kararının onaylanmaması durumunda da tedbirin sona erdirilmesi gerekmektedir.¹⁵¹ Bu durumda, Cumhuriyet savcısının talimatı ile iletişimin denetlenmesine son verilir.

¹⁵⁰ Taşkın, s.138.

¹⁵¹ CMK m. 135/1-3.

3.2.1.1.7.2 Tedbir Koşullarının Ortadan Kalkması Üzerine Sonlandırma

Tedbire belirli bir süreyle karar verilmiş olması, bu sürenin sonuna kadar tedbirin uygulanabileceği anlamına gelmez. Eğer süre sona ermeden tedbirin uygulanmasına ilişkin koşullardan birisi ortadan kalkmışsa, tedbire derhal son verilmesi gerekir. Şüpheli veya sanığın suçu işlediğine veya iştirak ettiğine ilişkin şüphenin ortadan kalkması halinde sona erdirilmesi gerekir. Bu durumda, dinlemeyi yapan personelin konu hakkında tanzim edeceği rapor ilgili soruşturma savcısına gönderilir, soruşturma savcısının talimatı doğrultusunda iletişimin denetlenmesine son verilir.

Şüpheli hakkında kovuşturmaya yer olmadığına karar verilmesi durumunda da tedbirlerin uygulanmasına derhal son verilir.¹⁵²

3.2.1.1.7.3 Denetleme Süresinin Bitmesi ile Sonlandırma

Tedbirlere ilişkin karar, kural olarak sürenin sona ermesiyle kendiliğinden ortadan kalkar. Dolayısıyla, tedbirlerin uygulanmasını yapmakta olan Cumhuriyet Savcısı derhal tedbirlerin uygulanmasını sona erdirir. Sürenin bitiminden sonra TİB tarafından herhangi bir kayıt tutulmadığından dolayı herhangi bir veriye ulaşılabilmesi söz konusu değildir.

3.2.1.1.8 Denetleme Süresinin Uzatılması

İletişimin denetlenmesi görevini yapan personel iletişimin denetlenmesi esnasında elde edilen bilgileri rapor haline getirerek iletişimin denetlenmesinin devamının uygun olacağı şeklinde görüşünü belirtir, tanzim edilen rapor ilgili soruşturma savcısına gönderilir, savcının uzatma talebini uygun görmesi durumunda uzatma kararı verilmesi için ilgili mahkemeden talepte bulunur.

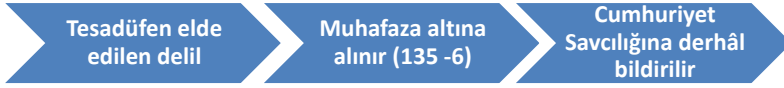
3.2.1.1.9 Tesadüfen Elde Edilen Deliller

3.2.1.1.9.1 Katalog Suçlara İlişkin Elde Edilen Tesadüfî Deliller

Tesadüfen elde edilen delillerden anlaşılması gereken yapılan bir soruşturma sırasında ele geçen ancak ilgili olmayan ve başka bir suçun işlendiğini gösteren delillerdir. Kanunda tesadüfen elde edilen delillerin sınırsız olarak kullanılmasına olanak tanınmamış, bu delilleri iki açıdan incelenmiştir. Tesadüfen elde edilen delil, *arama veya el koyma koruma tedbirlerinin uygulanması sırasında elde edilmişse* bu deliller ‘sınırsız’ olarak

¹⁵² CMK m. 137/3.

kullanılabilir. *İletişimin denetlenmesi sırasında* elde edilecek tesadüfî delil ise yalnızca katalog suçlardan birinin işlendiği şüphesini uyandırması durumunda kullanılabilir; bu tür delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir.¹⁵³ Cumhuriyet savcısı eldeki bilgileri dikkate alarak soruşturma açabilir.



3.2.1.1.9.2 Katalog Harici Suçlara İlişkin Elde Edilen Tesadüfî Deliller

Tesadüfen elde edilen deliller belirtilen 17 suçun dışında bir suç ile ilgili olduğu takdirde ister şüpheli için olsun ister üçüncü kişi için olsun kullanılamayacaktır.¹⁵⁴ Bu delilin muhafazası mümkün değildir, yasa dışı yollardan elde edilmiş delil olarak görülmektedir ve savcılık talimatıyla derhal yok edilmelidir.¹⁵⁵ Nitekim bu durum Yargıtay Ceza Genel Kurulu tarafından hükme bağlanmıştır.

Yüksek Mahkemenin uyuşturucu ticareti yapılan soruşturma kapsamında alınan tedbir kararının uygulanması sonucu elde edilen delillere de dayanılarak bazı sanıklar hakkında uyuşturucu madde kullanmak suçundan veya uyuşturucu madde ticaretiyle birlikte uyuşturucu madde kullanmak suçundan mahkûmiyet kararları verdiği görülmektedir.¹⁵⁶ Sanıklar hakkındaki hükümler, iletişimin denetlenmesi neticesinde elde edilen delillerin uyuşturucu madde kullanma suçu bakımından delil olarak değerlendirilemeyeceği şeklinde bir gerekçeyle bozulmayarak Yargıtay 10. Ceza Dairesince onanmıştır.¹⁵⁷

Nihayetinde, tesadüfen elde edilen deliller konusunda kanunda belirsizlikler olsa da

¹⁵³ Ünver,/Hakeri s.187; Öztürk, s.601.

¹⁵⁴ CMK m.. 138/2.

¹⁵⁵ Y.C.G.K. 2006/4.MD-122 E., 2006/162 K. Söz konusu olayda, çete kurmak suçundan telefonu hakim kararı ile dinlenen bir kişinin, bir başka çete üyesi ile görüşmesi sırasında, bir hakimin, arkadaşlarını tahliye edeceğine ilişkin bir konuşma geçmektedir. Telefon konuşmasında belirtildiği gibi sözü edilen kişi belirtilen tarihte tahliye edilmiştir. Ancak tahliye ile ilgili koşullar tamamen kanunlara uygundur. Bu telefon konuşması üzerine tahliye karar veren hâkim hakkında görevi kötüye kullanmak suçundan soruşturma açılmıştır. CGK olayda tesadüfen elde edilen ve delil olduğunu, elde edilen delilin hakkında dinleme kararı verilmeyen bir kişiyle ilgili olduğunu, bu delilin katalog haricinde kalan bir suçla ilgili olduğu gerekçesiyle hukuka aykırı delil sayılarak buna göre işlem yapılamayacağına hükmetmiştir.

¹⁵⁶ Kaymaz, s. 472.

¹⁵⁷ Yargıtay 10. CD. 27.6.2007 ve 2007/5954 E, 2007/8035 Karar.

katalog suçlardan olsun veya olmasın her türlü suça ilişkin deliller tutanağa geçirilmeli ve “Bir suça muttali olan kamu görevlisi, bu suçu Cumhuriyet savcısına bildirmekle yükümlüdür” kuralı gereği Cumhuriyet savcısının talimatı doğrultusunda hareket edilmelidir.¹⁵⁸

3.2.1.1.10 Verilerin Yok Edilmesi

İletişimin denetlenmesi sonucu elde edilen bilgilere ilişkin kayıtların, kullanıldıktan veya onlara ihtiyaç kalmadığının anlaşılmasından belirli bir süre sonra yok edilmesi gerekmektedir.

Veriler, gecikmesinde sakınca bulunan halde savcı tarafından alınmış kararın derhal hâkim onayına sunulmaması, sunulmasına rağmen onaylanmaması ya da şüpheli hakkında kovuşturmaya yer olmadığına karar verilmesi durumunda yok edilir.

Yok etme işlemi, tedbirin uygulanmasına son verme tarihinden itibaren en geç 10 gün içinde Cumhuriyet savcısının denetiminde yapılır. Yok etme işlemi ve nedenleri bir tutanakla tespit edilir.¹⁵⁹

Tablo 9- İmha Süreci (CMK 137)

1. fıkra	2. fıkra	3. fıkra	4. fıkra
•Cumhuriyet Savcısı veya görevlendireceği adli kolluk görevlisi, kararın yerine getirilmesini yazılı olarak ilgili iletişim kurumuna bildirir. •Zor kullanılabilir. •İşlem tutanakla tespit edilir.	•Tutulan kayıtlar, cumhuriyet savcılığınca görevlendirilen kişiler tarafından çözülerek metin hâline getirilir. •Yabancı dildeki kayıtlar, tercüman aracılığı ile türkçe'ye çevrilir.	•Kovuşturmaya yer olmamamsı ya da hâkim onayının alınamaması halinde, C. Savcısı tarafından derhâl son verilir. •Kayıtlar, C. Savcısının denetiminde en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilir.	•Kayıtların yok edilmesi halinde, en geç on beş gün içinde, C.Başsavcılığı tedbirin •Nedeni, •Kapsamı, •Süresi ve •Sonucu hakkında ilgilisine yazılı olarak bilgi verir.

¹⁵⁸ TCK m. 279.

¹⁵⁹ CMK m. 137/3.

Tablo 10- İmha Tutanağı Örneği

İMHA TUTANAĞI

..... Mahkemesi hakimi/savcısı tarafından karar verilen tarihli ve soruşturma sayılı tedbirinin tarihleri arasında uygulanması sonucunda elde edilen aşağıda cins ve miktarları yazılı bilgi ve belgeler günü saat’te, karşılığında belirtildiği şekilde imha edilmiştir.

Sıra No:**Türü-Cinsi :****Adedi : İmha Şekli*****İmha Nedeni :**

Bu tutanak tarihinde saat’da tanzim edilmiş ve tarafımızdan imzalanmıştır.

C.Savcısı
İMZA

Kolluk Görevlisi
İMZA

Kolluk Görevlisi
İMZA

* İmha işlemi, sebebi de belirtilerek Cumhuriyet savcısının denetiminde yapılır.

*Yakma, Silme, Kırma, Kıyma vb.

Veri taşıyıcısının Cumhuriyet Başsavcılığına gönderilmesinden sonra yok etme işlemi, Cumhuriyet savcısının belirleyeceği yöntemle gerçekleştirilir. Kayıtların silinmesi suretiyle de yok etme yükümlülüğü yerine getirilebilir.

3.2.1.1.11 Tedbirin Uygulandığının İlgililere Bildirimi

İletişimin denetlenmesi, kişilerin haberleşme özgürlüğüne yapılan ağır bir müdahale olarak kabul edildiğinden, keyfi uygulamaların önüne geçilmesi amacıyla iletişime yapılan müdahalenin sonra ermesine müteakip, hakkında tedbir uygulanan kişiye, uygulanan tedbirle ilgili bilgi verilmesi gerekmektedir.

Haklarında denetleme tedbiri uygulanan kişiler hakkında tutulan tespit ve dinlemeye ilişkin kayıtların yok edilmesi durumunda, soruşturma evresinin bitiminden

itibaren en geç 15 gün içinde, Cumhuriyet Başsavcılığı **tedbirin nedeni, kapsamı, süresi ve sonucu** hakkında ilgisine yazılı olarak bilgi verir.¹⁶⁰

Tedbire son verilmesinin ardından 10 gün içerisinde kayıtlar yok edilir. Ancak, bu kayıtlar yok edilir edilmez ilgisine bildirim yapılmaz ve soruşturma evresinin sona ermesi beklenir. Soruşturma sonlandıktan en geç 15 gün içerisinde bildirim yapılır.

3.2.1.2 İletişimin Denetlenmesi Yöntemleri

23.07.2006 tarihinden itibaren Adli ve Önleme amaçlı tüm dinlemeler Telekomünikasyon İletişim Başkanlığı tarafından yani tek bir merkezden yürütülmektedir. İletişimin denetlenmesi kapsamında iletişimin dinlenmesi, tespiti, mobil telefonun yerinin tespiti ve sinyal bilgilerinin değerlendirilmesi tedbirlerinden nasıl faydalandığına paylaşıcağız. Ayrıca bu iletişimin denetlenmesi yöntemlerinin yanı sıra görevli personel tarafından sık başvuran bazı ilave yöntemlere de değinilecektir.

Tablo 11- İletişimin Denetlenmesi Yöntemleri



Denetleme yöntemlerini günümüzde kullanılan teknoloji ürünlerini de dikkate alarak 3 farklı başlıkta incelemek mümkündür.

Bunlar;

¹⁶⁰ CMK m. 137.

1. İçerik takibi
2. Trafik takibi
3. Konum belirlemedir.

4. Tablo 12- İletişim Yöntemleri

Telefon ile İletişim	İnternet ile İletişim	Diğer İletişim Yöntemleri
• Sabit Telefon ve Faks lar • GSM Telefonları • Uydu Telefonları • Araç Telefonları	• Elektronik Posta • Messenger • Skype, VOIP vb.	• Telsiz ile İletişim • Posta ile İletişim

3.2.1.2.1 İçerik Takibi

Telekomünikasyon yolu ile yapılan iletişimin denetlenmesi tedbirlerinden biri olan iletişimin dinlemesi kapsamında sabit, mobil, araç veya uydu telefonlarıyla yapılan konuşmalar, internetten yapılan görüşmeler ve yazışmalar ile telsizlerle yapılan iletişimin içeriği takip edilebilmektedir. İletişimi yazılı, sözlü ve elektronik olarak üçe ayırabiliriz.

3.2.1.2.1.1 Yazılı İletişimde İçerik Takibi

Yazılı iletişime yönelik içerik takibi sık başvurulanan ve en eski yöntemlerden biridir. Matbu yazışmalar ve el yazısı ile hazırlanmış mektup gibi metinlerin elde edilerek okunmasını içerir. Bu uygulamaya özellikle cezaevlerinde sıkça başvurulduğu bilinmektedir. Ancak, bu şekilde yapılan yazılı içerik takibi, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi kapsamına girmemektedir. Matbu yazışmaların içeriği TCK'da yer alan arama ve elkoyma hükümlerine ve eğer posta yoluyla yapılan bir gönderi söz konusuysa bu belgeler TCK'da yer alan Postada El Koyma tedbiri hükümlerine tabidir.¹⁶¹



3.2.1.2.1.2 Sözlü İletişimde İçerik Takibi

Telekomünikasyon yoluyla yapılan sözlü iletişimin denetlenmesi çerçevesinde hâkim kararı doğrultusunda TİB devreye girerek cep telefonu ve sabit telefon işletmecilerinin altyapıları üzerinden telefon görüşmelerini kaydetmektedir.

¹⁶¹ CMK m. 129.

3.2.1.2.1.3 Elektronik İletişimde İçerik Takibi

Elektronik ortamda gerçekleştirilen yazılı, sözlü ve görüntülü her türlü iletişim biçimine yönelik olarak içerik takibi yapılabilmektedir.

Elektronik ortamdaki bu iletişim yasal olarak yine TİB aracılığıyla takip ediliyor, kaydedilebilmektedir. Anlık mesajlaşma yanında Messenger ve IP adresleri üzerinden ses iletimi sağlayan protokol olan VOIP (Voice Over IP), Skype gibi veri iletimi sağlayan programları iletişimin dinlenmesi kapsamında takip etmek mümkündür.

3.2.1.2.2 Trafik İzleme

Sabit telefonla yapılan görüşmelerde, cep telefonlarıyla yapılan görüşmelerde, İnternet üzerinden yapılan elektronik haberleşmelerde (e-posta, anlık ileti, İnternet sitelerine yapılan ziyaretler) kimin, kiminle, ne zaman ve ne kadar süre iletişim kurduğunun saptanması şeklinde özetlenebilir.

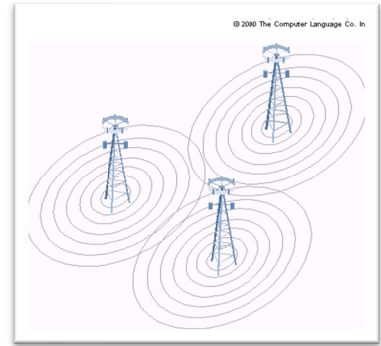
3.2.1.2.3 Konum Belirleme

Kimin, ne zaman, nerede bulunduğunun tespiti için ayrıca başvuru yöntemleri bulunmaktadır. Tarihsel olarak hafiyecilik, dedektiflik gibi yöntemlerle yapılan kimin nerede bulunduğuna ilişkin tespit, günümüzde elektronik cihazlara kaymıştır. Bu maksatla, Küresel konum belirleme (GPS) aletleri, Ekip Mobil, baz istasyonları, İnternet'e çıkışı sağlayan IP numarası kullanılabilmektedir.

3.2.1.2.3.1 Ekip Mobil

Cep telefonu işletmecileri araç takip sistemleri (fleet management- filo yönetimi) aracılığıyla görüşme ve konum takibi olanağı sağlamaktadırlar. Turkcell Ekip Mobil hizmeti mevcuttur.

Çok sayıda ticari şirket tarafından da kullanılmaktadır. Şirketler mobil ekiplerini, ekip mobil yardımı dijital haritalar üzerinden izleyebilir, konum bilgisini alabilir ve bir adrese en yakın personelin tespitini yapabilirler.



3.2.1.2.3.2 Küresel Konum Belirleme (GPS-Global Positioning System)

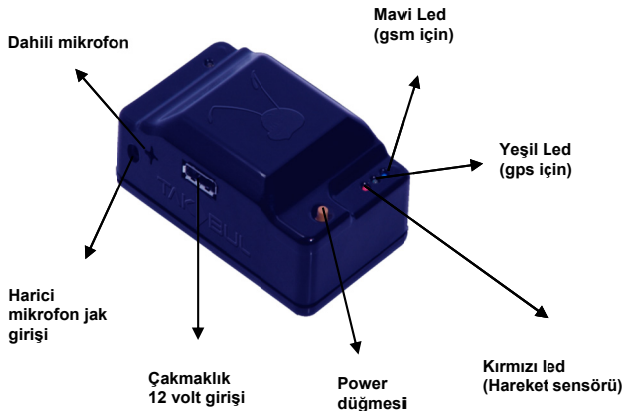
GPS yer tespitinde kullanılan temel yöntemlerden biridir. Düzenli olarak kodlanmış bilgi yollayan bir uydu ağıdır ve uydularla GPS kullanıcısı arasındaki mesafeyi ölçerek dünya üzerindeki kesin yeri tespit etmeyi mümkün kılan bir radyo navigasyon sistemidir.

Bu sistem, ABD Savunma Bakanlığına ait, yörüngede sürekli olarak dönen 24 uydudan oluşur. Bu uyduların yörüngesi öyle ayarlanmıştır ki, dünyanın üzerindeki herhangi bir nokta herhangi bir zamanda en az 4 uyduyu görebilir. Konum belirleme için 3 uydudan gelen bilgiler yeterli olmaktadır. Bu uyduların her biri kendine özgü kodlar ve yörünge bilgisi içeren çok düşük güçlü radyo sinyalleri yayarlar.

Uyduların kodlarına sahip yeryüzündeki GPS alıcısı, bu sinyalleri çözümleyerek yer ve hız bilgisi üretir.¹⁶² Böylece konum belirlenmesi mümkün olur. Bu bilgiler ise GPS kullanıcısını takip eden merkeze, mekanizma içinde kurulu GPRS sistemi üzerinden eş zamanlı olarak iletilir.

Bu sistemin ilk kuruluş hedefi tamamen askeri amaçlar içindir. GPS alıcıları yön bulmakta, askeri çıkartmalarda ve roket atışlarında kullanılmak üzere tasarlanmıştır. 1980'ler de sivil kullanıma da açılmıştır.

GPS'in baz istasyonun bilgisini veren mobil telefonla yapılan yer tespitinden farkı nokta tayini yapmasıdır. Şartlar ne olursa olsun, bir GPS alıcısı size yeryüzünde nerede olduğunuzu söyleyebilir. Neredeyse her yerde 365 gün 24 saat çalışabilirler. Tipide, yoğun siste, hatta okyanusun ortasında referans noktanız olmadığı zaman bile çalışırlar.



¹⁶² Çınar Soner, "GPS İle Araç Takip ve Yönlendirme Sistemi", Ankara: Yüksek Lisans Tezi, s.6.

Şekil 1. GPS Cihazı

Ticari sektörde GPS aletlerini şirketler çalıştırdıkları personeli takip amacıyla da kullanılmaktadırlar.

Özellikle kurye, nakliye işi yapan firmaların bu tür aletleri kullandığı bilinmektedir. Bu konum belirleme cihazları bazı cep telefonlarında, saat gibi taşınabilir elektronik cihazlarda da bulunabilmektedir. Alzheimer hastalarının veya çocukların takibi gibi amaçlarla kullanılabilen bu cihazların yasa dışı kullanımı da söz konusudur. Ayrıca ormancılık, dağcılık, yamaç paraşütü, trekking gibi doğa sporları tutkunları arasında popülaritesini arttırmıştır ve geniş bir kullanıcı kitlesine ulaşmıştır.

3.2.1.3 İletişimin Denetlenmesi Sistematığı

İletişimin denetlenmesinde delillerin toplanması süreci, yürütülen bir suç soruşturmasının veya kovuşturmasının en önemli aşamasını oluşturmaktadır. Elde edilen deliller ile hakkında kuvvetli şüphe sebepleri bulunan kişinin suçsuzluğu ortaya çıkacak ya da suçlu olduğu kanıtlanacaktır. Tedbirin doğru bir şekilde uygulanmaması soruşturmanın başarısızlıkla sonuçlanmasına yol açabilecektir. Doğru bir iletişimin denetlenmesi sistematığını üç aşamada incelememiz mümkündür. Bunlar soruşturma hakkında bilgi toplanan *hazırlık aşaması*, dinlemenin ve takibin yapıldığı *dinleme aşaması* ve elde edilen verilerin analizinin yapıldığı *değerlendirme aşamalarıdır*.

3.2.1.3.1 Hazırlık Aşaması

3.2.1.3.1.1 Gerekli Donanımın Sağlanması

İletişim denetlemesi yapmakla yetkili personelin görev yaptığı Teknik Takip ünitelerinde daha etkin hizmet verebilmesi için denetleme esnasında elde etmiş olduğu bilgileri zenginleştirilmesi, anlamlandırılması ve teyidi gibi hususlarda ilave donanımlara ihtiyacı bulunmaktadır. Artık günümüzde açık istihbarat kaynağı hale gelmiş olan internet gibi teknolojilerin kullanımı ve takibi ile hizmete özel ve gizli dereceli bilgilere ulaşmaya imkân tanıyan Pol-Net üzerinde çeşitli sorgulama sayfalarının (otel kayıtları, GBT vb.) düzenlenmesi çok önemlidir. Ayrıca, personelin düzenli bilgi paylaşımını sağlayabilmesi için telsiz ve telefon gibi iletişim araçlarıyla desteklenmesi gerekmektedir.

3.2.1.3.1.2 Görevlinin Bilgilendirilmesi

İletişimin denetlenmesi görevini yapacak soruşturma savcısının görevlendirdiği personel tedbirin şekli, amacı, süresi, tedbir esnasında dikkat edilmesi gereken konular hakkında bilgilendirilir. Hakkında çalışma yapılmasına karar verilen suça yönelik olarak önceden derlenen bilgilerin iletişimin denetlenmesiyle görevli personele aktarılır. Bu bilgiler ilgili personelin her zaman ulaşabileceği bir dosyada muhafaza edilmelidir. Çalışmanın kapsamı amacı ve hedeflerinin önceden öğrenilmesi amaca ulaşmayı kolaylaştırır. Soruşturma dosyasındaki bilgilerin “ne, nerede, niçin, nasıl, ne zaman ve kim” sorularıyla özümzenmesi sağlanmalıdır.



Personel tedbirin uygulanması esnasında istifade edilecek programlar ve materyaller hakkında eğitimden geçirilir.

3.2.1.3.1.3 Eksik Bilgi ve Delillerin Araştırılması

Yürütülen soruşturmanın sadece iletişimin denetlenmesinden ibaret olmadığı göz önüne alınarak, soruşturmayı yürüten birimlerce, soruşturmanın her aşamasında koordinasyon içerisinde hareket edilerek eksik bilgi ve delillerin araştırılır, gerekiyorsa görev bölümü yapılır.

3.2.1.3.2 Dinleme Aşaması

3.2.1.3.2.1 Elde Edilen Verilere İlişkin Not Alınması

Dinleme yapılırken görevli personelce görüşme içeriğine ilişkin kısa, öz ve anlaşılır bir şekilde notlar alınır. Elde edilen verilerle ilgili notlar daha önceden belirlenmiş standart bir formata işlenir. Böylece yeni verilerin eklenmesi sağlanır. Nihayetinde, elde edilen veriler ile formata işlenmiş bu bilgiler soruşturmada görevli birimlerce paylaşılarak değerlendirmeye tabi tutulur.

3.2.1.3.2.2 Hedef Profiline Çıkarılması

- **Açık Kimliği:** Hedef şahsın ve hedef şahısla iletişim kuran işbirliği yaptıkları şüphelenilen kişilerin açık kimliğinin belirlenmesi amacıyla internet ve Pol-Net

sorgulama sayfalarından (ehliyet, pasaport, vatandaşlık ve GBT kayıtları gibi) yararlanılır.

•**Dil ve Lehçe:** Hedef şahsın kullandığı dilleri, lehçeleri ve konuşma aksanının bilinmesi önem taşımaktadır. Şüpheli şahsın Farsça biliyor olması yapılacak bir uyuşturucu sevkياتın kaynağına ilişkin ipuçları verebileceği gibi örgütün muhtemel bir uyuşturucu pazarlığında yer alabileceğini gösterir.

•**Suç İlişkileri ve Konumu:** Hedef şahsın suç organizasyonu içerisindeki konumunun ortaya çıkarılması, bu organizasyonda yer alan diğer kimselerin konumları ile birlikte belirlenmesi ve mağdur, müşteki, tanık gibi şahıslarla aralarındaki ilişkilerinin boyutunun belirlenmesi ayrı ayrı önem taşımaktadır.

3.2.1.3.2.3 Suç Unsurlarının Tespiti

Kişinin suç profilinin çıkarılmasının ardından mahkemede kişinin lehine ve aleyhine kullanılacak bilgilerin elde edilmesi gerekmektedir. Suç unsurlarının tespitinde aşağıdaki unsurlara dikkat edilmesi gerekir.

•**Suç konu olay ya da olayların tespiti:** Hedef şahsın veya suç örgütünün kısmen veya tamamen gerçekleştirdiği olay ya da olayların tespit edilerek tutanak ve rapor haline getirilir.

•**Suç eşyasının tespiti:** Suç eşyası, suçu işlemeye elverişli ve suç konu olan her türlü araç ve gereç olarak tanımlanabilir. Bu anlamda hakkında iletişimin tespit ve denetlenmesi işlemi gerçekleştirilen şahıs ya da örgütün suçta kullandığı veya suçtan kaynaklı temin ettiği eşyanın menşeyinin, zilyedinin ve suçta kullanıcısının tespiti, suçun gerçekleştirilmesi akabinde muhafazasının nasıl ve nerede gerçekleştirildiğinin ortaya çıkarılması amaçlanmalıdır.

•**Delillerin tespiti ve toplanması:** İletişimin tespiti ve denetlenmesi tedbirinin uygulanmasının asıl amacı suçta karışanların tespiti ile suç delillerinin bulunmasıdır. Bu nedenle elde edilen her bilgi ve verinin, soruşturma dosyası kapsamında delil olarak kullanılabilecek seviyeye getirilmesi için ayrı ayrı araştırılması ve teyidi gerekmektedir. Bu şekilde yapılacak araştırmalarla suçta ilişkin delillerin toplanması sağlanacaktır.

• **Tesadüfî delillerin kaydedilmesi:** İletişimin denetlenmesi sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ve ancak, katalog suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir.

• **Yakalamaya yönelik bilgi toplama:** Soruşturma safhası içerisinde yeterli delilin toplanmasından sonra şüphelilerin yakalaması ve kişilerin barındıkları yerlerde delil araması yapabilmek için gerçekleştirilecek operasyonlar öncesinde takip edilen hedeflerin bulundukları ve bulunabilecekleri yerlerin tespitine yönelik bilgi toplama faaliyetleri tamamlanmış olmalıdır.

3.2.1.3.2.4 Bilgi Paylaşımı

Soruşturmayı yürüten birimler soruşturmanın her aşamasında birbirlerini bilgilendirmeleri gerekmektedir. Bilgi paylaşımından amaç, elde edilen her türlü bilgi ve verinin teyidinin sağlanması, böylece birimler arası koordinenin kurulmasıyla bu bilgi ve verilerin delillendirilmesi ve uygulanacak hareket tarzları ve stratejilerin belirlenmesidir. Bu süreç boyunca soruşturmanın gizliliği hiçbir şekilde ihlal edilmeden hiyerarşik sıra takip edilir ve soruşturma savcısı durumdan haberdar edilir. Nitekim paylaşılmayan bilgi yanlış yorumlara, gereksiz risklerin alınmasına, zaman ve işgücü kaybına, belki de kolluk güçlerinin muhbir tarafından yanlış yönlendirilmesine sebep olacaktır.

3.2.1.3.3 Değerlendirme Aşaması

İletişimin dinlenmesi ile elde edilen bilgi ve verilerin değerlendirilmeye alınarak analiz edilmesi sağlanmalıdır. Takip edilen şahıslarla ilgili olarak iletişimin dinlenmesi sonucu elde edilen veriler ışığında, hedef şahısların işlemiş oldukları suçlar analiz yapılabilecek şekilde sistemli halde toplanması gerekmektedir.

Bu şekilde, elde edilen veriler ışığında yapılacak analizler sayesinde delillerin yeterliliği, hedef şahıs sayısı, operasyonel müdahale şekli ve tarihleri gibi hususların ele alınarak değerlendirilmesi noktasında kolaylıklar sağlayacaktır.

Değerlendirme aşamasını birkaç kategoride incelememiz mümkündür.

3.2.1.3.3.1 Olay Analizi

Takip edilen hedef şahıs ya da suç örgütünün gerçekleştirdiği olayların tüm tarafları ile birlikte ve 5N-1K sorularına cevap verecek şekilde, olayın hazırlık-başlangıç-gelişme-oluşma ve sonuç aşamalarının ortaya konulmuş tarzda analizi yapılmalıdır.

Bir olayın gerçekleştiği düşünülen zamanda, hedef şahısların baz bilgilerinden faydalanarak olay yeri ve şüphelinin hareketleri tespit edilebilir.

Olay öncesi, olay esnası ve olay sonrası hedef şahsın ve gördüğü kişilerin incelenmesi ve değerlendirilmesi ile yeni şüphelilere ulaşmamız mümkündür. Bu durumda hedefin irtibat kurduğu şahsın çalışma kapsamına dâhil edilip edilmemesi noktasında karar vermek gerekecektir.

3.2.1.3.3.2 İlişkiler Analizi

Takip edilen suç örgütü mensuplarının birbirleri ile olan ilişkilerinin değerlendirilmesi yapılarak aradaki ilişkinin kaynağı ve dayanağının ortaya çıkartılması ile bunun yanı sıra suç örgütünün diğer kişilerle olan ilişkilerinin de değerlendirilmesi gerekmektedir.

3.2.1.3.3.3 Örgüt Analizi

İletişimlerin dinlenmesi sonucu elde edilen bilgiler ışığında, takip edilen suç örgütünün ne amaçla kurulduğunun, işleyişinin, görev dağılımının, baskı unsurlarının, niteliklerinin ve hedeflerinin belirlenerek analizi yapılmalıdır.

3.2.1.4 İletişimin Denetlenmesi Yasak Olan ve Özel Usullere Tabi Kişiler

3.2.1.4.1 İletişimin Denetlenmesi Yasağı

İletişimin denetlenmesi tedbirinin uygulanması sıkı koşullara bağlandığını ve tedbirin CMK'nın 135'inci maddesinde belirtilen şartlar dışında kullanılmasının yasak olduğunu gördük. Bu şartların yanı sıra, insan haklarına saygının bir gereği olarak şüpheli veya sanığın görüştüğü bazı kişilerin iletişimlerinin denetlenmesine de sınırlama getirilmiştir. Şüpheli veya sanığa yüklenen suç dolayısıyla savunmasını yapan avukatının iletişimi denetlenemez ve tanıklıktan çekinme hakkına sahip yakınlarıyla gerçekleştirdiği iletişim kayda alınamaz.

3.2.1.4.1.1 Avukatlar

Avukat, ceza yargılamasında, kamu görevi niteliğinde olan savunma makamını temsil etmektedir.¹⁶³ Şüpheli ya da sanığın savunmasının özgürce yapılabilmesi için avukatlara ayrıcalıklar tanınmıştır. Avukatlar meslek gereği öğrendiği bilgiler bakımından tanıklık yapmaktan çekinebilirler. Avukatın sanıkla arasındaki mektup ve belgeler denetime tabi tutulamaz, el konulamaz. Bunun gibi, şüpheli veya sanığa yüklenen suç dolayısıyla müdafinin bürosu, konutu ve yerleşim yerindeki telekomünikasyon araçları hakkında iletişimin denetlenmesi tedbiri uygulanamaz. Şüpheli hakkında delil elde etmek için müdafinin bu yerlerdeki iletişimi denetlenemez.

Bu yasak avukatların hiçbir zaman iletişimlerinin denetlenemeyeceği anlamına gelmez. Avukatların katalog suçlardan birini işledikleri şüphesi ile iletişimlerinin denetlenmesine her zaman karar verilebilir.¹⁶⁴ Bu yasak avukatın sadece müdafiliğini yaptığı şüpheli veya sanığa yüklenen suçla ilgilidir ve müdafinin bürosu, konutu veya işyerinde bulunan telekomünikasyon araçları ile sınırlıdır.¹⁶⁵

Avukat tarafından kullanılan mobil telefon bu yasak kapsamında değildir. Yukarıda sayılan yerler dışında kalan ankesörlü telefon, cep telefonu, araç telefonundan avukatın şüpheli veya sanıkla yaptığı suçla ilgili görüşmeler denetlenebilir. Ayrıca, şüpheli veya sanığın yakalayabilmesi için avukatının mobil telefonunun yerinin tespitine kararı verilebilir.

Avukat mahkemede müdafî olarak değil de şüpheli adına vekâleten yer alıyorsa, şüpheli/sanık ile aralarındaki iletişim denetlenebilir. Yine de bu durumdan istifade etmek isteyen örgüt üyelerinin avukatlarının evlerinde ikamet ettikleri, iletişimlerini avukatları vasıtasıyla kurdukları bilinmektedir.¹⁶⁶

3.2.1.4.1.2 Tanıklıktan Çekinme Hakkı Sahipleri

Tanıklıktan çekinme hakkı sahiplerinin şüpheli veya sanık ile aralarındaki iletişimlerinin kayda alınması konusunda bazı yasaklar getirilmiştir. Bu düzenleme kaynağını Anayasa'nın 38'inci maddesinde yer alan "Hiç kimse kendisini ve kanunda

¹⁶³ Taşkın, 2008, s. 152.

¹⁶⁴ 26434 sayılı TİB Yönetmeliği m. 7/5.

¹⁶⁵ CMK m. 136.

¹⁶⁶ Taşkın, 2008, s. 135.

gösterilen yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlayamaz” kuralından alır. Bu doğrultuda, şüpheli veya sanık ile tanıklıktan çekinebilecek kişiler arasında kurulan iletişim kayda alınamaz.¹⁶⁷

Kimler şüpheli hakkında tanıklıktan çekinme hakkına sahiptir? Kişi, akrabalık ile mesleki veya sürekli uğraş olmak üzere iki nedenle tanıklıktan çekinme hakkına sahiptir. **Akrabalık nedeniyle** şüpheli veya sanık hakkında tanıklıktan çekinebilecek kimseler aşağıda verilmiştir.¹⁶⁸

a) Şüpheli veya sanığın nişanlısı.

b) Evlilik bağı kalmasa bile şüpheli veya sanığın eşi.

c) Şüpheli veya sanığın kan hısımlığından veya kayın hısımlığından üstsoy veya altsoyu.

d) Şüpheli veya sanığın üçüncü derece dahil kan veya ikinci derece dahil kayın hısımları.

e) Şüpheli veya sanıkla aralarında evlâtlık bağı bulunanlar.

Meslekleri ve sürekli uğraşları sebebiyle tanıklıktan çekinebilecekler ile çekinme konu ve koşulları şunlardır:¹⁶⁹

a) Avukatlar veya stajyerleri veya yardımcılarının, bu sıfatları dolayısıyla veya yükledikleri yargı görevi sebebiyle öğrendikleri bilgiler.

b) Hekimler, diş hekimleri, eczacılar, ebeler ve bunların yardımcıları ve diğer bütün tıp meslek veya sanatları mensuplarının, bu sıfatları dolayısıyla hastaları ve bunların yakınları hakkında öğrendikleri bilgiler.

c) Malî işlerde görevlendirilmiş müşavirler ve noterlerin bu sıfatları dolayısıyla hizmet verdikleri kişiler hakkında öğrendikleri bilgiler.

Şüpheli veya sanığın burada sayılan kişilerle kurduğu iletişim kayda alınamaz. Kayda alma gerçekleşikten sonra bu durumun anlaşılması hâlinde, alınan kayıtlar Cumhuriyet savcısının huzurunda derhâl imha edilir ve bu husus tutanağa bağlanır.¹⁷⁰ İmha

¹⁶⁷ CMK m.135/2.

¹⁶⁸ CMK m. 45.

¹⁶⁹ CMK m. 46.

¹⁷⁰ Suç şüphelisi bile olsa tanıklıktan çekinme hakkına sahip kişilerin şüpheli veya sanıkla iletişimlerinin kayda alınamayacağına hükmetmiştir. Danıştay 10. Daire, 14.10.2008 tarih ve 2007/2795 E sayılı yürütmeyi durdurma kararı.

edilmeden dosyaya konulsa bile delil olarak kullanılamaz. Ancak bu kişiler suç şüphesi altındaysalar bu yasak kalkar.¹⁷¹

Ayrıca kayda alma dışında kalan iletişimin tespiti, mobil telefonun yerinin tespiti, sinyal bilgilerinin değerlendirilmesi gibi diğer denetleme tedbirleri bu kişiler için uygulanmasında sınırlama yoktur.

3.2.1.4.2 İletişimi Denetlenmesi Özel Usullere Tabi Olan Kişiler

3.2.1.4.2.1 Milletvekilleri

CMK’da iletişimin denetlenmesine karar verilecek kişinin konumu ve görevi açısından herhangi bir istisnaya yer verilmemiştir. Hakkında soruşturma veya kovuşturma yapılan herkes için iletişimin denetlenmesi kararı verilebilir. Ancak, milletvekillerinin temsil görevlerini gereği gibi yerine getirmelerinin sağlanması, keyfi ve asılsız nedenlerle görevlerini yapmaktan alıkonulmamaları için yasama dokunulmazlığı kabul edilmiştir.

Milletvekilleri hakkında soruşturma veya kovuşturma yapabilmek için TBMM’nin kararı gerekmektedir. Dolayısıyla bir milletvekilli hakkında suç isnadında bulunulmuş olması durumunda, haklarında soruşturma başlatılabilmesi ve böylece iletişimlerinin denetlenebilmesi TBMM iznine tabidir.¹⁷² Milletvekili olmayan Bakanlar için de bu dokunulmazlık düzenlemesi geçerlidir.

Milletvekilli dokunulmazlığı bazı durumlarda devreye girmemektedir. Şöyle ki, ağır cezayı gerektiren bir suçüstü hali olması veya seçimlerden önce soruşturulmasına başlanmış olması kaydıyla Anayasa’nın 14. maddesindeki durumların söz konusu olması halinde, milletvekilleri dokunulmazlığa sahip bulunmamaktadırlar.

3.2.1.4.2.2 Kamu Görevlileri

Kamu görevlilerinin gereksiz şikâyet ve ihbarlar ile soruşturma ve kovuşturmayla uğrama korkusu taşımadan bu görevlerini güven içinde yapmalarının sağlanması düşüncesiyle kamu görevlilerinin görevleriyle ilgili işlemiş oldukları suçların soruşturulması farklı usullere tabi tutulmuştur. 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanuna göre kamu görevlilerinin işlemiş olduğu görevleriyle ilgili suçların (görevle ilgili olmayan suçlar hariç) soruşturmasının

¹⁷¹ 26434 sayılı TİB Yönetmeliği m. 7/4.

¹⁷² Anayasa m. 83/2.

başlatılabilmesi için önceden izin alınması gerekmektedir.¹⁷³ Bu izni adli soruşturma izni vermeye yetkili makamlar vermeye yetkilidir. Soruşturma izninin verilmesinin ardından iletişimin denetlenmesi tedbirine başvurulabilir. Ağır cezayı gerektiren suçüstü hali genel hükümlere tabidir.

Memur ve diğer kamu görevlilerinin kişisel suçlar ve görev nedeniyle işledikleri bazı suçlar ise bu yasa kapsamında değerlendirilmemektedir. Bankalar kanununda yazılı suçlarla, irtikâp, rüşvet, basit ve nitelikli zimmet, görev sırasında veya görev sırasında veya görevinden dolayı kaçakçılık, resmi ihale alım ve satımlarına fesat karıştırma, Devlet sırlarının açıklanması veya açıklanmasına sebebiyet verme suçlarından veya bu suçlara iştirak etmekten sanık olanlar hakkında Cumhuriyet savcıları izne gerek duymadan iletişimin denetlenmesi tedbirine başvurulabilirler.¹⁷⁴

Aynı zamanda yüz kızcırtıcı suçlar, organize suçlar, adli görev sırasında işlenen suçlar, işkence ve kötü muamele, Atatürk aleyhine işlenen suçlar, seçim suçları, Devlet düzenini bozan ve güvenliği aleyhine işlenen suçlarda izne gerek duyulmadan doğrudan soruşturma açılır.

3.2.1.4.2.3 Hâkimler ve Savcılar

24.2.1983 tarihli 2802 sayılı Hakimler ve Savcılar Kanununda Hâkim ve Cumhuriyet savcılarının görevleri sırasında veya görevleri sebebiyle işlemiş oldukları suçlarla ilgili soruşturma ve kovuşturma yapılması Adalet Bakanlığının iznine tabidir hükmü yer almaktadır.¹⁷⁵ Buna karşın 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun ile getirilen düzenlemelerle Anayasa'nın 144 ve 159'uncu maddelerinde yapılan değişiklik sonucunda; adalet hizmetleri ile Cumhuriyet savcılarının idari görevlerine ilişkin hususlar hariç olmak üzere hâkim ve savcıların görevlerini; kanun, tüzük, yönetmelikler ve genelgelere (hâkimler için idari nitelikteki genelgelere) uygun olarak yapıp yapmadıklarını denetleme; görevlerinden dolayı veya görevleri sırasında suç isleyip islemediklerini, hâl ve eylemlerinin sıfat ve görevleri icaplarına uyup uymadığını araştırma ve gerektiğinde haklarında inceleme ve soruşturma işlemleri, Adalet Bakanlığından alınarak Hâkimler ve Savcılar Yüksek

¹⁷³ 4483 sayılı Kanun.

¹⁷⁴ 3628 sayılı Mal Bildiriminde Bulunulması, Rüşvet ve Yolsuzlukla Mücadele Kanunu m. 17.

¹⁷⁵ 2802- m. 82, 87.

Kurulunun ilgili dairesinin teklifi ve Hâkimler ve Savcılar Yüksek Kurulu Başkanının oluru ile Kurul müfettişlerine yaptırılacağı hüküm altına alınmıştır.

Ayrıca 11.12.2010 tarihli ve 6087 sayılı Hâkimler ve Savcılar Yüksek Kurulu Kanununun “Kurulun görevleri” kenar başlıklı 4’üncü maddesinin birinci fıkrasının (c) bendinde; bazı özel görevleri olanlar¹⁷⁶ hariç araştırma, inceleme ve soruşturma işlemlerinin Kurul tarafından yapılacağı hükme bağlanmıştır.

2802 sayılı Kanunda, yukarıda sözü edilen Anayasa değişikliği ile uyumlu biçimde henüz değişiklik yapılmadığından ve aynı konuyu düzenleyen 6087 sayılı Kanunun sonradan yürürlüğe girmiş olmasından dolayı çelişen yerlerde 6087 sayılı Kanunun uygulanması gerekmektedir.¹⁷⁷ Dolayısıyla Kurul tarafından izin verilirse ancak soruşturma açılabilir ve iletişimin denetlenmesi yapılabilir. İzin verilmez ise iletişim denetlenmesi yapılamaz.

2802 sayılı Kanunun 94’üncü maddesine göre, ağır ceza mahkemesinin görevine giren suçüstü hâllerinde ise hazırlık soruşturması genel hükümlere göre yapılacak ve soruşturma yetkili Cumhuriyet savcıları tarafından bizzat yürütülecektir.¹⁷⁸ Bu halde durumun hemen Adalet Bakanlığına (Anayasa hükümleri karşısında Hâkimler ve Savcılar Yüksek Kuruluna) bildirilmesi gerekmektedir.

Kişisel suçlar bakımından ise soruşturma yapılması izne tabi değildir. Kanunda sadece yetkili adli merciler tayin edilmiştir.¹⁷⁹

¹⁷⁶ 6087 sayılı Kanunun 4’üncü maddesinin birinci fıkrasının “c” bendi:

“... ”

1) Bakanlık merkez, bağlı ve ilgili kuruluşları ile uluslararası mahkemeler veya kuruluşlarda görev yapan hâkim ve savcılar.

2) Geçici yetki veya görevlendirme ile başka bir kurum, kurul veya kuruluşta çalışan hâkim ve savcılar.

3) İdari görevleri yönünden savcılar.

4) Komisyon işlerine yönelik görevleri yönünden adalet komisyonu başkan ve üyeleri

“... ”

¹⁷⁷ Çakmak Seyfullah, Hâkim ve Savcılar Hakkındaki Araştırma, İnceleme ve Soruşturma İşlemleri, Adalet Dergisi, 43. Sayı, Mayıs 2012. s. 104–135.

¹⁷⁸ 2802 sayılı Kanunun “Ağır Ceza Mahkemesinin Görevine Giren Suçüstü Hâlleri” başlıklı 94’üncü maddesi:

“Ağır ceza mahkemesinin görevine giren suçüstü hâllerinde hazırlık soruşturması genel hükümlere göre yapılır. Hazırlık soruşturması yetkili Cumhuriyet savcıları tarafından bizzat yürütülür.

Bu halde durumun hemen Adalet Bakanlığına bildirilmesi zorunludur.”

¹⁷⁹ 2802 sayılı Kanunun “Kişisel Suçlarda Soruşturma ve Kovuşturma” başlıklı 93’üncü maddesi:

“Hâkim ve savcıların kişisel suçları hakkında soruşturma, ilgilinin yargı çevresinde bulunduğu ağır ceza mahkemesine en yakın ağır ceza mahkemesi Cumhuriyet başsavcısına ve son soruşturma o yer ağır ceza mahkemesine aittir.

O nedenle, kişisel bir suç nedeniyle veya suçüstü ağır suç halinde hakkında soruşturma ve kovuşturma yapılan Cumhuriyet Savcısı veya hâkimin iletişimi denetlenebilecektir.

3.2.1.4.2.4 Yargıtay Üyeleri

Yargıtay Birinci Başkanı, birinci başkan vekilleri, daire başkanları, üyeleri, Yargıtay Cumhuriyet Başsavcısı ve Yargıtay Cumhuriyet Başsavcı vekilinin görevleriyle ilgili veya kişisel suçlarından dolayı haklarında soruşturma yapılabilmesi Yargıtay Birinci Başkanlık Kurulunun kararına bağlıdır. Ancak, ağır cezayı gerektiren suçüstü hallerinin hazırlık ve ilk soruşturması genel hükümlere tabidir. Birinci Başkanlık Kurulu kararıyla soruşturma izni verilmeden adı geçen Yüksek Mahkeme mensupları hakkında soruşturma yapılması ve iletişimlerinin denetlenmesi mümkün değildir.¹⁸⁰

Diğer yüksek yargı organlarının başkanları, üyeleri veya diğer kişilerle ilgili olarak yürütülecek soruşturmaların usul ve esasları da 06.01.1982 tarihli ve 2575 sayılı Danıştay Kanununun 76'ncı maddesi, 03.12.2010 tarihli ve 6085 sayılı Sayıştay Kanununun 66'ncı maddesi, 30.03.2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanunun 16 ve 17'nci maddeleri, 27.06.1972 tarihli ve 1600 sayılı Askeri Yargıtay Kanununun 37 ve 38'inci maddeleri, 04.07.1972 tarihli ve 1602 sayılı Askeri Yüksek İdare Mahkemesi Kanununun 32 ve 33'üncü maddelerinde düzenlenmiştir.

3.2.1.4.2.5 Yabancılar

CMK' da ve diğer kanunlarımızda, yabancılar bakımından iletişimin denetlenmesi tedbirine ilişkin herhangi bir hüküm bulunmamaktadır. Bu sebeple, diplomatik dokunulmazlığı bulunanlar hariç, ülkemiz bulunan yabancıların iletişiminin denetimi CMK'nın 135'inci maddesi koşullarına bağlıdır. Diplomatik dokunulmazlığı olan kişilere karşı ise Türk Mahkemelerinde dava açılmaz¹⁸¹ ve CMK kapsamında iletişimleri denetlenemez.¹⁸²

Adalet Bakanlığı merkez, bağlı ve ilgili kuruluşlarındaki hakim ve savcıların kişisel suçları hakkında soruşturma ve kovuşturma Ankara Cumhuriyet Başsavcısı ve ağır ceza mahkemesine aittir."

¹⁸⁰ 2797 sayılı Yargıtay Kanunu m. 46.

¹⁸¹ BM Viyana Sözleşmesi m. 31 – 1. Diplomatik ajan, aşağıdaki hususlar dışında, kabul eden Devletin medeni ve idari yargısından da bağıstıktır. a) Kabul eden Devletin topraklarında bulunan özel bir taşınmazla ilgili bir aynı hak davası, yeter ki bu taşınmaz, gönderen Devlet adına ve misyon amaçları için kullanılmak üzere diplomatik ajanın tasarrufunda bulunmamış olsun, b) Diplomatik ajanın gönderen Devlet adına değil de bir özel kişi olarak vasiyeti tenfiz memuru, mirasın idarecisi, mirasçı veya vasiyet olunan kişi sıfatıyla ilgili

Tablo 13- Mukayeseli Hukuka Göre Adli Amaçlı İletişimin Denetlenmesi

ABD	İNGİLTERE	FRANSA	ALMANYA	İTALYA	TÜRKİYE
Hâkim Savcı	İçişleri Bakanı	Sorgu Hâkimi	Hâkim Savcı	Mahkeme, ivedi durumda Savcı	Hâkim Savcı
Uyuşturucu madde suçları, örgütlü suçlar, ekonomik suçlar, atom tesislerinin korunmasını ihlal eden suçlar ve cinsel suçları, en az 1 yıl hapis cezası gerektiren suçlar	3 yıl cezaayı gerektiren suçlar ve örgütlü suçlar.	Cürümler ve suçlar iki yıl ya da daha fazla süreli hapis cezası.	Sınırlı bir suç listesi.	En az beş yıl cezaayı içeren suçlardan oluşan sınırlı bir liste.	Sınırlı bir suç listesi
30 gün Yenilenebilir.	2 ay: Yenilenebilir.	4 ay: Yenilenebilir.	3 ay: Yenilenebilir.	15 gün: Yenilenebilir.	3 Ay: Yenilenebilir.
Basit şüphe	Şüphe derecesi düzenlenmemiştir.	Şüphe yeterlidir.	Özel Şüphe derecesi aranır.	Özel Şüphe derecesi aranır.	Özel Şüphe derecesi aranır.

3.2.2 Önleme Amaçlı İletişimin Denetlenmesi

Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanlığı; yasaların kendisine verdiği yetki ve sorumluluk çerçevesinde, devletin ülkesi ve milletiyle bölünmez bütünlüğüne, anayasal düzenine, genel güvenliğine yönelik önleyici ve koruyucu tedbirleri almak, emniyet ve asayiş sağlamak üzere ülke seviyesinde istihbarat faaliyetinde bulunmaktadır. Bu görevin yerine getirilmesine yönelik olarak 3713 sayılı TMK'nın 10'uncu maddesinin dördüncü fıkrasında belirtilen suçların önlenmesi amacıyla önleyici amaçlı iletişime müdahale usulü uygulanmaktadır.

Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanlığı bünyesinde yürütülen iletişime müdahale faaliyetlerine, 2559 sayılı PVSK'nın ek 7'nci maddesi hükümleri uyarınca TMK'nın 10'uncu maddesi ile yetkili Ağır Ceza Mahkemeleri ve Özgürlük

bulunduğu mirasa ilişkin bir dava; c) Diplomatik ajanın kabul eden Devlet dâhilinde resmi görevleri dışında icra ettiği herhangi bir mesleki veya ticari faaliyet ile ilgili bir dava. 3. Bu haller dışında bir diplomatik ajan hakkında hiçbir icra önemi alınmaz. Söz konusu durumlarda dahi ajanın şahsının veya konutunun dokunulmazlığı ihlal edilemez.

¹⁸² 1961 tarihli Diplomatik İlişkiler hakkında BM Viyana Sözleşmesi m. 27.

Hâkimlerinden alınan Hâkim Kararları ile izin verilmekte ve kararlar TİB (Telekomünikasyon İletişim Başkanlığı) üzerinden işleme konulmaktadır.

23 Temmuz 2005’de yasalaşan 5397 sayılı kanun ile bütün dinleme faaliyetlerinin tek bir merkez olarak TİB üzerinden yapılması, bu faaliyetlerin denetimini ve disiplin içinde yürütülmesini sağlamıştır.

3.2.2.1 İletişimin Denetlenmesi Süreci

İlk aşamada; İstihbarat Şube Müdürlüklerinin saha çalışması, muhbir kaynaklı bilgiler, ihbarlar, operasyonlarda elde edilen bilgiler, analiz çalışmaları ve açık kaynaklardan elde edilen bilgilerin hassas bir şekilde değerlendirilmesi sonucunda; terör suçları, uyuşturucu madde imal ve ticareti ile cebir ve tehdit içeren organize suçların işlenmesinin önlenmesi amacıyla iletişimi denetlenecek şahıslar ve kullandıkları iletişim araçları tespit edilmektedir.

İkinci aşamada istihbarat görevlisi tarafından; hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespiti imkân veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenleri içeren gerekçeli talep yazılı olarak hazırlanır ve sıralı amirlerin onayına sunulur. Sıralı amirlerin onayından geçen dinleme talebi resmi yazı ile yetkili mahkemelere gönderilir.

İlgili Bölge Ağır Ceza Mahkemesi Hâkimliği veya Özgürlük mahkemeleri tarafından istihbarat biriminin talebi incelenerek, uygun görüldüğü takdirde önleme amaçlı dinleme kararı verilir.

Yetkili mahkemelerden alınan hâkim kararları işleme konulmak üzere Telekomünikasyon İletişim Başkanlığına gönderilir. Burada hukuk ve teknik biriminin onayından geçtikten sonra iletişim araçlarının verileri Başkanlığımıza yönlendirilir.

İstihbarat Dairesi Başkanlığı bünyesinde dinleme işleminin gerçekleştirildiği teknik takip merkezlerinde gerekli güvenlik tedbirleri alınmış olup, merkez içerisine cep telefonu, USB bellek, video kamera vb. görüntü ve ses kaydı alabilecek herhangi bir cihazın sokulması kesinlikle yasaktır.

Dinleme yapılan bilgisayarlardan herhangi bir veri aktarımı yapılması da teknik olarak da mümkün değildir. CD-DVD Rom ve USB bellek okuyucu sistemleri bu bilgisayarlarda kullanılmamaktadır. Giriş kapıları devamlı kapalı tutulmakta, giriş çıkışlar kameralar ve kapı kontrol sistemleriyle sürekli denetim altında bulundurulmaktadır. Ayrıca dinleme işlemini gerçekleştiren personele aidiyet numarası tanımlı olup, ilgisiz kişilerin dinleme işleminin yapıldığı bilgisayara giriş yapabilmesi de mümkün değildir.

İstihbarat Dairesi Başkanlığınca yapılan dinleme işlemleri kapsamındaki kayıtlar tedbirin sonlanmasına müteakip en geç on gün içerisinde geri getirilemeyecek şekilde imha edilir ve görevli personeller tarafından imha tutanağı tanzim edilir. Bu imha tutanağı denetimlerde ibraz edilmek üzere muhafaza edilir. Ayrıca bu işlemlere ilave olarak kullanılan hard diskler, teknolojik ömrü tamamlandıktan sonra hard disk kırma makinesi ile parçalanarak imha edilir.

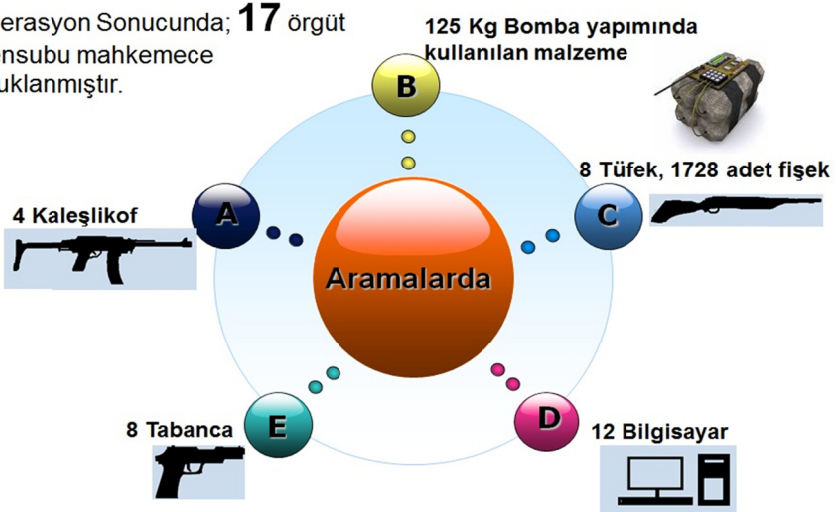
Dinleme işleminin gerçekleşmesi için, iletişim aracının tespit edilmesi, uygun görüş sorulması, mahkemeye gönderilmesi, mahkemeden alınan kararın Başkanlığımızda görevli personellerce kontrol edilmesi ve TİB'e gönderilerek Hukuk ve Teknik Dairesi Başkanlığınca onaylanması, bu çerçevede birden çok kurumun (İstihbarat birimleri, Mahkemeler, TİB) ve birden çok görevlinin kontrol ve denetiminden geçmesi gerekmektedir. Bu bağlamda hâkim kararına dayanmayan, yasa dışı ve keyfî bir dinleme işlemi mümkün değildir.

3.2.2.2 Önleme Amaçlı İletişimin Denetlenmesi Sonucu Yapılan Operasyonlardan Örnekler



Şekil 2. El Kaide Operasyonu

Operasyon Sonucunda; **17** örgüt mensubu mahkemece tutuklanmıştır.



Şekil 3. El Kaide Operasyonu Sonuçları

3.2.2.3 İstihbarat Faaliyetlerinin Sonuçları

- ✓ 2012 yılında Terör Örgütlerine yönelik yapılan operasyonlarda;
- 138 bombacı örgüt mensubu yakalanmış,
- 10.000 gr RDX,
- 37.890 gr TNT,
- 196.348 gr A-4 Patlayıcı,
- 37.300 gr C-4 Plastik Patlayıcı,
- 607.292 gr kimyasal madde ele geçirilmiştir.
- 2010-2011-2012 tarihleri arasında gerçekleştirilen operasyonlarda (100) eylem aydınlatılmış, (284) eylem engellenmiştir.
- ✓ Son bir yılda organize suç örgütlerine yönelik yapılan operasyonlarda ise;
- 26.284.362 gr uyuşturucu madde,
- 1099 adet ateşli silah ve 63.036 adet fişek,
- 27.127.841 adet gümrük kaçağı malzeme,
- 54.523.700 sahte para,
- 1.204.031 adet uyuşturucu hap,
- 4.902 adet muhtelif tarihi eser ele geçirilmiş,
- 17.471 kişi gözaltına alınmış, bunlardan 6.478 kişi tutuklanmıştır.
- ✓ 2012 Yılı Mart ayında Ankara ve İstanbul ilinde DHKP/C örgütüne yönelik yapılan operasyonda; 6 kişi yakalanmış olup, yapılan aramalarda;
- Sayın Başbakanımızın ikametine yönelik eylem çalışması,

- Ankara Adliyesinde görevli hâkim ve savcılarının araç ve lojmanlarına yönelik eylem çalışması,
- Geçmiş dönemde yaşanan Çorum Olayları’nda adı geçen Muharrem ŞEMSEK’in evi ve işyeri hakkında eylem çalışması,
- Adalet Bakanlığı Ceza İşleri Genel Müdürlüğü personeline ait araçların tespitine yönelik eylem çalışması,
- Adalet Eski Bakanlarından Hikmet Sami TÜRK’ün Bolu’daki evine ait eylem çalışması, olduğu değerlendirilen fotoğraflar ve krokiler ele geçirilmiştir.

3.3 Jandarma Teşkilatı

3.3.1 Telekomünikasyon Yoluyla İletişimin Tespiti, Dinlenmesi ve Kayda Alınmasına İlişkin Uygulamalar

Jandarma Genel Komutanlığınca, iletişimin denetlenmesine yönelik faaliyetler mevzuat esasları çerçevesinde, (TİB) imkân kabiliyetleri kullanılmak suretiyle yürütülmektedir.

Telekomünikasyon yoluyla iletişimin tespiti, dinlenmesi ve kayda alınmasına ilişkin faaliyetler adli maksatlı ve önleyici maksatlı olmak üzere iki şekilde icra edilmektedir.

Adli maksatlı faaliyetler CMK’nın 135’inci maddesine göre; bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkanının bulunmaması durumunda suç ve suçluların tespiti maksadıyla hâkim ve gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla katalog suçlara yönelik icra edilmektedir.

Önleyici maksatlı faaliyetler ise Jandarma Teşkilat Görev ve Yetkileri Kanunu’nun ek 5’inci maddesine göre; Jandarmanın mülki görevlerini yerine getirirken önleyici ve koruyucu tedbirleri almak üzere, sadece kendi sorumluluk alanında suçların işlenmesinin önlenmesi amacıyla, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Jandarma Genel Komutanı veya İstihbarat Başkanının yazılı emriyle katalog suçlara yönelik icra edilmektedir.

3.3.2 Adli Teknik Takip Faaliyetlerinin İcrası

3.3.2.1 Mahkeme Kararı Alınmadan Önce Yapılan İşlemler

Bir suç dolayısıyla ya da suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda hakkında tedbir uygulanacak şahıs ile ilgili olarak;

- Kullandığı numaranın abone kimlik bilgileri sistem üzerinden tespit edilir.
- Suç bilgileri Kaçakçılık İstihbarat Harekât ve Bilgi Toplama (KİHBİ) sisteminden belirlenir.
- Jandarma sorumluluk sahasında faaliyet yürüttüğüne dair faaliyet alanı, ev ve iş adresleri vb. bilgiler tespit edilir.
- Diğer tespitlerle (ifade tutanakları, açık kaynak bilgileri, daha önceki iletişimin denetlenmesi faaliyetlerinden elde edilen veriler vb.) ilgili çalışma yapılır.
- Yapılan bu tespitler ile şahsın suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığını ortaya koyacak şekilde ayrıntılı bir araştırma tutanağı tanzim edilir.
- İletişimin denetlenmesine yönelik talepler, ilgili ilçe Jandarma Komutanlığı tarafından Cumhuriyet savcısına iletilir. Bu talep uygun görüldüğü takdirde Cumhuriyet savcısınca yetkili mahkemeye yapılır.

3.3.2.2 Mahkeme Kararı Alındıktan Sonra Yapılan İşlemler

Birlikler tarafından, teknik takip kararlarının yetkili adli makamlardan alınmasını müteakip, elektronik ortamda Teknik İstihbarat Daire Başkanlığına gönderilir. Mahkeme Kararları, şeklen kontrolün yapılmasını müteakip Jandarma İstihbarat Teknik Analiz Sistemi üzerinden başlatma tutanağı tanzim edilerek Telekomünikasyon İletişim Başkanlığına (TİB) elektronik ortamda gönderilir.

İletişimin denetlenmesine ilişkin veriler; TİB tarafından kararın hukuki incelenmesi yapılmasını müteakip, kararda görevlendirilmiş personelin aidiyet numarasına güvenlikli hatlar üzerinden gönderilir.

İletişimin denetlenmesi faaliyetleri, Cumhuriyet Savcılığınca yetkilendirilmiş aidiyet numaralı personel tarafından, İl Jandarma Komutanlıklarında tesis edilmiş teknik istihbarat odalarında, TİB tarafından gönderilen veriler üzerinden icra edilmektedir. Yapılan tüm faaliyetler Cumhuriyet savcılarının gözetim ve denetiminde icra edilmektedir. Görevli personel, faaliyet esnasında tespit ettiği suçla ilgili bilgileri anında Cumhuriyet savcısına bildirmekte ve talimatı doğrultusunda hareket etmektedir.

3.3.2.3 Mahkeme Kararının Sona Ermesini Müteakip Yapılan İşlemler

İletişimin denetlenmesi faaliyeti mahkeme kararı veya Cumhuriyet savcısının kararı ile sonlandırılmaktadır. Faaliyet esnasında herhangi bir suç ve/veya suçluların tespit edilmesi durumunda;

- ✓ İletişimin denetlenmesine ilişkin tüm kayıtlar ve veriler Cumhuriyet savcısına teslim edilir.
- ✓ Cumhuriyet savcısının denetiminde iletişimin içeriğine ait tüm kayıtlar en geç 10 gün içinde imha edilir.
- ✓ İletişimin denetlenmesi kararına ait tüm evrak, dinlemeye ilişkin veriler hariç tek dosyada arşivlenir.

Şüpheli hakkında kovuşturmayla yer olmadığına dair karar verilmesi halinde,

- ❖ Cumhuriyet savcısının denetiminde iletişimin içeriğine ait tüm kayıtlar en geç 10 gün içinde imha edilir.
- ❖ İletişimin denetlenmesi kararına ait tüm evrak, dinlemeye ilişkin veriler hariç tek dosyada arşivlenir.

3.3.3 Önleyici Teknik Takip Faaliyetlerinin İcrası

3.3.3.1 Mahkeme Kararı Alınmadan Önce Yapılan İşlemler

Jandarma, mülki görevlerini yerine getirirken önleyici ve koruyucu tedbirleri almak üzere, sadece kendi sorumluluk alanında suçların işlenmesinin önlenmesi amacıyla hakkında tedbir uygulanacak şahıs ile ilgili olarak;

- Kullandığı numaranın abone kimlik bilgileri sistem üzerinden tespit edilir.
- Suç bilgileri Kaçakçılık İstihbarat Harekât ve Bilgi Toplama (KİHBİ) sisteminden belirlenir.
- Jandarma sorumluluk sahasında faaliyet yürüttüğüne dair faaliyet alanı, ev ve iş adresleri vb. bilgiler tespit edilir.
- Diğer tespitlerle (ifade tutanakları, açık kaynak bilgileri, daha önceki iletişimin denetlenmesi faaliyetlerinden elde edilen veriler vb.) ilgili çalışma yapılır.
- İletişimin denetlenmesine yönelik talepler, İl Jandarma Komutanı tarafından yetkili Ağır Ceza Mahkemesine veya gecikmesinde sakınca bulunan hallerde Jandarma Genel Komutanlığına veya İstihbarat Başkanlığına yapılır.

3.3.3.2 Mahkeme Kararı Alındıktan Sonra Yapılan İşlemler

Birlikler tarafından, iletişimin denetlenmesi kararlarının alınmasını müteakip, elektronik ortamda Teknik İstihbarat Daire Başkanlığına gönderilir. Mahkeme kararları ile yazılı emrin, şeklen kontrolün yapılmasını müteakip Jandarma İstihbarat Teknik Analiz Sistemi üzerinden başlatma tutanağı tanzim edilerek Telekomünikasyon İletişim Başkanlığına (TİB) elektronik ortamda gönderilir.

İletişimin denetlenmesine ilişkin veriler; TİB tarafından kararın hukuki incelenmesi yapılmasını müteakip, Teknik İstihbarat Daire Başkanlığına gönderilir. Teknik İstihbarat Daire Başkanlığı tarafından da güvenli hatlar üzerinden birliklere gönderilir. İletişimin denetlenmesi faaliyetleri, merkezde İstihbarat Başkanlığınca, İl Jandarma Komutanlıklarında ise aidiyet numarası verilmiş İstihbarat personeli tarafından teknik

istihbarat odalarında yetkili komutanlıkların denetiminde TİB tarafından gönderilen veriler üzerinden icra edilmektedir. Görevlendirilen personel tarafından yapılan tüm işlemlerin kayıtları sistem üzerinden muhafaza edilmekte ve denetlenebilmektedir.

İletişimin denetlenmesi esnasında bir suç oluşmasına vakıf olunması veya kuvvetli belirtinin tespiti durumunda, idari tedbir sona erdirilerek adli işlemlerin başlatılması maksadıyla Cumhuriyet savcısı bilgilendirilmektedir.

3.3.3.3 Mahkeme Kararının Sona Ermesini Müteakip Yapılan İşlemler

İletişimin denetlenmesi faaliyeti mahkeme kararı veya İl Jandarma Komutanlığı tarafından sonlandırılmaktadır. Faaliyet esnasında herhangi bir suç oluşumuna vakıf olunması durumunda;

- Adli işlemlerin başlatılması maksadıyla Cumhuriyet savcısına bilgi verilir.
- Ayrıca yetkili komutanlıkların denetiminde iletişim içeriğine ait tüm kayıtlar en geç 10 gün içinde imha edilir.
- Karara ait tüm evrak tek dosyada arşivlenir.
- Faaliyet esnasında herhangi bir suç oluşumuna vakıf olunmaması durumunda ise; yine tüm kayıtlar imha edilir ve karar ait evrak tek dosyada arşivlenir.

3.3.4 Teknik Takip Faaliyetlerinin İcra Edildiği Ortam

Jandarma Genel Komutanlığınca gerçekleştirilen teknik takip faaliyetlerinin icra edildiği odaların her türlü fiziki güvenliği sağlanmış, bu odalara giriş çıkışlar sadece yetkili personel olmak üzere sınırlandırılmıştır. Ayrıca bu faaliyetlerin gerçekleştirildiği bütün birimlerde giriş-çıkış kayıt defterleri tutulmaktadır.

3.3.5 Teknik Takip Faaliyetlerinin Denetimi

Jandarma Teşkilat Görev ve Yetkileri Kanununun ek 5'inci maddesi, Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmeliğinin 24'üncü

maddesi ve İçişleri Bakanlığının, Jandarma ve Emniyet İstihbarat Birimlerinin Telekomünikasyon Yoluyla yaptıkları Önleyici İstihbarat Faaliyetlerinin Denetimine ilişkin görev ve Çalışma Yönergesi, esaslarına uygun olarak denetim faaliyetleri gerçekleştirilmektedir.

Bu kapsamda;

- o İçişleri Bakanlığı mülkiye müfettişlerince tüm istihbarat birimlerinde,
- o Jandarma Genel Komutanlığı Kurmay Başkanı başkanlığında oluşturulan heyet marifetiyle 6 aylık periyotlarla İstihbarat Başkanlığında,
- o İl Valisi tarafından zamana bağlı kalmaksızın, İstihbarat Başkanlığı heyeti tarafından da 3 yılda bir olmak üzere bütün İl Jandarma Komutanlıklarında teknik takip faaliyetlerinin denetimi yapılmaktadır.

Denetimlerde;

- a. Teknik takip odalarının güvenliğin alınması,
- b. Hizmet içi eğitim planlaması,
- c. Faaliyetlerin icrasında yasal prosedüre uyulması,
- d. Elde edilen kayıtların mevzuatta belirtilen amaçlara uygun kullanılması,
- e. Kayıtların saklanması ve korunmasında gizlilik ilkesine uyulması
- f. Görevlilerin uyacakları usul ve esaslarla ilgili düzenleyici metinlerin bulunmasına bakılır.

Ayrıca önleyici teknik takip faaliyetlerinde;

- ❖ Başlama, son verme ve imha tutanaklarının tutulması,
- ❖ İşlemlerin aidiyet numarası verilen kişiler tarafından yapılması,
- ❖ Tedbir sona erdiğinde dinlemenin içeriğine ilişkin kayıtların yetkili amirlerin denetiminde imha edilmesi,

- ❖ Bütün kayıtların denetimlerde ibraz edilmek üzere muhafazası,
- ❖ Kararda ve yazılı emirde belirtilmesi gereken hususlara talep formunda yer verilmesi sağlanır.

Teknik takip odalarına yetkisiz kişilerin girişini önleyecek tedbirlerin alınması, cep telefonu ve iletişime imkân veren diğer cihazların teknik takip odalarına girişini önleyecek tedbirlerin alınması ve Sıralı amirler tarafından gerekli denetimlerin yapılması konularında incelemeler yapılmaktadır.

3.3.6 Teknik Takip Faaliyetlerinin Sonuçları

Jandarma Genel Komutanlığınca; telekomünikasyon yoluyla iletişimin tespiti, dinlenmesi ve kayda alınması faaliyetleri, mahkeme kararları doğrultusunda Telekomünikasyon İletişim Başkanlığı tarafından gönderilen veriler üzerinden yetkilendirilmiş personel vasıtasıyla yasalara uygun olarak icra edilmektedir.

Jandarma; sorumluluk alanında tüm faaliyetlerini mevzuat çerçevesinde, insan odaklı, açık, şeffaf ve hesap verebilir bir anlayışla ve insan haklarına saygılı bir şekilde yürütme gayretini sürdürmektedir.

Jandarma Genel Komutanlığınca 2007 - 2012 yılları arasında gerçekleştirilen teknik takip faaliyetleri sonucunda elde edilen sonuçları ve bu sonuçların yıllara göre dağılımı aşağıdaki listelerde ayrıntılı olarak yer almaktadır.

J.Gn.K.lgınca 2007-2012 yılları arasında (6) yıllık dönemde; yapılan teknik takip faaliyetleri sonucunda;

- 533 silahlı terörist etkisiz hale getirilmiş,
- 34.594 şahıs hakkında adli işlem yapılmış,
- 3.406 göçmen şahıs yakalanmış,
- 14 (adet) makinalı tüfek,
- 257 (adet) uzun namlulu tüfek,
- 11 (adet) roketatar,
- 7.925 (adet) tabanca,
- 295.546 (adet) muhtelif çapta mühimmat,
- 294 (adet) el bombası,
- 158 (adet) el yapımı patlayıcı madde düzeneği,
- 811 (adet) fünüye,
- 541 (kg) plastik patlayıcı,
- 1.728 (kg) bomba yapımında kullanılan kimyasal madde,
- 1.839 (kg) eroin,
- 39.726 (kg) esrar,
- 112.956 (kök) hint keneviri,
- 334.419 (adet) sentetik hap,
- 12.000 (ton) akaryakıt,
- 42.757 (parça) tarihi eser,
- 8.262 (adet) kaçak hayvan,
- 21.096 (adet) sahte para,
- 7.235.104 (paket) sigara yakalanmıştır.

Ayrıca, son altı yıl içerisinde teknik imkanlar kullanılarak (208) kayıp şahıs bulunmuştur.

**Tablo 14- Jandarma Genel Komutanlığınca İcra Edilen Teknik Takip Faaliyetleri
Neticesinde Elde Edilen Sonuçlar**

SIRA NU.	ŞÜPHELİ VE MALZEME DURUMU	2007	2008	2009	2010	2011	2012	TOPLAM
1	YAKALANAN/ETKİSİZ HALE GETİRİLEN TERORİST	155	93	80	81	68	56	533
2	HAKKINDA ADLI İŞLEM YAPILAN ŞAHIS	5.417	6.729	7.542	5.870	3.651	5.385	34.594
3	GOÇMEN ŞAHIS	603	786	325	576	588	528	3.406
4	MAKİNALİ TÜFEK	0	2	4	1	5	2	14
5	UZUN NAMLULU TÜFEK	42	29	32	51	27	76	257
6	ROKETATAR	2	1	3	2	1	2	11
7	TABANCA (ADET)	2.525	1.534	2.419	665	439	343	7.925
8	MUHTELİF ÇAPTA MÜHİMMAT	61.218	53.313	135.365	18.690	10.248	16.712	295.546
9	EL BOMBASI (ADET)	89	27	62	26	38	52	294
10	EYP DÜZENEGİ (ADET)	25	9	27	34	5	58	158
11	FÜNYE (ADET)	139	134	179	161	119	79	811
12	PLASTİK PATLAYICI (GRAM)	21.317	13.681	39.555	11.340	6.800	448.350	541.043
13	BOMBA KİMYASALI (KG)	31	12	167	299	590	630	1.728
14	EROLIN (KG)	296	385	613	244	134	167	1.839
15	ESRAR (KG)	3.568	1.514	11.819	16.225	871	5.729	39.726
16	HİNT KENEVİRİ (KÖK)	0	18.086	0	0	0	94.870	112.956
17	SENTEKİK HAP (ADET)	74.043	125.372	87.826	29.797	3.108	14.273	334.419
18	AKARYAKIT (LT)	1.999.167	1.468.576	1.036.058	1.773.662	1.924.031	3.688.024	11.889.518
19	TARİHİ ESER (PARÇA)	11.438	5.781	13.774	2.849	3.447	5.468	42.757
20	KAÇAK HAYVAN (BÜYÜK-KÜÇÜKBAS)	1.176	704	460	1.192	638	4.092	8.262
21	SAHTE PARA (ADET)	3.181	446	537	238	16.472	222	21.096
22	SİGARA (PAKET)	182.292	249.065	1.336.264	473.014	701.862	4.292.607	7.235.104

3.4 Milli İstihbarat Teşkilatı

01/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 4'üncü maddesinde Milli İstihbarat Teşkilatı Müsteşarlığının 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 Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak.

b) Devletin milli güvenlik siyasetiyle ilgili planların hazırlanması ve yürütülmesinde; Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamak.

c) Kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için Milli Güvenlik Kurulu ve Başbakana tekliflerde bulunmak.

d) Kamu kurum ve kuruluşlarının istihbarat ve istihbarata karşı koyma faaliyetlerine teknik konularda müşavirlik yapmak ve koordinasyonun sağlanmasında yardımcı olmak.

e) Genelkurmay Başkanlığınca Silahlı Kuvvetler için lüzum görülecek haber ve istihbaratı, yapılacak protokole göre Genelkurmay Başkanlığına ulaştırmak.

f) Milli Güvenlik Kurulunda belirlenecek diğer görevleri yapmak.

g) İstihbarata karşı koymak,”

şeklinde belirtilmektedir.

MİT Müsteşarlığı bu görevlerini yerine getirirken, yine 2937 sayılı Kanunda belirtilen yetkileri kullanmaktadır. İstihbari faaliyetler çerçevesinde, 2937 sayılı Kanunda düzenlenen haber toplama kaynaklarından en önemli olanlarından biri de “iletişimin denetlenmesi” faaliyetleridir. İstihbarat alanında, suçla ilişkili dinleme faaliyetlerinin dışında özel bir dinleme yetkisi ihtiyacı olan istihbarat teşkilatlarının, ulusal güvenliğin

sağlanması amacıyla, demokratik hukuk devletine yönelik tehdit unsurlarına ilişkin olarak düzenli ve sistemli bilgi toplama ve değerlendirme ihtiyacı bulunmaktadır.

Bu ihtiyaçtan hareketle, başta Avrupa Birliği (AB) ülkeleri olmak üzere tüm yabancı ülkelerin ulusal güvenlik servisleri, istihbarat servis kanunlarında yer alan düzenlemeler çerçevesinde, iletişime müdahale konusunda muhtelif şekillerde yetkilendirilmişlerdir.

Aynı doğrultuda olmak üzere, MİT Müsteşarlığının da; İKK görevi kapsamında 04.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununda (CMK) belirlenen usul ve esaslar çerçevesinde yürütülmekte olan adli dinlemeye ilişkin görev ve yetkisinin yanı sıra, 2937 sayılı Kanunun 6'ncı maddesi ile düzenlenen iletişime istihbari amaçlı müdahale görev ve yetkisi bulunmaktadır.

Bu kapsamda, MİT Müsteşarlığınca yürütülen istihbari ve adli dinlemeye ilişkin olarak ilgili mevzuatta yer alan usul ve esaslar aşağıda sunulmuştur.

3.4.1 İstihbari Amaçlı İletişimin Denetlenmesi Faaliyetleri

23.07.2005 tarihli ve 25884 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren 5397 sayılı Kanunla; 2937 sayılı Kanunun 6'ncı maddesinde değişiklik yapılmış ve Teşkilatın görev alanına giren konularda istihbari amaçlı dinleme yapabilmesi hukuki zemine kavuşturulmuştur.

Ceza Muhakemesi Hukukunda soruşturmaya başlanabilmesi için, öncelikle suç işlendiğine ilişkin bir şüphenin mevcudiyetine ihtiyaç duyulmaktadır. Ancak, istihbari amaçlı dinleme faaliyetlerinde henüz bir başlangıç şüphesi ya da somut bir tehlike durumu bulunmamasına rağmen, telekomünikasyon yoluyla yapılan iletişime müdahale edilmektedir. Bu itibarla, istihbari amaçlı dinleme faaliyetleri ceza muhakemesinin soruşturma evresinden önceki bir dönemi içermektedir.

3.4.1.1 Kapsamı

MİT Müsteşarlığına 2937 sayılı Kanunun 4'üncü maddesi ile verilmiş görevlerin yerine getirilmesini teminen; Anayasa'nın 2'nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve

terörist faaliyetlerin önlenmesine ilişkin olarak, telekomünikasyon yoluyla yapılan iletişim tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması konularında yetki verilmiştir.

3.4.1.2 Kararı Vermeye Yetkili Makam

Telekomünikasyon yoluyla yapılan iletişimin istihbari amaçla tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması işlemleri hâkim kararı ile yapılabilmektedir. Bu konuda karar vermeye yetkili ve görevli hakim ise talepte bulunan birimin bulunduğu yer itibarıyla yetkili olan ve 3713 sayılı Terörle Mücadele Kanununun 10’uncu maddesine göre kurulan ağır ceza mahkemesinin üyesidir.

Ancak, “gecikmesinde sakınca bulunan hallerde MİT Müsteşarı veya yardımcısının yazılı emriyle” de telekomünikasyon yoluyla yapılan iletişimin tespitine, dinlenmesine, sinyal bilgilerinin değerlendirilebilmesine ve kayda alınabilmesine imkân tanınmıştır. Ayrıca, gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmi dört saat içinde yetkili ve görevli hâkimin onayına sunulmak zorundadır. Hâkim bu konudaki kararını en geç yirmi dört saat içinde verecek ve hâkim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılacaktır.

Diğer taraftan, ilgili mevzuatta bahse konu işlemlerin 04.07.1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyet Kanununun ek 7’nci maddesinin onuncu fıkrası uyarınca Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde Kurum başkanına doğrudan bağlı olarak “Telekomünikasyon İletişim Başkanlığı (TİB)” adıyla kurulan tek bir merkezden yürütüleceği, hususu düzenlenmiştir.

3.4.1.3 Kararın/ Yazılı Emrin İçeriği

Kararda ve yazılı emirde;

- Hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, Kullandığı telefon numaraları veya iletişim bağlantısını tespitte imkân veren kodundan belirlenebilenler,
 - Tedbirin türü, kapsamı ve süresi,
 - Tedbire başvurulmasını gerektiren nedenler,
- belirtilir.

3.4.1.4 Kararın Süresi

2937 sayılı Kanunun 6’ncı maddesinin dördüncü fıkrasında; “kararların en fazla üç ay için verilebileceği, bu sürenin aynı usulle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabileceği, ancak casusluk faaliyetlerinin tespiti ve terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hakimün üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebileceği hüküm altına almıştır.

3.4.1.5 Kararın Sona Ermesi

Dinleme süresinin sona ermesi veya gecikmesinde sakınca bulunan hallerde hakim tarafından yetkili amirin yazılı emrinin aksine karar verilmesi halinde, tedbir derhal kaldırılır.

Bu durumda, dinlemenin içeriğine ilişkin kayıtlar en geç 10 gün içinde yok edilir, durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.

3.4.1.6 Denetim

Bu maddede yer alan faaliyetlerin denetimi, sıralı kurum amirleri ve Başbakanlık teftiş elemanları tarafından yapılır.

3.4.1.7 Cezai Hükümler

2937 sayılı Kanunun 6’ncı maddesindeki hükümlere göre yürütülen dinleme faaliyetleri neticesinde elde edilen kayıtlar, anılan Kanunda belirtilen amaçlar dışında kullanılamaz. Elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik ilkesi geçerlidir. Bu ilkeye aykırı hareket edenler hakkında, görev sırasında veya görevden dolayı işlenmiş olsa bile Cumhuriyet savcılarınca “doğrudan” soruşturma yapılır.

Ayrıca, Kanunun 6’ncı maddesinde belirlenen usul ve esaslara aykırı olarak yapılan dinlemeler hukuken geçerli sayılmaz ve bu şekilde dinleme yapanlar hakkında 26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu (TCK) hükümlerine göre işlem yapılır.

3.4.2 Adli Amaçlı İletişimin Denetlenmesi Faaliyetleri

2937 sayılı Kanunun “Yetkiler” başlıklı 6’ncı maddesinin son fıkrası “Bu Kanunda yazılı görevlerin yerine getirilmesi sırasında genel zabıtaya tanınmış olan hak ve yetkilerin, MİT mensuplarından kimlere tanınacağı, yönetmelikte belirtilir.” hükmünü amirdir.

Anılan hüküm uyarınca yürürlüğe konulan ilgili yönetmelikte ise; “İstihbarata karşı koyma (Kontr/Espiyonaj) konularında görevli MİT personelinin genel zabıtaya tanınmış olan hak ve yetkilerin tamamını bizzat kullanacakları” hüküm altına alınmıştır.

Genel zabıta (kolluk); asıl olarak polis ve jandarmadan oluşmaktadır. Yukarıda belirtilen hükümler uyarınca İKK faaliyetlerinde görevli MİT personeli, kolluğa tanınan yetkileri haizdir.

CMK’ya göre, ceza yargılaması “soruşturma” evresiyle başlar. Cumhuriyet Savcısı tarafından hazırlanan iddianamenin mahkemece kabul edilmesiyle yani davanın açılmasıyla birlikte soruşturma evresi tamamlanır ve “kovuşturma” evresine geçilir.

CMK, soruşturma evresi içerisinde Cumhuriyet Savcısına kolluk görevlileri vasıtasıyla delil toplama görevi yüklemiştir. Bu bağlamda, İKK konularında görevli Teşkilat personeli soruşturma evresi içerisinde, yetkili ve görevli Cumhuriyet Savcısı tarafından soruşturma kapsamında delil elde etmek amacıyla kullanılan ve “koruma tedbirleri” adı verilen “yakalama, ifade alma, arama, el koyma” gibi işlemlerde görevlendirilebilecektir.

Bahse konu koruma tedbirlerinin bir kısmı ise “gizli müdahale” niteliğinde olup, bunlar arasında CMK 135-138’inci maddelerinde düzenlenmiş bulunan “Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi” ve 140’inci maddede yer alan “Teknik Araçlarla İzleme” sayılmaktadır.

Özetle; Cumhuriyet Savcısı tarafından soruşturmaya başlandıktan sonra, İKK faaliyetleri kapsamında “delil elde etmek amacıyla” iletişimin tespiti ve denetlenmesi ile teknik araçlarla izleme yöntemlerine de başvurulabilecektir.

3.4.2.1 Kapsamı

Telekomünikasyon yoluyla yapılan iletişimin CMK’nın 135’inci maddesi çerçevesinde denetlenebilmesi; bir suç dolayısıyla yapılan soruşturma ve kovuşturmada delil elde etmek amacıyla başvurulabilecek bir yöntemdir.

CMK’nın 135’inci maddesinin altıncı fıkrasında, iletişimin denetlenmesine hangi suçlar bakımından başvurulabileceği belirtilmiş olup, anılan fıkranın (a) bendinin 14’üncü alt bendinde Devlet Sırlarına Karşı Suçlar ve Casusluk (TCK madde 329, 330, 331, 333, 334, 335, 336, 337) suçları yönünden de iletişimin denetlenebileceği hüküm altına alınmıştır.

İletişimin CMK kapsamında denetlenmesi, sadece şüphelinin ya da sanığın iletişiminin denetlenmesi amacıyla uygulanabilecek bir yöntemdir. Şüpheli ve sanık kavramları CMK’nın 2’nci maddesinde tanımlanmıştır. Şüpheli ve sanık dışında kalan üçüncü kişiler hakkında ise CMK’nın 135’inci maddesinde düzenlenen yöntem uygulanamaz.

3.4.2.2 Dinleme Yasakları

CMK’nın 135/2 ve 136’ncı maddelerinde iletişimin denetlenemeyeceği iki durum belirtilmiştir. CMK’nın 135’inci maddesinin ikinci fıkrasına göre; “Şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda alınamaz. Kayda alma gerçekleşikten sonra bu durumun anlaşılması halinde, alınan kayıtlar derhal yok edilir”. Tanıklıktan çekinebilecek kişiler ise CMK’nın 45’inci maddesinde sayılmıştır.

CMK’nın 136’ncı maddesine göre ise; “Şüpheli veya sanığa yüklenen suç dolayısıyla müdafinin bürosu, konutu ve yerleşim yerindeki telekomünikasyon araçları hakkında, 135’inci madde hükmü uygulanamaz.” Müdafî (avukat) hakkındaki bu denetim yasağı şüpheli veya sanığa yüklenen suç dolayısıyla getirilmiş bir kısıtlamadır. Ancak, müdafinin de şüpheli veya sanık olması durumunda iletişiminin denetlenmesi mümkün olabilecektir.

3.4.2.3 Kararı Vermeye Yetkili Makam

İletişimin denetlenmesi kararını verme yetkisi “hâkim” ve “gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısına” aittir. Ancak, Cumhuriyet savcısı kararını derhal hâkimin onayına sunar ve hâkim en geç yirmi dört saat içinde kararını açıklar.

MİT Müsteşarlığının görev ve faaliyetleri kapsamındaki casusluk suçlarına ilişkin CMK kapsamındaki dinlemelerde de karar vermeye yetkili hâkim, 3713 sayılı Kanunun 10’uncu maddesine göre kurulan ağır ceza mahkemesinin üyesidir.

3.4.2.4 Kararın İçeriği

Kararda;

- Yüklenen suçun türü,
 - Hakkında tedbir uygulanacak kişinin kimliği,
 - İletişim aracının türü,
 - Telefon numarası veya iletişim bağlantısını tespiti imkân veren kodu,
 - Tedbirin türü, kapsamı ve süresi,
- belirtilir.

3.4.2.5 Kararın Süresi ve Uygulanması

CMK’nın 135’inci maddesi kapsamındaki dinlemenin süresi en çok üç aydır ve bu süre bir defa uzatılabilir. Ancak, örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak ise gerekli görülmesi halinde, hâkimin bir aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebileceği hüküm altına alınmıştır.

2937 sayılı Kanunun 6’ncı maddesinin ikinci fıkrasında “CMK’nın 135’inci maddesinin altıncı fıkrasının (a) bendinin (14) numaralı alt bendi [Devlet Sırlarına Karşı Suçlar ve Casusluk (TCK madde 329, 330, 331, 333, 334, 335, 336, 337) Suçları] kapsamında yapılacak dinlemelerin de Telekomünikasyon İletişim Başkanlığı (TİB) üzerinden yapılacağı” hüküm altına alınmıştır.

3.4.2.6 Kararın Sona Ermesi

CMK’nın 137’nci maddesinin üçüncü fıkrasında; iletişimin tespiti ve dinlenmesi yönündeki kararların iki şekilde sona ereceği belirtilmiştir. Buna göre;

- Dinleme kararının uygulanması sırasında şüpheli hakkında Cumhuriyet Savcısı tarafından kovuşturmaya yer olmadığına dair karar verilmesi halinde tedbire son verilir. Yani dinleme işlemi, Cumhuriyet Savcısını kamu davası açmak için yeterli delile ulaştırmamış ise kovuşturmaya yer olmadığı kararı ile birlikte tedbire de son verilecektir.

- Diğer taraftan, dinleme kararının gecikmesinde sakınca bulunan bir halden dolayı Cumhuriyet Savcısı tarafından verilmiş olması ve hâkim tarafından bu kararın onaylanmaması halinde, dinleme uygulamasına Cumhuriyet Savcısı tarafından derhal son verilecektir.

Yukarıda belirtilen hususlardan herhangi birinin gerçekleşmesi üzerine dinleme uygulamasına son verilmesi halinde, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet Savcısının denetimi altında en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilecektir.

Ayrıca CMK’da, dinlemeye ilişkin kayıtların yukarıdaki sebeplerden biri nedeniyle yok edilmesi halinde “ilgisine haber verme” mecburiyeti getirilmektedir. CMK’nın 137’nci maddesinin dördüncü fıkrası uyarınca; tedbirin yukarıda belirtilen sebeplerden birinin varlığı ile sona ermesi ve kayıtların yok edilmesi halinde, Cumhuriyet Başsavcılığının, soruşturma evresinin bitiminden itibaren en geç on beş gün içinde, tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgisine yazılı olarak bilgi vermek yükümlülüğü bulunmaktadır.

3.4.2.7 Cezai Hükümler

CMK’da belirlenen esas ve usuller dışında (istihbari amaçlı dinlemeler haricinde) bir başkasının telekomünikasyon yoluyla yaptığı iletişim dinlenemez ve kayda alınamaz.

Aksine hareket edenler hakkında, TCK’nın 132 vd. maddelerindeki müeyyideler uygulanır.

Ayrıca; CMK’nın 138’inci maddesinin ikinci fıkrasına göre; telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında tesadüfen yapılmakta olan soruşturma veya kovuşturma ile ilgisi olmayan, ancak CMK’nın 135’inci maddesinin altıncı fıkrasında sayılan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilmesi halinde, bu delil muhafaza altına alınacak ve durum derhal Cumhuriyet Savcılığına bildirilecektir.

3.4.3 İstihbari ve Adli Amaçlı İletişimin Denetlenmesi Tedbirlerinin Karşılaştırması

İletişimin istihbari amaçlı denetlenmesi ile CMK'nın 135'inci maddesi kapsamındaki adli dinleme faaliyetlerinin kısa bir karşılaştırmasının, konunun daha rahat anlaşılmasına katkı sağlayacağı değerlendirilmiştir. Bu çerçevede;

MİT Müsteşarlığının görev ve faaliyetleri kapsamında, telekomünikasyon yoluyla yapılan iletişimin gerek istihbari ve gerekse adli denetlenmesi kararlarını vermeye 3713 sayılı Kanunun 10'uncu maddesine göre kurulan ağır ceza mahkemesi hâkimleri yetkili ve görevlidir.

İstihbari dinlemelerde gecikmesinde sakınca bulunan hallerde MİT Müsteşarı ya da Yardımcısına yazılı emirle dinleme kararı verme yetkisi tanınmıştır. CMK kapsamındaki dinlemelerde ise gecikmesinde sakınca bulunan hallerde dinleme kararı verme yetkisi sadece ilgili Cumhuriyet Savcısına verilmiştir.

İstihbari dinlemelerin süresi en fazla üç ay olmakla birlikte, bu süre her defasında üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilmektedir. Diğer taraftan, casusluk faaliyetinin tespiti ve terör örgütünün faaliyeti çerçevesinde yapılan dinlemelerde hâkim kararının süresi üç aydan fazla olmamak üzere müteaddit defalar uzatılabilmektedir. CMK kapsamındaki dinlemelerin ise süresi en çok üç aydır ve bu süre ancak bir defa uzatılabilmektedir. Ancak, örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi halinde, her seferinde bir aydan fazla olmamak kaydıyla sürenin müteaddit defalar uzatılmasına karar verilebilmektedir.

İstihbari ve adli dinlemelerin her ikisi de Telekomünikasyon İletişim Başkanlığı (TİB) üzerinden gerçekleştirilmektedir.

İstihbari dinlemelerde, kişiler bakımından telekomünikasyon yoluyla yapılan iletişime müdahaleye bir sınırlama getirilmemiştir. CMK kapsamındaki iletişimin tespit ve dinlenmesinde ise, şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle ve müdafii ile arasındaki iletişimi kayda alınamamaktadır.

Adli dinlemelere ilişkin kararlarda; yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespiti imkân veren kodu ile tedbirin türü, kapsamı ve süresinin mutlaka yer

alması gerekmektedir. İstihbari dinlemelere ilişkin kararlarda ve yazılı emirlerde ise; tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenlerin yazılması zorunlu tutulmuştur. Bunun dışında, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespiti imkân veren kodunun yazılması zorunlu görülmemiş, ancak belirlenebilmeleri halinde tespit edilen bilgilere yer verilmesi yeterli görülmüştür.

İstihbari dinlemelerde ilgisine herhangi bir bildirim mecburiyeti bulunmamaktadır. CMK kapsamındaki dinlemelerde ise kovuşturmayla yer olmadığı kararı verilmesi ya da hâkimin aksi görüşü üzerine dinlemeye son verilerek kayıtların yok edilmesi halinde, Savcılık tarafından soruşturma evresinin bitimini takiben on beş gün içinde, tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgisine yazılı olarak bilgi verilmesi zorunluluğu bulunmaktadır.

İstihbari dinlemeler sonucunda elde edilen kayıtlar yargı organı önünde delil olarak kullanılmamakta, CMK kapsamındaki dinlemeler ise delil elde etmek amacıyla yapılmaktadır.

3.5 Telekomünikasyon İletişim Başkanlığı

3.5.1 Kuruluşu

Ülkemizde telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbirini tek merkezden yürütmek ve uluslararası standartlarda uygulanmasını sağlamak amacıyla, 03.07.2005 tarihinde TBMM’de kabul edilen 5397 Sayılı Kanunla 2559 Sayılı Polis Vazife ve Salahiyet Kanunu’nun ek 7’nci maddesine eklenen hükümler ile Telekomünikasyon İletişim Başkanlığı (TİB) kurulmuştur.¹⁸³

Başkanlık kurulmadan önce, iletişimin denetlenmesi kararlarını yerine getirmek için adli ve istihbari birimler (Emniyet, Jandarma ve MİT) telekomünikasyon şirketleri ile doğrudan irtibata geçmekte ve her bir kurum kendileri ile işletmeciler arasında var olan hatlar üzerinden dinlemeleri gerçekleştirmekteydi. Ancak bu yapı, hem ilgili kurumlar arasında koordinasyon ve faaliyetlerinin denetimi konusunda dağınıklığa neden olmakta hem de iletişimin denetlenmesi faaliyetlerinin hâkim kararları çerçevesinde gerçekleştirilip

¹⁸³ 5397 Sayılı Kanunun Gerekçesi.

gerçekleştirilmediği hususunda tereddütlere sebep olmaktaydı.¹⁸⁴ 5397 Sayılı Kanunla uygulamalardaki dağınıklığı gidermek ve kamuoyundaki tereddütleri bertaraf etmek amacıyla söz konusu faaliyetler tek merkezde toplanmıştır.¹⁸⁵

Yeni oluşturulan bu merkezle iletişime müdahale tedbirinin uluslararası nitelikteki ilke ve kararlar ile Anayasa’da belirtilen hükümlere uygun olarak yürütülmesinin sağlanması ve bireylerin özel hayatlarının gizliliği ile haberleşme hürriyetlerinin korunması açısından önemli bir güvence getirilmiştir.

Bu kapsamda TİB, hem adli mercilerin gereksinim duyduğu kanuni delillerin temini yönüyle hem de yetkili kurumların gerçekleştirdikleri dinlemelerin hukuka uygun olarak yürütülmesi konusunda çok önemli bir fonksiyon icra etmektedir.¹⁸⁶

İletişimin denetlenmesi işlemlerinin tek merkezli yürütülmesi, özellikle keyfiliğin önlenmesi bakımından son derece önemli bir güvence olarak kabul edilmekte ve TİB tarafından bu işlemlerin gerçekleştirilmesi de demokratik sistem açısından ileri bir gelişme olarak görülmektedir.¹⁸⁷

Başkanlığın çalışma usul ve esasları, 5397 sayılı Kanun gereğince Başbakanlık tarafından çıkarılan 10.11.2005 tarihli ve Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kurulu, Görev ve Yetkileri Hakkında Yönetmelikte düzenlenmiştir.

3.5.2 İdari Yapısı

Başkanlığın bağlı olduğu Bilgi Teknolojileri ve İletişim Kurumu düzenleyici ve denetleyici üst kurullar arasında yer almakta olup, kamu tüzel kişiliğine haiz, idari ve mali özerkliğe sahiptir. Görevlerini yerine getirirken bağımsızdır ve hiçbir organ, makam, merci veya kişi Kuruma emir ve talimat veremez.¹⁸⁸

¹⁸⁴ Geleri s.29.

¹⁸⁵ Geleri s.29.

¹⁸⁶ TBMM Araştırma Komisyonu Raporu, s. 39.

¹⁸⁷ Yardımcı, s. 273

¹⁸⁸ 2813 Sayılı Yasanın 5/1-2 nci fıkraları.

Bilgi Teknolojileri ve İletişim Kurumu¹⁸⁹ bünyesinde yer alan Başkanlık, doğrudan BTK Başkanına bağlı olarak faaliyetlerini yürütmektedir. Başkanlık, Telekomünikasyon İletişim Başkanı ile Hukuk, Teknik İşletme, Bilgi Sistemleri, İdari ve İnternet daire başkanlıklarından oluşmaktadır.¹⁹⁰

Kendi kurumları ile TİB arasında koordinasyonu sağlamak üzere Başkanlıkta Milli İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığının ilgili birimlerinden birer temsilci bulunmaktadır. Bu temsilciler Başkanlıktaki görevleri esnasında Başkanın talimatlarına ve Başkanlık tarafından belirlenen kurum içi düzenlemelere riayet ederler.¹⁹¹

Başkanlığa ilgili mevzuat ile verilen görevlerin gerektirdiği asli ve sürekli görev ve hizmetler teknik, hukukçu ve idari personelden oluşan “meslek personeli” ve “diğer personel” eliyle yürütülmektedir.

TİB Başkanı, 5651 Sayılı Kanunun ek 1’inci maddesinde¹⁹² yer alan hükme göre müşterek kararname ile atanmaktadır. TİB personeli ise, Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Yönetmeliği gereğince KPSS sınavında belli bir puanı geçenler arasından yazılı ve sözlü sınav yapılmak suretiyle Kuruma alınmaktadır.

Başkanlığın taşra teşkilatı bulunmamaktadır.

3.5.3 Görevleri

5397 Sayılı Kanunda belirtilen işlemler ve 5271 sayılı Kanunun 135’inci maddesi kapsamında yapılacak dinlemelerin tek bir merkezden yürütülmesi amacıyla kurulan Telekomünikasyon İletişim Başkanlığının (TİB) görev ve yetkileri 10 Kasım 2005 tarihli ve 25989 sayılı Yönetmeliğin 17’nci maddesinde belirtilmektedir. Buna göre Başkanlığın görevleri;

“ a) 2559 sayılı Kanunun ek 7 nci maddesi, 2803 sayılı Kanunun ek 5 inci maddesi ve 2937 sayılı Kanunun 6 ncı maddesi uyarınca, telekomünikasyon yoluyla yapılan

¹⁸⁹ 11/10/2008 tarihli ve 5809 Sayılı Kanunun 67/2 maddesinin “a” bendi ile Telekomünikasyon Kurumunun adı “Bilgi Teknolojileri ve İletişim Kurumu” olarak değiştirilmiştir.

¹⁹⁰ 09/09/2011 tarihli ve 28049 sayılı Yönetmelik değişikliği.

¹⁹¹ 10/11/2005 tarihli 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 Yönetmeliğin 16 ncı maddesi.

¹⁹² 24/10/2011 tarihli ve 661 Sayılı KHK’nin 80. maddesiyle ek cümle.

iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına yönelik iş ve işlemleri tek bir merkezden yürütmek,

b) 5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine yönelik iş ve işlemleri tek bir merkezden yürütmek,

c) (a) ve (b) bentleri kapsamındaki taleplerin bu Yönetmeliğe ve diğer ilgili mevzuata uygun olup olmadığını incelemek ve gerektiğinde yetkili mercilere başvuruda bulunmak,

d) (a) ve (b) bentleri uyarınca gerçekleştirilen işlemler sonucunda elde edilen verileri ve bilgileri ilgisine göre Millî İstihbarat Teşkilatı Müsteşarlığına, Emniyet Genel Müdürlüğüne ve Jandarma Genel Komutanlığına, talep etmeleri halinde mahkemeye ve Cumhuriyet başsavcılıklarına iletmek,

e) (Değişik:RG-7/8/2009-27312) Bu Yönetmelik çerçevesinde yapılacak tespit, dinleme, sinyal bilgilerinin değerlendirilmesi ve kayda alınması faaliyetleri ile 5651 sayılı Kanunla ve diğer mevzuatla verilen görevlerin ifasını olanaklı kılacak her türlü teknik alt yapının, kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşlar ve işletmeciler tarafından kurulmasını sağlamak, sağlamak, gerekli alt yapıyı kurmayan işletmecilerin cezalandırılması yönünde girişimde bulunmak,

f) (Değişik: RG-04/07/2007-26572)(1) 12 nci maddenin ikinci fıkrası ile 15 inci maddenin üçüncü fıkrası saklı kalmak kaydıyla, Başkanlık faaliyetleriyle ilgili olarak kamu kurum ve kuruluşları, kamu hizmeti veren kuruluşlar ile işletmecilerden gelen her türlü bilgi, belge ve kayıtların bilgi güvenliği kriterlerine uygun olarak arşivlenmesini sağlamak,

g) (Değişik:RG-7/8/2009-27312) Görev alanına giren konularla ilgili ulusal ve uluslararası alanda meydana gelen gelişmeleri takip etmek, bu kapsamda uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak ve gelişmelerin Başkanlık hizmetlerine yansıtılması için gerekli önlemleri almak,

h) Başkanlık faaliyetleri için yurt içinden ve yurt dışından teminine ihtiyaç duyulan her türlü malzeme, sistem, yazılım ve donanımı belirleyerek Kurum Başkanına bildirmek,

i) Başkanlık faaliyetleriyle ilgili olarak talep ettiğinde derhal Başbakana bilgi vermek,

j) (Ek:RG-7/8/2009-27312) 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun kapsamında Ulaştırma Bakanlığı, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşları ile içerik, yer ve erişim sağlayıcılar ve ilgili sivil toplum kuruluşları arasında

koordinasyon oluşturarak internet ortamında yapılan ve 5651 sayılı Kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye yönelik çalışmalar yapmak; bu amaçla, gerektiğinde, her türlü giderleri Kurumca karşılanacak çalışma kurulları oluşturmak,

k) (Ek:RG-7/8/2009-27312) İnternet ortamında yapılan yayınların içeriklerini izleyerek, 5651 sayılı Kanun kapsamına giren suçların işlendiğinin tespiti halinde, internet ortamında yapılan yayınlara erişimin engellenmesine yönelik olarak 5651 sayılı Kanunla öngörülen tedbirleri almak,

l) (Ek:RG-7/8/2009-27312) İnternet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirlemek,

m) (Ek:RG-7/8/2009-27312) Kurum tarafından işletmecilerin yetkilendirilmeleri ile mülkî idare amirlerince ticarî amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik esas ve usûlleri belirlemek,

n) (Ek:RG-7/8/2009-27312) İnternet ortamındaki yayınların izlenmesi suretiyle, 5237 sayılı Türk Ceza Kanununda yer alan; intihara yönlendirme (madde 84), çocukların cinsel istismarı (madde 103, birinci fıkra), uyuşturucu veya uyarıcı madde kullanılması kolaylaştırma (madde 190), sağlık için tehlikeli madde temini (madde 194), müstehcenlik (madde 226), fuhuş (madde 227), kumar oynanması için yer ve imkân sağlama (madde 228) suçları ile 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dâhil, gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak,

o) (Ek:RG-7/8/2009-27312) İnternet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgarî kriterleri belirlemek,

p) (Ek:RG-7/8/2009-27312) (n) bendinde sayılan suçların, internet ortamında işlenmesini konu alan her türlü temsili görüntü, yazı veya sesleri içeren ürünlerin tanıtımı, ülkeye sokulması, bulundurulması, kiraya verilmesi veya satışının önlenmesini teminen yetkili ve görevli kolluk kuvvetleri ile soruşturma mercilerine, teknik imkânları dâhilinde gereken her türlü yardımda bulunmak ve koordinasyonu sağlamak,

r) (Ek:RG-7/8/2009-27312) İnternet Kurulu ile gerekli işbirliği ve koordinasyonu sağlamak; İnternet Kurulunca izleme, filtreleme ve engelleme yapılacak içeriği haiz

yayınların tespiti ve benzeri konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları almak,

s) (Ek:RG-7/8/2009-27312) (Değişik:RG-9/9/2011-28049) İlgili mevzuat kapsamında hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararlarını uygulamak ve buna ilişkin iş ve işlemleri yürütmek,

t) (Ek:RG-7/8/2009-27312) İçeriği (n) bendinde belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsan bile, içeriği çocukların cinsel istismarı (madde 103, birinci fıkra) ve müstehcenlik (madde 226) suçlarını oluşturan yayınlara ilişkin olarak resen erişimin engellenmesi kararı vermek ve bu kararı, erişim sağlayıcısına bildirerek gereğinin derhal ve en geç kararın bildirilmesi anından itibaren yirmidört saat içinde yerine getirilmesini istemek,

u) (Ek:RG-7/8/2009-27312) (t) bendine göre verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi hâlinde, Cumhuriyet başsavcılığına suç duyurusunda bulunmak,

v)(2) Kanunlarla verilen diğer görevleri yerine getirmek.”

şeklinde sayılmıştır.

Görüldüğü üzere, Başkanlığın 5397 ve 5271 sayılı kanunlar kapsamındaki iletişimin denetlenmesi faaliyetlerinin yürütülmesine dair görevlerinin yanı sıra, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun kapsamında da görevleri bulunmaktadır.

Ayrıca Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çerçevesinde Başkanlığa yeni görevler verilmiş olup Ulaştırma, Denizcilik ve Haberleşme Bakanlığı’nın 6 Şubat 2013 tarihli oluru ile Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Başkanlığa kurulması ve Başkanlıkça işletilmesi uygun görülmüştür.

İlgili mevzuat hükümlerinden de anlaşılacağı üzere, Başkanlığın yasa dışı dinleme yöntemlerinden biri olan ortam dinlemesi ve ortam dinlemesi yapanların tespitine yönelik görevi bulunmamaktadır.¹⁹³

¹⁹³ TİB’in 15.03.2013 tarihli ve 86122112-090.01.00-2013.152186 sayılı yazısı ve ekleri.

3.5.4 Kararların Uygulanması

23 Temmuz 2006 tarihinde faaliyetlerine başlayan Telekomünikasyon İletişim Başkanlığı 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun ek 7'nci maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5'inci maddesi, 01.11.1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 6'ncı maddesi ile 5271 sayılı Ceza Muhakemesi Kanununun 135 ilâ 138'inci maddeleri uyarınca telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine yönelik iş ve işlemlerin hakim kararları çerçevesinde yerine getirilmesini sağlayan bir birimdir.

Başkanlığın kurulmasıyla, hem önleyici hem de adli amaçlı iletişimin denetlenmesi faaliyetlerinin yürütülmesi tek merkezde toplanmıştır.

Ancak tek merkezlilik, dinlemelerin bu merkez tarafından yapıldığı şeklinde anlaşılmamalıdır. Oluşturulan bu yeni sistemde Başkanlığa dinleme yetkisi verilmeyip, dinlemeyi gerçekleştirecek kurum ile ilgili işletmeci arasındaki koordinasyonu sağlamak görevi tevdi edilmiştir.¹⁹⁴

Nitekim 10.11.2005 tarihli yönetmelikte kararların işletmecilere gönderilemeyeceği ve söz konusu kararların ilgili kurum görevlileri ve Başkanlık tarafından yerine getirileceği belirtilmiştir¹⁹⁵ ve 14 Şubat 2007 tarihli Yönetmelik ile Başkanlığın işletmecilerle ilgili tüm çalışmaları yaparak, bu Yönetmeliğin 6'ncı maddesine göre düzenlenmiş kararlar doğrultusunda verilere erişim ile ilgili işlemleri yürüteceği hükmü getirilmiştir.¹⁹⁶

Bu kapsamda yetkili ve görevli hâkimlerce verilen adli ve önleyici iletişimin denetlenmesi kararları ile gecikmesinde sakınca bulunan hallerde hâkim onayına sunulmak üzere verilen adli ve önleyici yazılı emirler ilgili kolluk birimleri tarafından elektronik ortamda Başkanlığa gönderilmektedir. Kolluk tarafından elektronik ortama aktarılan

¹⁹⁴ Geleri, s. 30

¹⁹⁵ 10/11/2005 tarihli 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 Yönetmeliğin 14 üncü maddesi.

¹⁹⁶ 14 Şubat 2007 tarihli ve 26434 sayılı Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin 9 uncu maddesi.

veriler ile mahkeme kararlarındaki bilgilerin kontrolü, Başkanlıkta görevli uzman hukukçular tarafından gerçekleştirilmektedir.¹⁹⁷

Telekomünikasyon yoluyla yapılan iletişimin denetlenmesine ilişkin kararlar uygulanmadan önce mevzuatta yazılı unsurlar bakımından şekli incelemeden geçirilmektedir. Söz konusu kararlar, ilgili kanunlarda ve bunların uygulanması ilişkin yönetmeliklerde belirtilen hususlar bakımından incelenmektedir.

Mevzuat bakımından kararda bulunması zorunlu olan hususlarda bir eksiklik tespit edildiği takdirde, ilgili mevzuat hükümleri gereğince Başkanlıkça karara itiraz edilmektedir. Ancak kararlara yapılan itiraz, mevzuat gereğince dinlemeye ilişkin kararların uygulanmasını geri bırakmamaktadır. Ayrıca itiraz sadece şekli eksikliklere ilişkin olup, Başkanlığın esasa yönelik itiraz yetkisi bulunmamaktadır.¹⁹⁸

¹⁹⁷ TİB'in 15.03.2013 tarihli ve 86122112-090.01.00-2013.152186 sayılı yazısı ve ekleri.

¹⁹⁸ Kunter, Yenisey, Nuhoğlu, s. 814.

DÖRDÜNCÜ BÖLÜM

TEKNİK UYGULAMALAR, YÖNTEMLER VE TEDBİRLER

4.1 Kavramlar ve Tarihsel Gelişim

Bilimin açtığı çığırdan doğup hızla hayatımızın her alanına giren teknolojik yeniliklerin bizlere sağladığı sayısız kolaylıklar, yaşam kalitemizi artırma yönündeki katkıları, yadsınamaz bir gerçek olarak önümüzde durmaktadır. Artık pek azımız bir tanıdığıyla buluşma saatini ve yerini önceden sıkı sıkıya kararlaştırıyor. Yine artık evinde bulamadığı yakınına mahalle bakkalından soranların sayısı da yok denecek kadar az. Cebinde bir telefonu olan kimse arabası bozulunca dağ başında kalmaktan, kilometrelerce yolu yürümek zorunda kalmaktan korkmuyor. Bilmediğimiz bir yere gittiğimizde yanımızda navigasyon cihazı elimizde bir adres olması yolumuzu bulmamız için yeterli oluyor. Hiç gitmediğimiz ülkeleri, hiç görmediğimiz şehirleri sokak sokak tanıyabilmemiz mümkün günümüzde. Sosyal medya hayatımızı çoktan kuşattı bile, eve gelen misafirlere albümleri heyecanla çıkarıp göstermeye gerek kalmadı, zaten pek çoğumuzun evinde artık albüm de kalmadı. Bundan otuz yıl öncesinin bir oda dolusu bilgisayarının toplam işlem kapasitesine ve kocaman bir televizyonunun çözünürlüğüne sahip küçük aletler artık elimizin altında. Alışveriş evden dışarı çıkmaya gerek kalmadan halledilebiliyor, eskiden koca bir günü dolduran faturaları yatırma çilesi işten sayılmıyor. Bulaşık makinaları, buzdolapları dahi akıllanıyor gitgide. Yakın gelecekte bugün çok aşına olduğumuz akıllı telefonlar gibi akıllı evler de hayatımızda sıradanlaşacak.

Teknolojinin hayatımıza kattıklarından ufak bir kaç bahisle konumuza bir girizgâh yapmak istedik. Peki, bizleri pek çok çileden azade eden teknoloji gerçekten de tamamen teslim olacağımız güvenli bir mecra mı? Güvenlik dünyasında yaygın kanaat, tıpkı her nimetin bir külfeti olduğu gibi, her kolaylığın da bir zaafı beraberinde getireceğidir. Yani teknoloji hayatın her alanına girdikçe, suiistimallere de kapılar aralanmakta, hatta bazen ardına kadar açılmaktadır. Teknolojiyi hayatımızdan tümüyle çıkararak yaşamayı düşünmediğimiz takdirde onu bilinçli kullanmayı öğrenmeli, gülü sevdiğimiz için dikenine katlanmak yerine dikenlerinden sakınabileceğimizi bilmeliyiz. Teknolojinin iyi-kötü ayırt etmeden herkese kucak açtığı, yani bize sağladığı kolaylıkları farklı güdülerle hareket edebilecek şahıslar için de sağladığını unutmamalı, kendi kişisel mahremiyet ve özel hayatımız için en üst seviye duyarlılığı ilk önce yine kendimiz göstermeliyiz.

Teknolojinin hayata bu denli girmesindeki temel sebep, onun bizim en temel ihtiyaçlarımızdan biri olan haberleşme ihtiyacımıza en üst seviyede cevap vermesidir. Uzak mesafelere oralara fiziken gitmeden haber götürmek ve oralardan haber alabilmek, bunu yapacak hızlı bir ulak bulmak, insanın hep arayışı olagelmıştır. Eski devirlerde insanlık zaman geldi dumanı kullandı bu uğurda. Belki bu yoldaki en büyük katkılardan biri yazının icadıyla beraber atın ehlileştirilmesi oldu. Zaman geldi bir posta güvercininin kanadında uçuruldu haberler. Görece yakın devirlerde batıdaki Rönesans ve Reform hareketlerinin tetiklediği bilimsel arayışlar 18. Yüzyıldan itibaren karşılığını buldu ve Coulomb¹⁹⁹, Ampere²⁰⁰, Ørsted²⁰¹, Faraday²⁰² gibi dâhiler; elektrik, manyetik ve endüksiyon prensiplerini ortaya koydular. 1838’de Samuel Morse’un kendi adıyla anılan alfabeyi ve kullanışlı bir elektrik telgrafını icat edip bir araya getirmesiyle haberleşmede yeni bir döneme geçilmiş ve tüm dünyaya telgraf şebekeleri yayılmaya başlamıştı.²⁰³ Aynı yüzyılın sonlarına doğru telsiz (kablosuz) haberleşmenin de yolları aranmaya başlamış, bunun için elektrostatik, endüksiyon ve elektrik prensipleri kullanılarak denemeler yapılmıştı. Özellikle endüksiyon ve elektrik yoluyla kablo kullanmadan belli mesafelere telgraf sinyalleri iletmekte başarı sağlanmışsa da bu metotlar pratiklikten bir hayli uzaktı.²⁰⁴ 1865 yılında James Clerk Maxwell elektrik ve manyetik yasaları üzerine yaptığı çalışmalar sonucu adeta büyük bir resmindeki eksik parçayı tamamladı ve o güne değin bilinen fizik yasalarına eşsiz bir katkı yaparak elektrik ve manyetik teorisini birleştirdi. Bu birleşmeden elektromanyetik dalgaların varlığının teorik ispatı doğmuş oldu.²⁰⁵ Bu dalgaların varlığını deneysel olarak ispatlayan ise 1886 yılında Heinrich Hertz oldu.²⁰⁶ Daha sonraları pek çok bilim adamı ve mühendis tarafından kablosuz iletişimde elektromanyetik dalgalardan yararlanılması yönelik çalışmalar yürütüldü. 1895 yılından itibaren başladığı çeşitli mesafelerdeki denemelerinin ardından 1901 yılında Guglielmo Marconi ilk transatlantik telgraf haberleşmesini elektromanyetik dalgalar marifetiyle

¹⁹⁹ Charles Augustin de Coulomb (1736 –1806)

²⁰⁰ André Marie Ampère (1775–1836)

²⁰¹ Hans Christian Ørsted (1777 –1851)

²⁰² Michael Faraday (1791 – 1867)

²⁰³ Lewis Coe, *The Telegraph: A History of Morse's Invention and Its Predecessors in the United States*, McFarland (2003).

²⁰⁴ R. W. Simons, Guglielmo Marconi and Early Systems of Wireless Communication, *Gec Review*, Vol. 11, No.1 (1996), s. 39-40.

²⁰⁵ John David Jackson, *Classical Electrodynamics- Third Edition*, John Wiley & Sons, Inc. (1998), s.237-239.

²⁰⁶ Simons, s. 38-39.

gerçekleştirdi ve haberleşmede yeni bir devri başlatmış oldu.²⁰⁷

Bilimsel gelişmelere paralel olarak haberleşme ve kayıt imkânları oluşup²⁰⁸, geliştikçe ortaya çıkan haberleşme ve kayıt cihazları zaman içerisinde haber alma maksatlı da kullanılmaya başlamıştır. Özellikle II. Dünya Savaşı ve takip eden Soğuk Savaş yıllarında, teknoloji bu yöndeki istekleri karşılayacak şekilde evrilmiştir. Sonuç olarak bugün gerek kişilerin haberleşme içeriklerine, gerekse bulundukları ortamlara müdahale edilmesine olanak sağlayan bir takım imkânlar ortaya çıkmıştır.²⁰⁹

Haberleşme cihazı olarak ele aldığımız cihazlar üzerlerinde en az bir anten taşıyor ve elde ettikleri verileri başka bir yere gönderirler. Bu cihazlara bu sebeple *açık devre cihazlar*²¹⁰ da denir. Kayıt cihazı olarak adlandırabileceğimiz cihaz veya sistemlerde ise sinyallerin elektriksel olarak iletildiği ve bilgilerin sistem dâhilindeki bir yerde işlendiği görülür. Bu tür cihazlar, üzerlerinde anten taşımadıkları ve herhangi bir dalga yaymadıkları için *kapalı devre cihazlar* olarak adlandırılır.

Teknik bir takım ayrıntılara girmeden önce “böcek” tabirine açıklık getirilmesi gerekmektedir. “Böcek nedir?” veya “Neye böcek denir?” sorusunun cevabını şu şekilde verilebilir: *Üzerindeki alıcı (mikrofon/kamera) vasıtasıyla algıladığı ortam verisini (ses/görüntü) başka bir merkeze aktaran gizlenmiş veri cihazlarına böcek denir.*

Bu tanımdan hareketle ortam verisinin²¹¹ temininin sabit olduğu durumlarda bir böceğin varlığından söz edebilmek için şu üç şart aranmalıdır.

- **Varlık:** Ortam verisini algılamak üzere yapay olarak yerleştirilmiş bir cihazın var olması.
- **Gizlilik:** Bu cihazın gizli veya gizletilmiş (kamufle) olması.
- **Aktarma:** Bu cihazın algıladığı veriyi başka bir yere aktarıyor olması.

²⁰⁷ Simons, s.41-46.

²⁰⁸ Jonathan Stern, The Audible Past: Cultural Origins of Sound Reproduction, Duke University Press (2003), s.137-177

²⁰⁹ Robert Louis Benson, A History of U.S. Communications Intelligence during World War II: Policy and Administration, United States Cryptologic History, Series IV, Volum 8, Center For Cryptologic History National Security Agency (1997), s.80-90.

²¹⁰Constantine A. Balanis, Antenna Theory: Analysis and Design – Third Edition, John Wiley & Sons, Inc. (2005), s.1-3, s.11-14

²¹¹ “Ortam Verisi”, ses veya görüntü veya her ikisi anlamında kullanılmaktadır.

4.2 Teknik Dinleme ve İzlemeler

Kişilerin bilgileri dâhilde veya olmadan ortamlarının izlenmesi ve/veya dinlenmesi kimi durumlarda kayda alınması **takip** olarak adlandırılmaktadır. Bu faaliyetlerin teknolojik imkânlar kullanılarak yapılması, kişilerin görüşmelerinin, irtibatlarının, konumlarının vs. kayıt altına alınmasına **elektronik takip** denmektedir. Teknik olarak elektronik takip; İşitsel Takip, Görsel Takip, Sanal Takip, Konum Takibi gibi çeşitli başlıklar altında incelenebilir.²¹² Elektronik takibin kolluk birimlerince icra edilmesi durumunda buna teknik takip/izleme denmektedir, ancak burada işitsel takip için *dinleme*, görsel takip için *izleme* terimleri kullanılacak ve *takip* terimiyle ile her ikisi birden kastedilecektir. Dinleme ve izleme derken takip kavramı yalnızca teknolojik boyutuyla ele alınmaktadır.

Dinleme ve İzlemeler teknik olarak dört alt başlıkta toplanabilir:

- Cihazlı Takipler
- Şebeke Takipleri
- Suiistimalle Takipler
- Akustik Dinlemeler

4.2.1 Cihazlı Takipler

Takibin ortama yapay olarak yerleştirilmiş bir cihazla yapılmasıdır. Burada yapaydan kasıt dinleme ve izleme amacına yönelik bir cihazın kasten ortamda bulunması veya yerleştirilmiş olmasıdır. Bu bir toplantı sırasında bir katılımcının cebinde getirdiği basit bir kayıt cihazı olabileceği gibi, daha inşaat aşamasında binanın kolonlarına yerleştirilmiş karmaşık bir böcek de olabilir.²¹³

Elektronik takip cihazlarının kayıt cihazları ve haberleşme cihazları olmak üzere iki ana türe indirgenebileceğinden bahsedilmişti. Buna göre cihazlarla yapılan dinleme ve izlemeleri de ikiye ayrılabilir.

- Kapalı Devre Cihazlarla Dinleme ve İzlemeler

²¹² Rachel Simpson, Listening Devices And Other Forms Of Surveillance: Issues And Proposals For Reform, Briefing Paper No 20/97, s.2-5.

²¹³ Peter Wright, Spycatcher: The Candid Autobiography of a Senior Intelligence Officer. New York: Viking Penguin Inc. (1987), s.292-294.

- Açık Devre Cihazlarla Dinleme ve İzlemeler

4.2.1.1 Kapalı Devre Cihazlarla Dinleme ve İzlemeler

Elektromanyetik, ses vb. yayın yapmayan, tamamen elektriksel (elektrik kablolarıyla) veya optoelektriksel olarak (fiberoptik kablolarla) kapalı bir sistemde çalışan cihazlar veya sistemlerle yapılan dinleme ve izlemelerdir. Ses kayıt cihazları, video kameralar, kapalı devre televizyon sistemleri(CCTV), MOBESE sistemleri bunlara örnek teşkil etmektedir. Bu cihazları üç alt kategoride incelemek mümkündür.

- Kayıt Cihazları
- Kayıt Sistemleri
- Kapalı Devre Böcekler

4.2.1.1.1 Kayıt Cihazları

Elde ettiği ses ve/veya görüntüyü kendi üzerindeki bir hafıza birimine yazan cihazlardır. Video kameralar, ses kayıt cihazları (Şekil 4), ses kaydı yapabilen mp3 çalarlar bu türe örnek teşkil ederler.



Şekil 4. Sıradan Ses Kayıt Cihazları

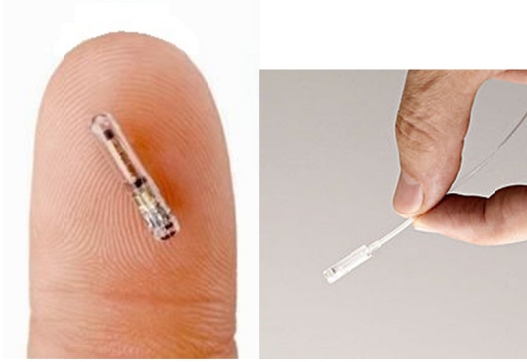
Ortam verilerinin gizlice kayıt altına alınması sıradan bir kayıt cihazı saklı kullanılmak suretiyle gerçekleşmiş olabilir. Diğer taraftan tamamen kişilerin gizli kayıt altına alınmalarına yönelik üretilmiş cihazlar da piyasada çeşitli sayı ve türde mevcuttur. Bu gizli cihazlara, ya farklı bir alet süsü verilmiş (kalem, gözlük, anahtarlık vs. (Şekil 5)) olabilmekte, ya da bunlar fark edilemeyecek kadar küçük (Şekil 6) ya da iyi saklanmış olmaktadır. Ancak belirtmek gerekir ki, bu tür cihazlar veri aktarımı yapmadıklarından, yukarıda yapılan *böcek* tanımı içerisine girmezler. Bu sebeple bunlar, belirtildiği üzere; *gizli ses kayıt cihazı*, *gizli kamera* ya da genel manada *gizli kayıt cihazı* şeklinde

adlandırılmalıdır.



Şekil 5. Araba Anahtarı Şeklinde Gizli Ses Kayıt Cihazı – Anahtarlık Kamera

Bu tür kayıt cihazlarının tespiti oldukça zordur. Herhangi bir yayın (elektromanyetik veya optik) yapmadıkları için sıradan tespit cihazlarıyla bulunamazlar. Genelde pil ile çalışırlar ama nadiren bağlı bulundukları bir cihazdan veya şebekeden de enerji alabilirler. Dışarıya yayın yapmadıkları için birkaç gün aralıksız çalışabilecek kadar pil ömürleri olabilir.



Şekil 6. Minyatür Kamera ve Mikrofon

Bu cihazları tespit için Yarıiletken Tespit Detektörleri (NLJD: Non-Linear Junction Detector) kullanılmaktadır. Ancak bu detektörlerin pek çok yarıiletkenin bulunduğu bir ortamda birçok yanlış alarm vermesi oldukça muhtemeldir. Bunun yanı sıra paslı inşaat demirleri ve demirler arası bağlantılar da yanlış alarmlara sebep olabilmektedir. Bu tür cihazların tespitinde ayrıca X-Ray, Holografik Radar yöntemleri ve Kızılötesi kameralar da

kullanılmaktadır.

4.2.1.1.2 Kayıt Sistemleri

Mağazalarda, AVM’lerde, çeşitli kurum ve kuruluşlarda bulunan kapalı devre kamera sistemleri (CCTV) (Şekil 7); kent yönetim sistemlerinde kullanılan MOBESE, EDS, bina içi haberleşmede kullanılan interkom telefonları en bilinen örnekleridir. Kamera veya kayıt cihazının gizlenmesi halinde böyle bir sistem gizli bir izleme/dinleme aracına dönüşebilir. Bilinen anlamda bir interkom şebekesi (bina içi telefon şebekesi) ortama gizlice döşenmiş olabilir. Yine var olan bir kapalı devre kayıt sistemi kişilerin bilgisi haricinde çalıştırılıyor olabilir. Bu sistemlerde alınan ses veya görüntü sistemin kendi iletim hattı üzerinden işleme birimine gönderilir ve orada işlenebilir (izlenebilir/dinlenebilir/kaydedilebilir). Ortama herhangi bir sinyal yayılmadığı için bu prensiple çalışan gizli sistemlerin sıradan verici tespit cihazlarıyla tespiti mümkün değildir.



Şekil 7. CCTV Kameraları

4.2.1.1.3 Kapalı Devre Böcekler

Kapalı devre çalışan böcekler elektromanyetik, optik, ses vs. yayın yapmadan, işledikleri veriyi ortamda zaten var olan bir iletim hattı üzerinden gönderebilirler. Algılanması zor olmamakla beraber genelde gözden kaçırıldığı için bir tehdit oluşturmaktadır.

a. Telefon Hattı Böcekleri

Algıladıkları ortam verilerini bağlı bulundukları ve enerjilerini temin ettikleri telefon şebekesi üzerinden aktaran böceklerdir. Belli bir mesafe içerisinde gönderilen veriyi telefon hattından alıp işleyen bir alıcı bulunmalıdır. Örneğin telefon hattı böceği üzerindeki mikrofon vasıtasıyla algıladığı ortam sesini FM modüli bir şekilde paralel bağlandığı telefon hattı üzerinden yollar. Böyle bir böcek telefon prizleri içerisine

yerleştirildiğinde enerjisini de telefon şebekesinden aldığı için uzun süre anlaşılmadan çalışabilir. Diğer taraftan bu böceklerin şebeke üzerindeki etkilerinden yararlanılarak tespit edilebildikleri bilinmektedir.²¹⁴

b. Şehir Şebekesi Böcekleri

Güç hattı böcekleri elde ettikleri ortam verilerini modüle ederek bağlı bulundukları şehir şebekesi üzerinden aktarırlar. Çalışmak için ihtiyaç duydukları enerjiyi de bu şebekeden sağlarlar. Aynı şebekeye bağlı ve belli bir mesafe içerisinde gönderilen veriyi alıp işleyen bir alıcı bulunmalıdır. Enerjisini şebekeden aldığı için uzun süre sorunsuz çalışabilir. Şebeke üzerindeki etkilerine bakılarak kolayca tespit edilebildikleri bilinmektedir.

4.2.1.2 Açık Devre Cihazlarla Dinleme ve İzlemeler

Açık devre cihazlar üzerlerindeki verici yapısı (anten) veya yapılarını kullanarak elde ettikleri verileri dışarıdaki alıcı veya alıcılara aktarabilen cihazlardır. Bu cihazların gizli olarak çalışanlarına *açık devre böcek* denilmektedir. Bunlar aslında birer haberleşme cihazıdır. Kullanılmaları daha kolay, veri iletme mesafeleri daha fazla oldukları için böceklerin büyük çoğunluğu bu tür açık devre cihazlardır.

4.2.1.2.1 Optik Böcekler

Aldığı veriyi ışığa veya optik palsa dönüştürerek aktaran cihazlardır. Bir lamba veya florasan içerisine gizlenmiş bir optik böcek ortam verilerini modüleli ışık titreşimleri şeklinde dışarıya aktarır, fakat bu titreşimler göz tarafından fark edilemez.

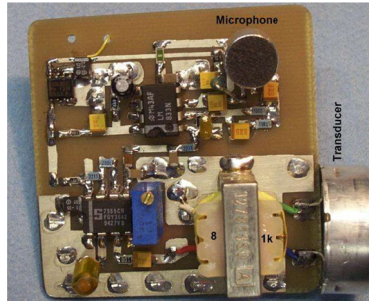
Lazerli dinleme cihazları²¹⁵ da bu alandaki örneklerdendir. Ortam verisini alan verici verileri lazerle kendi ışık hattı üzerinde hizalanmış lazer alıcısına gönderir. Lazerli dinleme cihazları oldukça maliyetli, kullanması zor ve bulunmaları kolay olduğu için pratikte pek kullanım alanı bulamadıkları düşünülmektedir.

²¹⁴ Robert Gruber, Physical and Technical Security: An Introduction, Thomson and Delmar Learning (2006), s. 297-299.

²¹⁵ Bu cihazlar “Lazer Dinlemesi” ile karıştırılmamalıdır.

4.2.1.2.2 Ultrasonik²¹⁶ Böcekler

Aldığı veriyi duyma bölgesinin üstündeki (20 kHz üstü) ses dalgalarına çevirerek ileten cihazlardır (Şekil 8). Ultrasonik bir vericinin gönderdiği verinin yakın bir noktada bir alıcı tarafından işlenmesi gerekir, zira ses dalgaları havada çok uzak mesafelere ilerleyemezler, ayrıca etraftaki cisimlerden fazlaca saçılırlar. Bununla birlikte ortam verilerini akustik bir iletken kullanarak (metal aksam, kalorifer borusu vs.) aktaran böcekler de bulunabilir. Ayrıca sualtında da görece uzak mesafelere yayın yapabilirler. Bu böceklerin sıradan böcek tarama sistemleriyle algılanması zordur. Ortamda ultrason yayını olup olmadığı ancak ultrason detektörleriyle anlaşılır. Ayrıca kimi hayvanların da bu frekanslardaki seslere duyarlı olduğu bilinmektedir.



Şekil 8. Ultrasonik Böcek Devresi

4.2.1.2.3 Radyo Frekans²¹⁷(RF) Böcekler

En çok bilinen ve genelde böcek denilince ilk akla gelen cihazlardır. Topladıkları verileri üzerlerindeki anten yapısı/yapıları sayesinde RF sinyallerine çevirerek iletirler. Oldukça küçük veya başka bir alet formunda veya içerisine gizlenmiş olarak bulunabilirler. Kullanılan frekans bandı ve protokoller göz önüne alınarak şu şekilde sıralanabilirler.

- GSM Böcekler
- Wi-Fi Böcekler
- Diğer...

²¹⁶ Ultrason bir çeşit akustik dalgadır. Akustik dalgalar, herhangi bir cismin titreşmesi veya iki cismin çarpışması, sürtüşmesi gibi mekanik bir sebepten ortama enerjinin titreşim şeklinde yayılmasıdır. Akustik dalga spektrumunda genellikle 20 Hz altı infrason, 20 Hz – 20 kHz aralığı - insan kulağı tarafından algılanabildiği için - ses, 20 kHz üstü ise ultrason şeklinde anılır. Ultrason dalgaları sonar, yön bulma, hareket, hız ve cisim sensörleri gibi uygulamaların yanı sıra tıbbi görüntüleme amaçlı da kullanılmaktadır.

²¹⁷ Elektromanyetik dalgaların telsiz haberleşmesinde kullanılan kısmına Radyo Frekans (RF) dalgaları denmektedir. Elektromanyetik dalgalar hakkında bilgi için Frekans Spektrumu bölümüne bkz.

a. GSM Böcekler

Bu böcekler aslında bir nevi cep telefonudur. Uzaktan aranarak, SMS mesajı, hareket, ses ya da ışık ile aktive olabilirler. Sürekli aktif olmadıkları ve cep telefonu gibi davrandıkları için bulunmaları oldukça zordur. Ortam verilerini GSM protokolü ile cep telefonu şebekesini kullanarak belirlenen bir noktadaki alıcıya (telefon, bilgisayar vs.) mesafe sınırı olmazsınız iletebilirler.²¹⁸ Boyutları oldukça küçüktür, sadece dinleme yapanlarının yanı sıra 3G üzerinden görüntü aktaranları da mevcuttur (Şekil 9). Bu böceklerin temini ve kullanılması oldukça kolay olduğu için popüler olduğu görülmektedir.

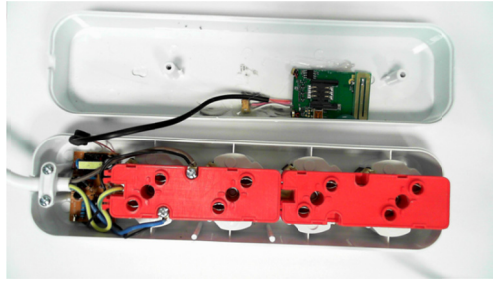


Şekil 9. 3G ile Çalışabilen Kameralı GSM Dinleme ve İzleme Modülü

GSM böcekler de hemen tüm böcekler gibi basit bir modül şeklinde olabileceği gibi (Şekil 9), bir eşya içerisinde veya şeklinde de karşımıza çıkabilmektedir. Örneğin bir bilgisayar faresi içerisinde saklanmış GSM böcek enerjisini bilgisayardan alarak bilgisayar çalıştığı müddetçe çalışmasını sorunsuz sürdürebilir, hatta bazıları üzerlerindeki takviye lityum piller sayesinde bilgisayar kapandıktan dört saat sonrasına kadar çalışmasını sürdürebilir.

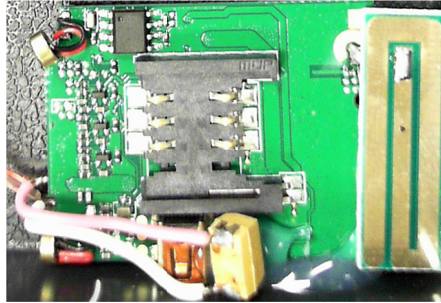
Bir priz veya uzatma içerisinde saklanmış bir GSM böcek ise enerjisini doğrudan elektrik şebekesinden alıp kesintisiz çalışabilir (Şekil 10).

²¹⁸ Abbas, R. Michael, K. Michael, M.G. Aloudat, A. Emerging Forms of Covert Surveillance Using GPS-Enabled Devices, Journal of Cases on Information Technology, vol. 13, no. 2, pp. 19-33 (2011), IGI Global



Şekil 10. Dörtlü Elektrik Uzatması İçerisine Saklanmış GSM Böcek

GSM böcekler yurtdışındaki internet sitelerinden 20 ila 40 dolar gibi fiyatlarla temin edilebilmekle beraber, bu cihazlar yurtiçi şebekeleri tarafından kayıtsız telefon olarak algılandığından bir süre sonra devre dışı bırakılmaktadır. Ancak çeşitli yollarla yurtiçine sokulan cihazlar, artık kullanılmayacak eski bir telefonun IMEI²¹⁹ numarasının böyle bir cihaza bir takım yazılımlar kullanılarak işlenmesi suretiyle²²⁰ yurt içi şebekelere uyumlu hale getirilmekte ve maliyetinin beş-on misline alıcı bulmaktadır. Bu konudaki bir başka tespit ise: yukarıdaki resimde örneği görülen uzatmalı çoklu priz gibi böceklerin - içerisine gizlenecek GSM devrelerinin (Şekil 11) yolcu bagajlarında yurda sokulduktan sonra- yurt içinde imal edildiği şeklinde olmuştur. Bu cihazlar da yukarıda sözü edilen klonlama yöntemi ile yurtiçi şebekelere uyumlu hâle getirilmektedir. Tüm bunlara ilaveten eski bir cep telefonunun içeriğinin de bir dinleme cihazına dönüştürülebileceği de göz ardı edilmemelidir.



Şekil 11. GSM Devresi Yurt Dışından Getirildikten Sonra Monte Edilmiş Cihaz

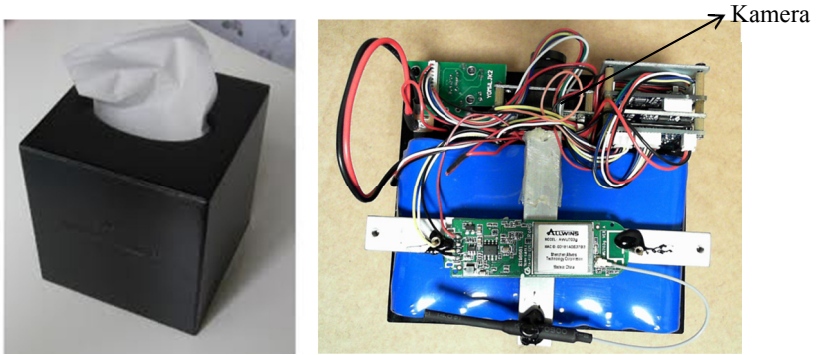
²¹⁹ IMEI: International Mobile Equipment Identity – Uluslararası Mobil Teçhizat Kimliği

²²⁰ Bu işlem “klonlama” olarak bilinmektedir.

b. Wi-Fi Böcekler

Wi-Fi²²¹ böcekler elde ettikleri verileri kablosuz ağ üzerinden aktaran böceklerdir. Aktif ve pasif olmak üzere iki çeşidi vardır. Pasif olan tipleri herhangi bir kablosuz cihazdan farklı değildir. Aldığı veriyi aktarmak için bir kablosuz çıkış noktasına ihtiyaç duyar. Yani var olan bir kablosuz ağa bağlanır ve o ağ üzerinden bilgi aktarılır. Aktif türlerinin üzerlerinde modem bulunur ve doğrudan internete çıkabilirler. Her iki durumda bu cihazlara dünyanın internete bağlı her yerinden erişilebilir.

Wi-Fi böceklerin genelde gerçek zamanlı görüntü iletmek için kullanıldığı görülmektedir. Tıpkı diğer böceklerde olduğu gibi çeşitli cihazlar içerisine gizlenmiş şekilde satılmaktadırlar (Şekil 12).



Şekil 12. Peçetelik İçerisine Gizlenmiş Wi-Fi Böcek

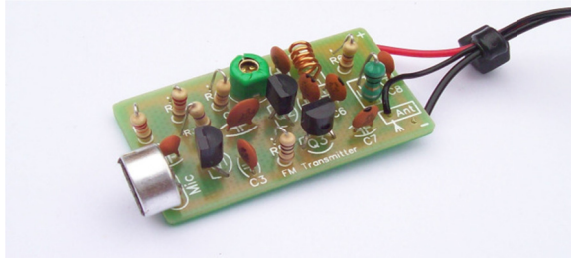
Wi-Fi frekanslarını kullanmak için lisans gerekmemektedir. Cep telefonu veya dizüstü bilgisayarla yapılan basit bir kablosuz ağ taramasında birçok kablosuz şebekenin ortamda zaten var olduğu görülebilir. Dolayısıyla bu cihazların tespiti bilinçli bir arama gerektirmektedir.

c. Diğer Tür Böcekler

Bunların dışında çeşitli değişik frekans bantlarını kullanan daha özel tip böcekler de vardır. Bunların da sürekli yayın yaptığı için frekans spektrumunda kolayca görülebilenleri olduğu gibi yalnızca gerektiğinde aktive olan/edilen türleri mevcuttur. Isı, ışık, ses, hareket, RF işaret ile aktive edilebilirler. Kullandıkları frekans bandına göre VHF böcek,

²²¹ Wi-Fi elektronik cihazların kablosuz ağlara bağlanarak veriliş-veriş yapmalarına imkân sağlayan teknolojidir.

UHF böcek vb. 88-108 MHz konvansiyonel bandını kullananlar için FM böcek gibi adlarla anılmaktadır. Örneğin Şekil 13’da görülen FM böcek aslında FM radyo üzerinden dinlenebilen herhangi bir FM Aktarım Cihazından²²² farksız çalışmaktadır.



Şekil 13. FM Böcek

Böcekler değişik protokolleri ve değişik frekansları - hatta UHF üstü olan 3GHz üzerindeki bantları - da kullanıyor olabilir. Bu yüksek frekanslarda bir böceğin, alıcı/verici antenlerinin boyutlarının küçüleceği, daha az enerjiyle yayın yapabileceği²²³, konvansiyonel böcek tarama sistemleri 3 GHz üstü spektrumu taramadıklarından spektrumun üst bölgesinde gizlenme imkânı bulabileceği düşünülebilir. Ancak yüksek frekanslı dalgalar havada fazlaca kayba uğrayacağından, uzak mesafelere veri iletmek güçleşecektir.²²⁴

Böcekler frekans atlama (FH), frekans yayma (DSSS) gibi yöntemleri kullanarak da kendilerini spektrumda gizleyebilirler.²²⁵

Genel olarak enerjisini şebekeden alan böceklerin çalışma süresi açısından herhangi bir kısıtı yoktur. Sistem kendi kullanım ömrü yettiğince veri akışı sağlayacaktır. Enerjisini pilden sağlayan sistemler ise pilleri yettiği ölçüde veri aktarabilirler. Pilin takviyesi ya da kayıt kapasitesinden dolayı saldırgan tarafından böceğe tekrar ulaşılması gerekecektir. Ancak enerjilerini oldukça tasarruflu kullanabilen akıllı sistemler ve günümüz pil teknolojisi düşünüldüğünde, bu sürenin haftaları hatta ayları bulmasının mümkün olabileceği düşünülmektedir. Diğer taraftan böceğin çalışma süresi hakkında; sistem

²²² FM Aktarım Cihazı (FM Transmitter): Genellikle USB girişi olmayan araçlarda içerisine kaydedilen müziği aracın radyosundan dinleten cihazdır.

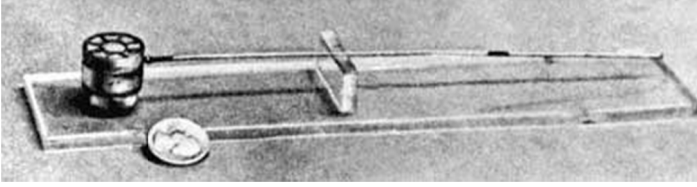
²²³ Balanis, s.811.

²²⁴ Balanis, s.95.

²²⁵ Gruber, s.279-290.

boyutu, pil kapasitesi, çalışma frekansı, alıcı/verici parametreleri bilinmeden sağlıklı bir değerlendirme yapılması zordur.

Geçmişte enerjisini tamamen dışarıdan alan pasif tipte böceklerle de rastlanmıştır. Örneğin 1952 yılında ABD'nin Rus Büyükelçiliğinde açığa çıkarılan böcek kendisine yakın bir menzilden gönderilen RF sinyaliyle aktive oluyor, ortam sesiyle modüle edilmiş sinyali geri yansıtıyordu.²²⁶



Şekil 14. Pasif Böcek Devresi İllüstrasyonu

4.2.1.3 Şebeke Dinlemeleri

Dinlemenin kurulu altyapı kullanılarak yapılmasıdır. Şebeke dinlemeleri iki ana başlık altında toplanabilir.

4.2.1.3.1 TİB Üzerinden Dinlemeler

TİB üzerinden gerçekleştirilen yasal takiplerdir. Bu konu ilgili bölümde ele alınmıştır.

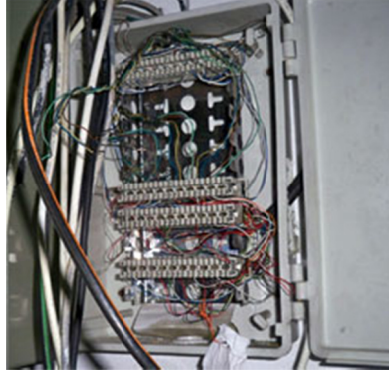
4.2.1.3.2 Saptama Dinlemeleri

Telefon görüşmelerinin kişinin hattına müdahale edilerek dinlenilmesidir. Analog telefon sistemleri herhangi bir şifreleme olmaksızın telefon görüşmelerinin hat üzerinden yollandığı sistemlerdir. Bu sistemlere hattın herhangi bir noktasından müdahale edilmesi son derece kolaydır, şöyle ki hatta paralel yeni bir telefon çekildiğinde görüşmeler rahatlıkla dinlenebilmektedir.²²⁷ Örneğin apartman içlerinde bulunan telefon kutularının müdahaleye oldukça açık olduğu bilinmektedir. (Şekil 15). Ayrıca telefon hattına seri veya

²²⁶ Peter Wright, s.19-20.

²²⁷ Gruber, s.291-300.

paralel döşenerek görüşmeleri RF üzerinden yayınlayan böceklerin de mevcut olduđu bilinmektedir.



Şekil 15. Apartman Dâhilindeki Telefon Hattı Dağıtım Kutusu

Bunun yansıra GSM sistemlerinde telefon ile baz istasyonları arasına giren sahte baz istasyonlarıyla dinleme yapılabildiğı gündemdedir. 2G şebekelerde GSM standartlarında kullanılan kimlik doğrulama yapısı, cep telefonu ve baz istasyonu arasında tek yönlü kimlik doğrulamayı kapsamakta, 3G şebekelerde ise kimlik doğrulama çift yönlü yapılmaktadır.²²⁸ Bu sebeple sahte baz istasyonunun 2G şebekelerde cep telefonu ile gerçek baz istasyonu arasına girerek güvenlik açığı oluşturabileceğı değerlendirilmektedir.

4.2.1.4 Dost Sistem Suiistimaliyle Takipler

Dost bir sistemin ele geçirilmesi ile de görsel ve/veya işitsel takip yapılabilmektedir. Örneğın internete bağılı bir bilgisayarın kamera ve mikrofonunun işletim sisteminin bazı güvenlik açıklarından yararlanan bir hacker tarafından kullanılarak ortam görüntüleme ve dinlemesi yapılabilmesi mümkündür.



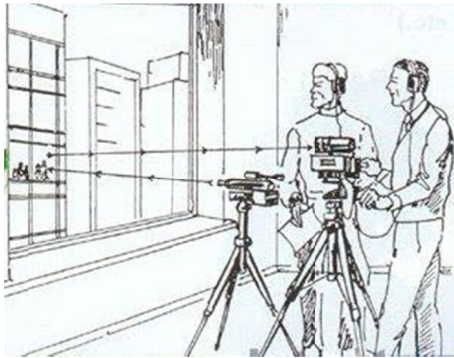
²²⁸ Christos Xenakis, Lazaros Merakos, “Security in 3G Mobile network”, Computer communications, vol. 27, (2004) s.638-650.

Ayrıca cep telefonlarına yüklenebilecek kötücül bir yazılım sayesinde bu telefonların bir dinleme cihazına dönüşebilmesi mümkündür. Ayrıca artık her telefonun üzerindeki kameraların uzaktan aktive edilmesi de mümkün hale gelmiştir. Özellikle son zamanlarda bir hayli yaygınlaşan akıllı cep telefonu teknolojisi bu bağlamda açık kapılar bırakmaktadır. Zira bu telefonlarda arka planda tam olarak ne yaptığı bilinmeyen pek çok yazılım koşturmaktadır.



4.2.1.5 Akustik Dinlemeler

Dinlemenin sesin doğal iletim yolları kullanılarak yapılmasıdır. Bu alanda en bilinen örnek lazer dinleme cihazlarıdır. Bu cihazlar dinleme yapılacak ortamın pencere camını bir diyafram gibi kullanırlar. Yakın bir binadan cama odaklanan lazer ışını ortam sesiyle modüle olmuş şekilde geri yansıtmakta, aynı noktada bir alıcı tarafından alınıp dinlenebilmekte veya kaydedilebilmektedir.



Şekil 16. Lazer Dinleme Cihazı ile Ortam Dinlemesi

Lazer dinlemelerine karşı tedbirler olarak; görüşmelerin yapılacağı ortamların penceresiz olması, ya da camlara film kaplanması veya buzlu cam olması sayılabilir. Bunun yanı sıra pencere camlarına yansıyan lazer hüzmelerinin, gelen hüzmeye aynı noktaya düşmesini engelleyecek şekilde pencere camlarının eğik olması da ilave bir tedbir olarak önerilebilir.

Aslen doğadaki sesleri dinlemeye yönelik tasarlanan fakat açık arazideki konuşmaları dinlemeye de yarayabilen sistemler de mevcuttur. Benzer teknikler ikinci dünya savaşı yıllarından beri kullanılmaktadır (Şekil 17).



Şekil 17. Birinci ve İkinci Dünya Savaşları Arasındaki Yıllarda Hollanda Ordusu Hava Savunma Sisteminin Bir Parçası Olarak Geliştirilmiş Akustik Dinleme Cihazları²²⁹

Akustik dinleme cihazı havadaki sesi parabolik alıcısı ile aldıktan sonra üzerindeki amfi sayesinde yükselterek çok uzaktaki seslerin duyulabilmesini sağlamaktadır (Şekil 18). Bunun yanı sıra duvar arkası dinlemeyi sağlayan cihazlar da mevcuttur.

²²⁹ <http://www.museumwaalsdorp.nl>



Şekil 18. Akustik Dinleme Cihazı

4.3 Dinleme ve İzleme Cihazları İthalatı²³⁰

4.3.1 Genel Olarak İthalat Gümrük Prosedürleri

Türkiye’ye ithal edilecek herhangi bir eşyanın; ya İthalat Rejim Kararı çerçevesinde ticari nitelikli olarak, ya da ticari nitelik arz etmeyecek şekilde yolcu beraberli getirilmesi mümkündür.

Türkiye’ye getirilip ithal edilecek eşya için öncelikle eşyaya ve taşıta ilişkin genel nitelikteki bilgilerin yer aldığı özet beyan verilir. Bu beyan; eşya Türkiye’ye gelmeden önce, eşyayı getiren veya eşyanın gümrük bölgesine taşıma sorumluluğunu üstlenen kişi tarafından verilmektedir.

Özet beyan üzerindeki kontrollerin tamamlanmasını müteakip eşya taşıttan boşaltılır.

Söz konusu eşya için daha sonra;

a) Denizyolu ile gelen eşya için kırk beş gün,

b) Diğer bir yolla gelen eşya için de yirmi gün içerisinde gümrük beyannamesinin verilmesi ve beyannameye ilişkin tüm işlemlerin bitirilmesi gerekmektedir.

²³⁰ Bu Bölüm Gümrük ve Ticaret Bakanlığınca Komisyonumuza iletilen bilgi notundan derlenmiştir.

Bu süreler içerisinde işlemlerin tamamlanmaması halinde eşya, gümrük mevzuatı çerçevesinde tasfiye edilir.

Eşyanın gümrük işlemleri, eşyanın sahipleri veya temsilcileri tarafından takip edilir ve sonuçlandırılır.

Gümrük idaresine verilen beyanın kontrolü ise; kırmızı, sarı, mavi ve yeşil hat olmak üzere sistem tarafından belirlenen 4 temel hat üzerinden yapılmaktadır.

- Kırmızı hat; eşyanın fiziki muayenesi ile birlikte belge kontrolünün de yapıldığı;
- Sarı hat; fiziki muayeneye gerek görülmeksizin eşyaya ait beyanname ve eklerinin doğruluğunun ve birbiriyle uygunluğunun kontrol edildiği;
- Mavi hat; eşyanın veya buna ilişkin yazılı beyan ve ilgili belgelerin veya ticari belge ve verilerin sonradan kontrol edildiği ve
- Yeşil hat, eşyanın belge kontrolüne veya muayeneye tabi tutulmadığı hattır.

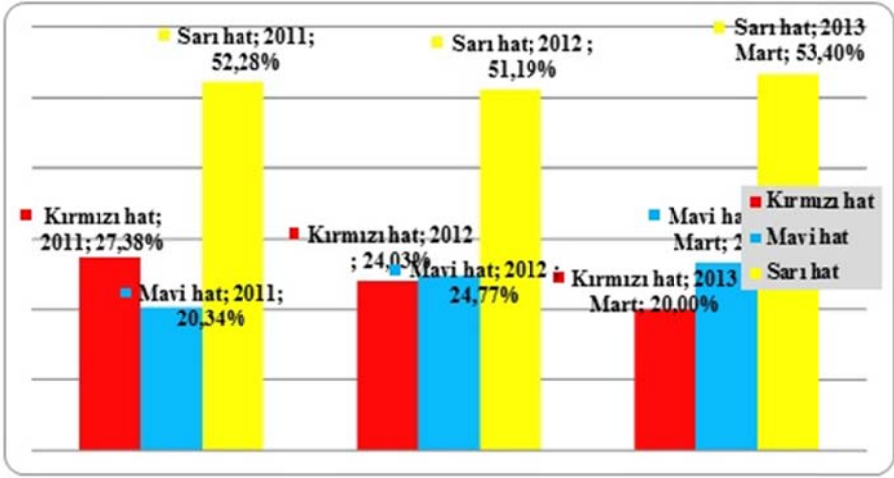
Son üç yıl itibarıyla; Türkiye'ye ithal edilen eşyanın gümrük kontrollerinin hangi hatta gerçekleştirildiğine ilişkin yüzdesel veriler, aşağıdaki grafikte sunulmaktadır.

[Ülkemizin söz konusu yıllar itibarıyla toplam ithalatı, 2012 ve 2013 yılları verileri geçici olmak üzere;

2011 yılı için: 240.841.676.274 ABD \$,

2012 yılı için: 236.545.042.030 ABD \$ ve

2013 Yılı için (ilk 2 ay itibarıyla): 38.195.077.402 ABD Dolarıdır.]



Şekil 19. Eşya Gümrük Kontrol Dağılımı

Eşyanın ithali; ticaret politikası önlemlerinin uygulanması, eşyanın ithali için öngörülen diğer işlemlerin tamamlanması ve kanunen ödenmesi gereken vergilerin tahsili ile mümkündür. Gümrük vergileri ise, gümrük yükümlülüğünün başladığı tarihte yürürlükte olan gümrük tarifesine göre hesaplanmaktadır. Gerek uygulanacak ticaret politikası önlemlerinin belirlenmesi, gerekse de ödenecek gümrük vergilerinin hesaplanması için öncelikle eşyanın tarife pozisyonunun belirlenmesi gerekmektedir.

Eşyanın, gümrük tarife istatistik pozisyonu (GTİP), eşyanın cins, nevi ve niteliğine göre uluslararası kurallar çerçevesinde belirlenen 12 rakamdan oluşan bir koddur.

Yolcular ise, beraberlerinde, ticari miktar ve mahiyet arz etmeyen “kişisel eşya” ile “hediyelik eşya” getirebilirler. Kişisel eşyaya ilişkin liste, 2009/15481 sayılı Bakanlar Kurulu Kararının Ekinde yer almaktadır. Bununla birlikte; her bir yolcu için değeri 430 Avroyu geçmeyen eşya için de hediyelik eşya muafiyeti uygulanmakta olup 15 yaşından küçük yolcular için bu tutar 150 Avro olarak uygulanmaktadır.

Öte yandan; nakil vasıtaları sürücüleri ve hizmetlileri yolcu sayılmadıklarından, yolcu beraberisi eşya muafiyetinden yararlanılmamaktadırlar.

Bununla birlikte, kara hudut kapısından diğer ülkelere giden yolcular, seyahat ettikleri ülkede en az üç gün geçmeden kara hudut kapısından dönmeleri halinde, yolcular için öngörülen muafiyet hakkından yararlandırılmamaktadırlar.

Yolcular, gümrüğe tabi eşyasının olup olmadığına ilişkin beyanı, yolcu salonlarında münhasıran bu işlemler için düzenlenmiş yeşil veya kırmızı hatlardan geçerek yapmaktadırlar. Yolcuların bagajlarında, yanlarında ve üstlerinde taşıdıkları eşyanın kontrolü de gümrük idaresince gerçekleştirilmektedir. Bu kontroller, bir ihbara dayalı olarak yapılabildiği gibi yolcu trafiğini aksatmayacak şekilde görevli personelin deneyimleri çerçevesinde risk unsuru taşıdığı addedilen kişilerin durdurulması suretiyle de yapılmaktadır.

Yolcu beraberinde getirilen eşyanın değeri, ibraz edilen faturaya, satış fişine veya eşya bedelinin ödendiğine ilişkin belgeye göre belirlenir. Bu tür belge ibraz edilememesi veya ibraz edilen belgede kayıtlı değer düşük bulunması halinde, eşyanın değeri gümrük idaresince belirlenmektedir.

18 yaş ve üzeri her bir yolcu için kıymeti 1500 Avroyu geçmeyen eşyanın geldiği ülkeye göre değişen oranda tek ve maktu vergi uygulanmaktadır. Bu oran Avrupa Birliği ülkelerinden getirilen eşya için % 18 iken; diğer ülkelerden getirilen eşya için % 20 olarak uygulanmaktadır. Yolcu beraberinde getirilen eşyanın tek başına kıymetinin 1500 Avroyu aşması halinde ise yürürlükte olan ithalat vergilerine ilişkin oranlar uygulanmaktadır.

4.3.2 Dinleme ve İzleme Cihazlarının İthalat Prosedürü

4.3.2.1 Dinleme ve İzleme Cihazlarının GTİP'inin Tespiti

Kamuoyunda “böcek” olarak tabir edilen dinleme ve izleme cihazları, İstatistik Pozisyonlarına Bölünmüş Türk Gümrük Tarife Cetveli’nde ismen yer almamaktadır.

Bununla beraber; söz konusu eşyanın

- “sesi kaydetme”,
- “ses frekansını yükseltme”,
- “kaydedilen sesi tekrar verme” ya da
- “ses ile beraber görüntü kaydetme” gibi özellikleri göz önünde bulundurulduğunda;

Muhtemel GTİP’lerinin

- 8518.40.80.00.00,
- 8519.81.95.00.00
- 8525.50.00.00.19 veya
- 8525.80.91.00.00 olabileceği tespit edilmiştir.

Ancak; belirtilen bu GTİP’lerde elektronik alanında faaliyet gösteren pek çok firmanın üretiminde kullanılan parçaların da sınıflandırılabilceği, ayrıca yaygın olarak kullanılan cep telefonları gibi esas niteliği ses kaydetme olmayan pek çok elektronik cihazın da ses kaydetmeye yönelik özelliklerinin olduğu, söz konusu cihazların, kullanım amacına göre kullanım yerinin değişmesinin mümkün olduğu, hususları gözden kaçırılmamalıdır.

4.3.2.2 Dinleme ve İzleme Cihazlarının İthalatı

Dinleme ve izleme cihazlarının GTİP tespitinde yer verilen hususlar bir arada değerlendirildiğinde; Gümrük ve Ticaret Bakanlığı Gümrük Veri Ambarı Sistemi (GÜVAS) üzerinde elde edilecek verilerle konuyla ilgili olarak sağlıklı bir istatistik analiz yapılmasının mümkün bulunmadığı değerlendirilmektedir. Diğer taraftan;

- Türk Ceza Kanununda suç olarak sayılan bir fiili işlemeye yönelik ve boyut, hacim ve ağırlık itibarıyla çok küçük olan, kamuoyunda “böcek” olarak tabir edilen cihazların gümrük idarelerine beyanda bulunularak, normal bir ticari ithalat kapsamında yurda sokulmasının söz konusu olmayacağı,

- Ancak, bu tür eşyanın gümrük idaresine herhangi bir beyanda bulunmaksızın, yasa dışı veya kaçak yollardan yurda sokulabileceği,

- Ya da, yolcu beraberinde beyan dışı olarak getirilebileceği,

- Bu tür cihazların, bir başka eşyanın içine monte edilerek (kalem, saat vb.) getirilmesinin de mümkün olduğu,

sonucuna varılmaktadır.

4.3.2.3 Dinleme ve İzleme Cihazlarının İthalat Denetimine İlişkin Mevzuat

Söz konusu GTİP’lerde sınıflandırılan eşyanın tabi olduğu ithalat denetimlerine ilişkin mevzuat aşağıdaki tabloda sunulmuştur:

Tablo 15- Dinleme ve İzleme Cihazlarının İthalat Denetimine İlişkin Mevzuat

GTİP	İLGİLİ DÜZENLEME	İLGİLİ DÜZENLEMİYİ HAZIRLAYAN KURUM	DENETİMİ YAPAN KURUM
8518.40.80.00.00 ve 8525.80.91.00.00	CE İşareti Taşınması Gereken Bazı Ürünlerin İthalat Denetimi Tebliği (Ürün Güvenliği ve Denetimi: 2013/9)	Ekonomi Bakanlığı	TSE
	İthalinde Garanti Belgesi Aranacak Maddelere İlişkin Tebliğ (İthalat: 2013/6)	Ekonomi Bakanlığı	Gümrük ve Ticaret Bakanlığı (Tüketicinin Korunması ve Piyasa Gözetimi Genel Müdürlüğü)
8519.81.95.00.00	---	---	---
8525.50.00.00.19	Telsiz ve Telekomünikasyon Terminal Ekipmanlarının İthalat Denetimi Tebliği (Ürün Güvenliği ve Denetimi: 2013/8)	Ekonomi Bakanlığı	Ekonomi Bakanlığı

4.3.2.4 Dinleme ve İzleme Cihazlarının İthalat Vergileri

Dinleme ve izleme cihazlarının ithalatında alınan gümrük vergisi, katma değer vergisi ve özel tüketim vergisinin oranları aşağıdaki tabloda sunulmuştur:

Tablo 16- Dinleme ve İzleme Cihazları İthalat Vergileri

GTİP	GÜMRÜK VERGİSİ (%)	KDV (%)	ÖTV (%)
8518.40.80.00.00	0 - 4,5	18	20
8519.81.95.00.00	0 - 2	18	---
8525.50.00.00.19	0 - 3,6	18	---
8525.80.91.00.00	0 - 4,9	18	---

4.3.2.5 Dinleme ve İzleme Cihazlarının İthalat Verileri

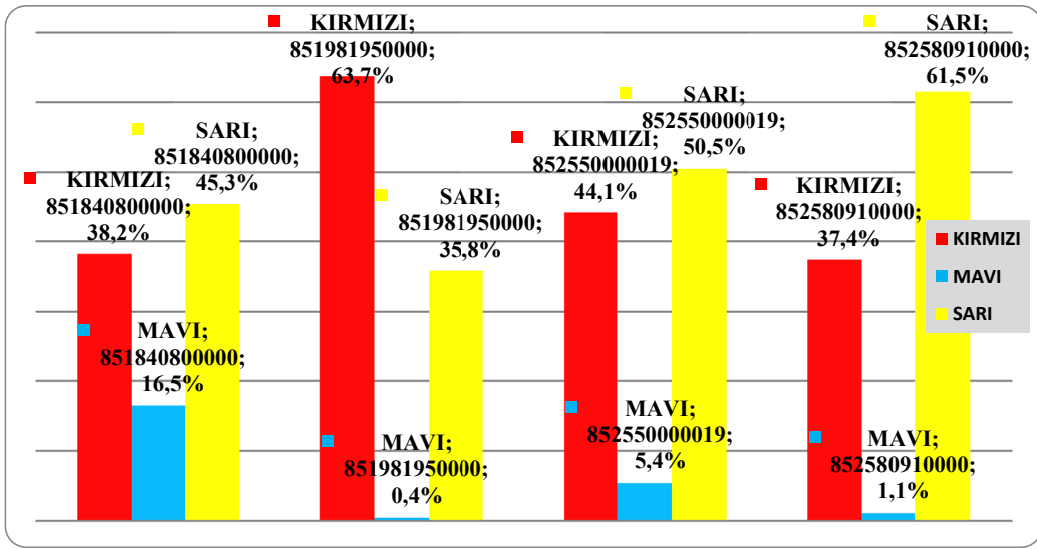
Belirtilen GTİP’lerden 1/1/2012 - 9/4/2013 tarihleri arasında ölçü birimi “adet” olarak beyan edilerek yapılan ithalatlar GÜVAS üzerinde sorgulandığında; ithale konu eşyanın ortalama ağırlığının 7,96 kg olduğu da dikkate alındığında; boyut, hacim ve ağırlık itibarıyla çok küçük olan ve “böcek” olarak tabir edilen bu cihazların, güvenlik birimlerince yapılan ithalatlar hariç; yasal olmayan yollardan yurda sokulabileceği değerlendirilmektedir. Yapılan GÜVAS sorgusu; sonucu söz konusu GTİP’lerden yapılan ithalata ilişkin istatistik aşağıda gösterilmiştir:

Tablo 17- Dinleme ve İzleme Cihazları İthalat Verileri

GTİP	Eşyanın Tanımı	İthal Eden Firma Sayısı	Eşya Miktarı	İstatistik Kıymet (USD)
8518.40.80.00.00	Diğerleri	313	251.474 adet	15.565.586
8519.81.95.00.00	Diğerleri	138	1.582.440 adet	10.886.791
8525.50.00.00.19	Verici diğer cihazlar	74	725.468 adet	2.131.587
8525.80.91.00.00	Sadece televizyon kameralarının aldığı ses ve görüntüleri kaydedebilenler	112	99.788 adet	19.739.251
YUKARIDAKİ 4 GTİP (Adet Haricindekiler)		23	Muhtelif ölçü birimleri (Set, çift, baş, kg gibi)	3.285.945

4.3.2.6 Dinleme ve İzleme Cihazlarının Gümrük Kontrolleri

2012 yılı itibarıyla; “851840800000”, “851981950000”, “852550000019” ve “852580910000” GTİP’lerinden gerçekleştirilen ithalatlara ilişkin hat oranlarını gösterir veriler, aşağıdaki grafikte sunulmaktadır.



Şekil 20. Dinleme ve İzleme Cihazları Gümrük Kontrol Dağılımı

4.3.2.7 Dinleme ve İzleme Cihazlarının Yakalama Verileri

Gümrük ve Ticaret Bakanlığı Kaçakçılık Bilgi Bankası kayıtları göre, “böcek” olarak tabir edilen bu cihazlar yakalamalarına ilişkin veriler aşağıdaki tabloda sunulmaktadır.

Tablo 18- Dinleme ve İzleme Cihazlarının Yakalama Verileri

Ses Dinleme ve Kayıt Cihazı Yakalamaları				
Olay Tarihi	Eşyanın Cinsi	Eşyanın Miktarı	Miktar Birimi	Eşyanın Değeri (TL)
18/12/2000	Ses Kaydına Mahsus Diğer Araçlar	2.500	Kilogram	0
05/08/2002	Ses Kayıt Cihazı	10	Adet	100
31/10/2004	Ses Kayıt Cihazı	8	Adet	400
08/11/2004	Ses Kayıt Cihazı	145	Adet	36.250
24/02/2005	Ses Kayıt Cihazı	1	Adet	787
08/03/2005	Ses Kayıt Cihazı	30	Adet	7.664
01/12/2005	Ses Kayıt Cihazı	72	Adet	9.628
29/06/2007	Ses Kayıt Cihazı	1	Adet	85
24/05/2009	Ses Kayıt Cihazı	6	Adet	240
15/07/2009	Ses Dinleme Cihazı	288	Adet	10.740
07/09/2010	Ses Cihazı	8	Adet	1.726
13/04/2011	Dijital Ses Kayıt Cihazı	11	Adet	741
15/04/2011	Ses Dinleme Cihazı	150	Adet	7.500

17/07/2011	Ses Dinleme Cihazı	4.818	Adet	916.919
17/10/2012	Ses Kaydedici	57	Adet	1.140
13/11/2012	Ses Kayıt Cihazı	2	Adet	12.154

Yakalamaların ağırlıklı olarak yolcu beraberli eşyanın bagaj kontrolleri sırasında yapıldığı, bir kısmının da ticari eşyanın kontrollerinde beyan harici olarak tespit edildiği anlaşılmıştır.

4.4 Frekans Spektrumu

4.4.1 Spektrum Hakkında Genel Bilgiler

4.4.1.1 Frekans Nedir?

Frekans kelimesi Türkçedeki asıl karşılığı “sıklık” olan Fransızcadan dilimize girmiş bir kelimedir (fréquence).²³¹ Herhangi tekrarlı bir olayda, bir saniyelik süre içerisinde gerçekleşen tekrarların sayısına o olayın frekansı denir. Frekans birimi, Alman Fizikçi Heinrich Hertz’e izafen, Hertz (Hz) olarak adlandırılmıştır. Örneğin saniyede bir kez salınan bir sarkacın salınım frekansı 1 Hz’dir. Hz birimi – tıpkı diğer birimlerde olduğu gibi - her bin katı için kilo, Mega, Giga, Tera şeklinde ön ekler alır. Buna göre:

$$1000 \text{ Hz} = 10^3 \text{ Hz} = 1 \text{ kHz} \text{ (Bin Hertz = Bir kiloHertz)}$$

$$1000000 \text{ Hz} = 10^6 \text{ Hz} = 1 \text{ MHz} \text{ (Bir milyon Hertz = Bir MegaHertz)}$$

$$1000000000 \text{ Hz} = 10^9 \text{ Hz} = 1 \text{ GHz} \text{ (Bir milyar Hertz = Bir GigaHertz)}$$

$$1000000000000 \text{ Hz} = 10^{12} \text{ Hz} = 1 \text{ THz} \text{ (Bir trilyon Hertz = Bir TeraHertz)}$$

şeklinde kullanılmaktadır.

4.4.1.2 Dalga Nedir?

Dalga enerjinin ortamda yayılmasıdır. Enerji maddesel bir alışverişi, bir gidiş-geliş olmadan bir noktadan başka bir noktaya dalgalar vasıtasıyla aktarılabilir. Enerjinin önceden tayin edilmiş bir protokolle aktarılmasıyla karşılıklı bilgi aktarımı da mümkün olur. Dalgalar taşıdıkları enerjinin ve hareket ettikleri ortamın cinsine göre adlandırılırlar. Dalgalar frekansla veya dalga boyuyla ifade edilebilirler. Bu iki parametre dalganın ortamda ilerleme hızı ile birbirine bağlıdır.²³²

²³¹ <http://www.tdk.gov.tr>

²³² Eugene Hecht, Optics - Third Edition, Addison Wesley Longman, Inc. (1998), s.11-21.

4.4.1.3 Elektromanyetik Dalga

Elektrik ve manyetik kuvvetler çok eski çağlardan beri biliniyordu. Daha eski Yunan’da kehribar taşının kumaşa sürtülmesiyle kumaş ile taş arasında bir çekim kuvveti olduğu gözlenmişti. Bu çekime sebep olan elektriklenme, ufak parçacıkların kumaştan kehribara geçmesi ile oluşmaktaydı. Bu olaydan ilhamla bu küçük parçacıklara yunanca kehribar kelimesinden türetilen “elektron” adı verildi. Sonrasında “Elektrik” kelimesi de yine aynı kökten türetilmiştir.²³³

Atom birbirini çeken iki zıt kutuptan oluşmuştur. Hareketli küçük eksi yük elektronun (-) yanı sıra çekirdekte yüklü parçacıklar olarak protonlar (+) bulunur. Bu iki kutup birbirinden ayrılınca aralarında bir çekim kuvveti oluşur. Kehribar kumaşa sürtülünce sürtünmeden kaynaklanan enerji elektronları atomlarından kopartarak kehribarın atomlarına geçmelerine sebep olur. Böylece bir tarafta elektronlarını kaybetmiş atomlar artı (+) ile, diğer tarafta fazladan elektron barındırmak zorunda kalan atomlar ise eksi (-) yüklenir. Aradaki bu yük dengesizliği kumaş ile kehribar arasında elektriklenme dediğimiz, elektriksel çekim kuvvetinin sebebidir. Herhangi bir noktadaki birim yüke etki eden kuvvet elektrik alan olarak adlandırılmaktadır. Yani günlük hayatta elektriklenme şeklinde ifade edilen olay fizikte bir elektrik alanın varlığıyla açıklanmaktadır.²³⁴

Yine eski dönemlerden beri magnetit taşının manyetik özellikleri biliniyordu.²³⁵ Eski devirlerde bu iki hadisenin de aynı sebepten olduğu sanılmakla beraber daha sonraki dönemlerde manyetik kuvvette elektrik olayından farklı olarak birbirinden ayrılabilen (+) ve (-) yüklerin olmadığı görüldü. Ortada sadece kaynağı olmayan bir kuvvet vardı. Elektriğin keşfinden sonra içinden elektrik geçen kabloların pusulaları saptırdığı görüldü.²³⁶ Bunun asıl sebebi ise akımın yani hareketli yüklerin manyetik alan oluşturmaya idi. Benzer şekilde değişen manyetik alanında elektrik alanı değiştirdiği tespit edildi. Bu olaya endüksiyon denilmektedir.²³⁷

1865 yılında James Clerk Maxwell daha önceden bilinen elektrik, manyetik ve endüksiyon prensiplerine bir ekleme yaptı. Şöyle ki yalnızca akan yükler değil değişen elektrik alan da manyetik alan oluşturmaktaydı. Bundan dolayı elektrik alandaki ani bir

²³³ David Halliday, Robert Resnick, Jearl Walker, Fundamentals of Physics – Fourth edition – Extended, John Wiley & Sons, Inc. (1993), s. 636

²³⁴ David Halliday, Robert Resnick, Jearl Walker, s. 654-655.

²³⁵ David Halliday, Robert Resnick, Jearl Walker, s. 636.

²³⁶ David Halliday, Robert Resnick, Jearl Walker, s. 848-858.

²³⁷ David Halliday, Robert Resnick, Jearl Walker, s. 875.

değişiklik değişen bir manyetik alan indüklemekte, oluşan bu manyetik alan da yeniden bir elektrik alan indüklemekte ve bu süreç böylece giderek boşlukta dalga şeklinde yayılmaktaydı. Bu dalgalara elektromanyetik dalga denilmiştir. Maxwell bu şekilde yola çıkarak elektromanyetik dalgaların varlığını teorik olarak ortaya koymuştur.²³⁸ Yine bu dalgaların varlığı 1886 yılında Heinrich Hertz tarafından deneysel olarak da gösterilmiştir.²³⁹

4.4.1.4 Elektromanyetik Spektrum

Elektromanyetik dalgalar frekanslarına göre sıralanarak elektromanyetik frekans spektrumunu oluştururlar. Elektromanyetik spektrumda dalgalar dalgaboylarına göre atomaltı değerlerden başlayarak (Gama Işınları) binlerce kilometre uzunlukta olabilecek radyo dalgalarına kadar sıralanırlar. Dalgaboyu ile frekans arasında ters bir orantı vardır. Dalgaboyu küçüldükçe frekans artar. Örneğin 1 MHz'lık dalganın dalgaboyu 300 metre iken, 1 GHz'lık dalganın dalgaboyu 300 milimetredir. Aradaki ters orantının katsayısı ışık hızıdır.²⁴⁰

Spektrumun elektronik haberleşme amacıyla kullanılan, genellikle 3 kHz - 3000 GHz (3 THz) arasındaki bölümü Radyo Frekans (RF) olarak adlandırılmaktadır. Radyo Frekans bölgesinin üstünde kızılötesi, görünür (optik), morötesi bölgeleri, daha ötesinde X-Işınları ve Gama-Işınları bölgeleri yer almaktadır (Şekil 21). RF bölgesinin üzerinde dalgalar frekanstan ziyade dalgaboylarıyla anılırlar.

Spektrumun fiziksel nedenlerden ötürü, sadece belirli bir bölümü kablosuz haberleşmede kullanılabilir. Düşük frekanslarda elektromanyetik dalga tarafından taşınabilen bilgi miktarı azalmaktadır. Yüksek frekanslarda ise elektromanyetik dalga tarafından taşınan bilgi miktarı artmasına rağmen dalganın yayılım alanı daralmaktadır. Bu nedenle yapılan haberleşmenin cinsine göre farklı frekans bantları tercih edilmektedir.²⁴¹ Örneğin denizcilik ve askeri haberleşmede çok uzak mesafelerle iyonosfer vasıtasıyla haberleşmenin kesilmeden yapılmasına imkân sağlayan HF (3 MHz – 30 MHz) bandı vazgeçilmezdir. Kaliteli bir ses yayını için yerel radyolara VHF bandı içerisinde FM bandı

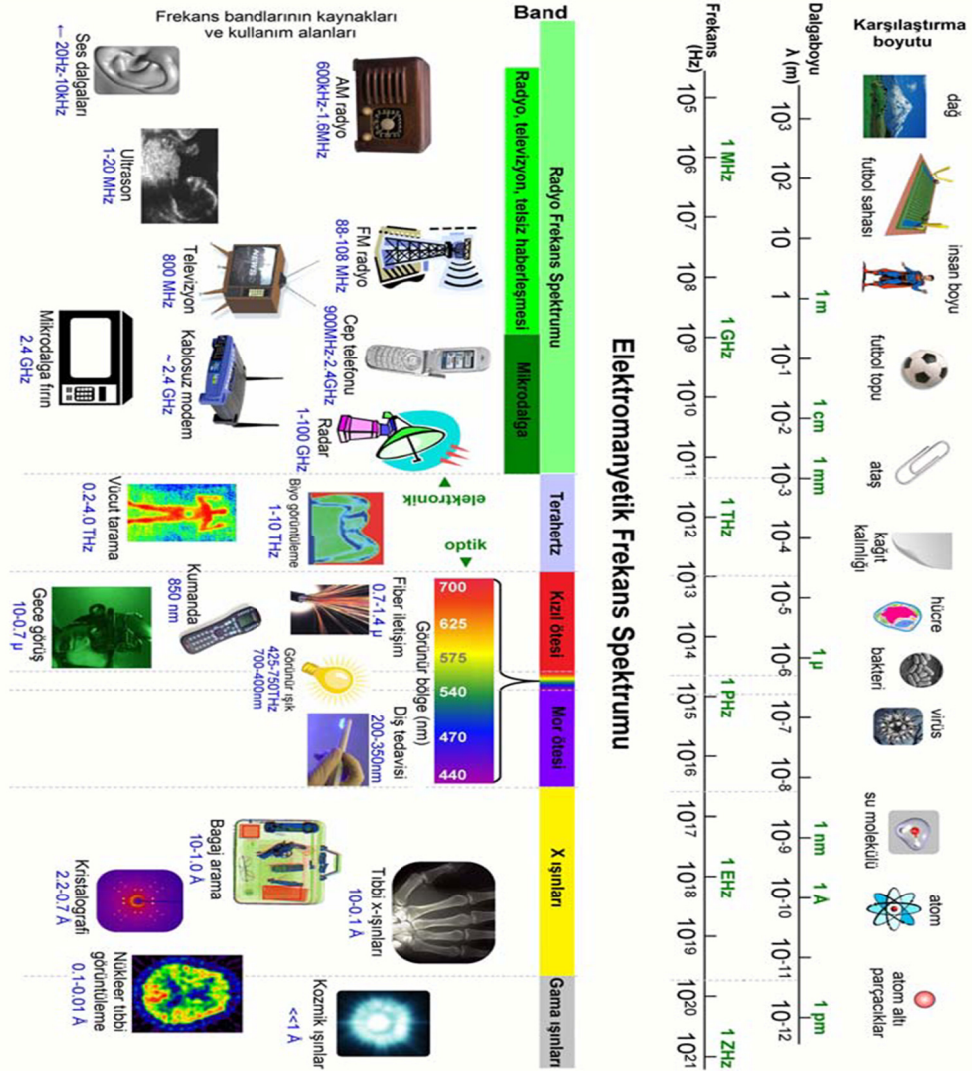
²³⁸ John David Jackson, s. 237-239.

²³⁹ Simons, s. 38-39

²⁴⁰ Hecht, s. 16.

²⁴¹ Spectrum as a Technical Resource, InfoDev (Information for Development) & ITU Joint Project, ICT Regulation Toolkit, www.ictregulationtoolkit.org/en/Section.2658.html

olarak anılan (88 MHz – 108 MHz) bölge tahsis edilmiştir. Televizyon yayınları, cep telefonları gibi daha yüksek veri aktarılan yayınlarda ise UHF bandı tercih edilmektedir.



Şekil 21. Elektromanyetik Frekans Spektrumu²⁴²

²⁴² Selek Y. K., İlhan E., Yayla F., Esnek Spektrum Yönetimi: Spektrum İhaleleri ve Spektrum Ticareti, Bilgi Teknolojileri ve İletişim Kurumu (2010).

Tablo 19- Frekans Tablosu

Band	Frekans	Yayılım alanı	Kullanım
VLF (Çok Düşük Frekans)	3-30 KHz	1000 km	Uzun mesafe radyo seyrüsefer
LF (Düşük Frekans)	30-300 KHz	1000 km	Uzun mesafe radyo seyrüsefer
MF (Orta Frekans)	300-3000 KHz	2-3000 km	Uzun mesafe radyo seyrüsefer
HF (Yüksek Frekans)	3-30 MHz	1000 km'ye kadar	Yayıncılık ve noktadan noktaya iletişim
VHF (Çok Yüksek Frekans)	30-300 MHz	2-300 km	Yayıncılık, kişisel haberleşme sistemleri WAN
UHF (Ultra Yüksek Frekans)	300-3000 MHz	< 100 km	Yayıncılık, kişisel haberleşme sistemleri WAN
SHF (Süper Yüksek Frekans)	3-30 GHz	30 km- 2000 km arasında değişmektedir	Yayıncılık, kişisel haberleşme sistemleri WAN, uydu iletişim
EHF (Ekstra Yüksek Frekans)	30-300 GHz	20 km- 2000 km arasında değişmektedir	Mikrocell, noktadan noktaya iletişim, kişisel haberleşme sistemleri ve uydu iletişim
THF (Aşırı Yüksek Frekans)	300-3000 GHz		Uydulararası iletişim

4.4.1.5 Spektrum Yönetimi

Spektrum yönetimi, spektrumun çeşitli yöntem ve yaklaşımlar çerçevesinde, bölgesel ve uluslararası koordinasyon kapsamında kullanıcılara veya hizmetlere, ülkelerin spektrum yönetimi otoritesi olan idare tarafından tahsis edilmesi şeklinde tanımlanabilir. Önceleri görece basit olan spektrum yönetimi, telsiz (kablolu) haberleşmesinin

yaygınlaşmasıyla daha karmaşıklaşmış ve daha etkin bir kullanımın gereğini ortaya çıkarmıştır.

Spektrum yönetimi, küresel, bölgesel ve ulusal olmak üzere üç seviyede yapılmaktadır. Küresel seviyede spektrumun kullanımı Uluslararası Telekomünikasyon Birliği (ITU) tarafından hazırlanan Telsiz Tüzüğü'yle düzenlenmektedir. Bölgesel seviyede ise çeşitli ülkelerin bir araya gelmesiyle oluşturdukları çok uluslu birlikler spektrumun hangi hizmetlere tahsis edileceğinin ayrıntılarını belirlemektedir. Türkiye'nin de içerisinde bulunduğu Avrupa bölgesinde, Avrupa Posta ve Telekomünikasyon İdareleri Birliği (CEPT), Avrupa'da spektrum kullanımını uyumlulaştırmaktadır. Ayrıca, Avrupa Bölgesi için Avrupa Birliği de spektrum kullanımına ilişkin politika belirlemekte, çeşitli düzenlemeler ile Birlik içerisinde spektrum verimini en üst düzeye çıkarmaya çalışmaktadır. Ulusal seviyede ise spektrum, ülkelerin ilgili düzenleyici idaresi tarafından, kamusal güvenlik, teknik ve ekonomik etkinlik gibi unsurlar dikkate alınarak yönetilmektedir.

Spektrum yönetiminin temel amacı spektrumun mümkün olan en verimli şekilde kullanılmasının sağlanmasıdır. Spektrumun etkin şekilde tahsis edilebilmesinin frekanslar arası karşılıklı ilişkiler ve farklı kullanım alanlarından dolayı zorlukları vardır. Frekans tahsisleri yapılırken gerek ekonomik gerekse teknik verimlilik göz önüne alınmalıdır. Bu bağlamda spektrum kaynağının ülkenin ekonomik büyümesine azami katkı sağlayacak şekilde kullanılması ekonomik verimliliği ifade ederken, frekans kaynağının en yüksek kapasitede ve frekanslar arası girişim olmaksızın kullanılması ve tüm spektrum uygulamalarına fırsat yaratılması ise teknik verimliliği ifade etmektedir.²⁴³

4.4.1.6 Ülkemizde Spektrum Yönetimi

Ülkemizde bugünkü bilinen anlamda frekans spektrumu yönetimi, 1983 yılında kabul edilerek yürürlüğe giren Telsiz Kanunu'na istinaden Ulaştırma Bakanlığına bağlı olarak kurulan Telsiz Genel Müdürlüğü ile birlikte başlamıştır. 1983 yılına kadar spektrumun sivil kullanımının yönetimi ITU ve CEPT hükümleri doğrultusunda PTT tarafından yürütülmüştür. Daha sonra, dünyada kabul gören telekomünikasyon piyasalarının serbestleştirilmesi ve özelleştirilmesi politikaları sonucu stratejik sektörler için bağımsız düzenleyici ve denetleyici otoritelerin kurulması uygulamaları paralelinde,

²⁴³ Cave M., Doyle C., Webb W., Essentials of Modern Spectrum Management, Cambridge University Press (2007), s 2-8.

2000 yılında Türkiye’de idari ve mali olarak bağımsız düzenleyici ve denetleyici otorite olan Telekomünikasyon Kurumu kurulmuştur. 2008 yılında çıkan Elektronik Haberleşme Kanunu (EHK) ile kurumun adı Bilgi Teknolojileri ve İletişim Kurumu (BTK) olarak değiştirilmiştir.

Bilgi Teknolojileri ve İletişim Kurumu, elektronik haberleşme sektöründe etkin rekabetin sağlanması ve ayrımcılık gözetilmemesi, şeffaflığın sağlanması, spektrumun etkin ve verimli bir şekilde kullanımının sağlanması, telsiz yayınlarının zararlı elektromanyetik girişime sebebiyet vermeden kullanılması için gerekli tedbirleri almakla görevlidir. Diğer taraftan yine elektronik haberleşme alanında ITU, IMO, ICAO ve CEPT gibi uluslararası ve bölgesel örgütlerin kararlarını, ikili ve çok taraflı anlaşmaları ve AB müktesebatını dikkate almak da kurumun vazifelerindendir. Kurum frekans planlaması ve tahsisi yapılırken komşu ülkelerle sınırlarda oluşabilecek zararlı elektromanyetik girişim etkilerinin önlenmesi veya en aza indirilmesi ve spektrumun karşılıklı olarak etkin ve verimli bir şekilde kullanımının sağlanması için gerekli çalışmaları da yapar.²⁴⁴

4.4.2 Tahsisler

Telsiz cihaz veya sistemi kurmak ve işletmek isteyenler BTK’ya başvurarak frekans tahsis işlemlerini yaptırırlar. Ancak, BTK tarafından yayımlanan yönetmeliklerde belirtilen herhangi bir izne ve telsiz ruhsatnamesine ihtiyaç kalmaksızın kullanılabilir telsiz cihaz ve sistemlerinde bu işleme gerek yoktur.

Frekans tahsislerinde, Dışişleri Bakanlığı, Türk Silahlı Kuvvetleri, Millî İstihbarat Teşkilatı Müsteşarlığı ve Emniyet Genel Müdürlüğü ve acil durum ihtiyaçlarına öncelik tanınır. Türk Silahlı Kuvvetleri ile Radyo ve Televizyon Üst Kurulu, Millî Frekans Planı çerçevesinde BTK tarafından kendilerine tahsis edilen frekans bantlarında frekans planlamasını yapar ve uygularlar. Frekans tahsislerindeki kanal planlaması ITU, IMO, ICAO, AB ve CEPT gibi uluslararası organizasyonların kararları dikkate alınarak yapılır.

Frekans tahsisleri belirli süreler için yapılır, süre sonunda uzatma talep edilirse uygun görülen telsiz sistemi kullanıcılarının kullanım süresi uzatılır. Tahsisli frekanslar için sistemin kullanım yeri, verici gücü, anten tipi, anten yönü ve anten yüksekliği vb. teknik parametrelerine BTK tarafından gerekli sınırlamalar getirilebilir. BTK, kullanım

²⁴⁴ Selek Y. K., İlhan E., Yayla F., s. 12.

tahsis ettiği frekansların temiz ve elektromanyetik girişimsiz olmasını temin etmek için gerekli tedbirleri alır.²⁴⁵

4.4.2.1 Spektrumun İzlenmesi ve Denetlenmesi

Elektronik Haberleşme Kanunu kapsamında işletmecilerin lisans sözleşmelerinin gereklerini yerine getirip getirmediği, telekomünikasyon tesislerinin kullandıkları teçhizatların standartlara uygunluğu ve telekomünikasyon sektörünün ilgili mevzuata uyup uymadığı denetlenmekte ve spektrum izleme ve denetimini yapmak görevi BTK'ya verilmiştir. Bu kapsamda BTK tarafından düzenlemelere uymayan işletmecilere müeyyide uygulanabilmektedir.

Bilgi Teknolojileri ve İletişim Kurumu, Spektrum İzleme ve Denetleme görevi kapsamında aşağıdaki işlevleri yerine getirmektedir:

- Telsiz haberleşmesinde usulsüz ve kaçak yayınlar ile enterferansları izlemek, tespit etmek, gidermek ve bu duruma sebebiyet verenler hakkında gerekli işlemleri yapmak,
- Telsiz haberleşmesinde ulusal ve uluslararası teknik monitör hizmetlerini yürütmek ve uluslararası kuruluşlar ile koordineli olarak çalışmalara iştirak etmek,
- Telekomünikasyon sektöründe kullanılan teçhizatın standartlara uygunluğunu denetlemek ve uygun olmayanların kaldırılmasını sağlamak,
- Ruhsat verilen telsiz sistemlerini, servis kalitesi ve verilen ruhsatlar doğrultusunda denetlemek,
- Her türlü telsiz yayınının birbirlerini etkilemeyecek şekilde yürütülmesini denetlemek, frekans bantlarının uygun şekilde kullanımını denetlemek ve uygunluğu sağlamak için gerekli tedbirleri almak, ilgili birimlerle bu konuda iş birliği yapmak,
- Telsiz sistemleri ile ilgili teknik denetim ve enterferans şikâyetlerinin incelenmesini sağlayacak teçhizatın temini, tesisi, bakımı ve işletmesini yapmak.

²⁴⁵ Selek Y. K., İlhan E., Yayla F., s. 16-22.

4.4.2.2 Milli Monitör Sistemi

Telsiz haberleşme trafiğinin düzenlenmesi, denetlenmesi ve telsiz kullanım ihlallerin tespit edilmesi amacıyla gerekli teknik cihaz ve sistem altyapısından oluşan ve 7 Bölge Müdürlüğünde kurulan Milli Monitör Sistemi (MMS) ile; yayın kapsama alanları, frekans kullanım yoğunluğu ve teknik parametrelerin ölçülmesi, AM/FM radyo ve TV yayınlarının teknik kalite kontrollerinin yapılması, elektromanyetik girişim olaylarının tespit edilmesi ve çözümlenmesi, illegal telsiz istasyonlarının yerlerinin bulunması, frekans yönetimi amacıyla istatistiki verilerin toplanması faaliyetleri yürütülmektedir.

Bu kapsamda 10 KHz - 2,5 GHz bandındaki her türlü elektromanyetik yayın izlenebilmekte ve Radyo ve TV yayınlarının kalite düzeyinin tespit edilmesi ve elektromanyetik girişim konularının çözümlenmesi mümkün olmaktadır. Ayrıca kaçak veya tahsis-dışı frekanstan yayın yapan istasyonların coğrafi konumları tespit edilebilmekte bunların yasal diğer cihaz ve sistemler üzerinde yaratabilecekleri zararlı elektromanyetik girişim önlenebilmektedir. Ancak bu sistemin her an her noktayı kapsamı mümkün değildir. Bu bağlamda ani ve yerel yayınların tespiti oldukça güçtür. Bu tür vericilerin tespiti ancak lokal aramalarla mümkün olabilecektir. Esas itibarıyla bu sistem, kişilerin telsiz haberleşme imkânlarından daha fazla ölçüde ve yüksek kalitede yararlandırılmasını, hava ve deniz seyrüsefer sistemlerinin uluslararası kriterlere uygun olarak işletilmesini ve bunların fonksiyonlarını yerine getirmesini sağlamaktadır.

Sistem Merkez ve 7 Bölge Müdürlüğünde olmak üzere;

- NCC-Milli Kontrol Merkezi
- RMC-Bölge Monitör Kontrol Merkezi
- RRS-Bölge Uzaktan Kumandalı Sabit Monitör İstasyonu
- TRRS-Bölge Uzaktan Kumandalı Seyyar Monitör İstasyonu
- MOBDF-Mobil Yön Kestirme ve Monitör İstasyonu
- MOBBC-Mobil Radyo-TV Yayınları Ölçüm Sistemi
- CMSV-Kontrol, Bakım-onarım ve İkmal Aracı
- PDFM-Portatif DF ve Monitör Teçhizatı

Olmak üzere sabit, seyyar, mobil ve portatif istasyonlardan oluşmaktadır.

4.5 Kablosuz Haberleşme

Kablosuz haberleşme bir verinin fiziksel şebeke bağlantısı olmayan iki nokta arasında taşınmasını sağlayan haberleşme türüdür. Teknolojik gelişmeler ve küreselleşen dünya gereksinimleri kablosuz iletişimin ve kablosuz sistemlerin doğmasına ve gelişmesine sebep olmuştur. İletişimin sınır tanımamasıyla kablonun ve fiziksel bağlantının pratik olmayacağı noktalarda kablosuz sistemler devreye girmektedir.

Günümüzde kablosuz iletişim hayatımızın vazgeçilmezlerinden birisi hâline gelmiştir. Televizyon kumandası gibi kısa mesafeli iletişimden, cep ve uydu telefonları gibi uzak mesafeli iletişime kadar hayatımızın her alanında kablosuz iletişimin örneklerini görmek mümkündür.

Hayatımızda en fazla yer işgal eden ve haberleşme deyince ilk aklı gelen sistem cep telefonu şebekesidir. Cep telefonu sistemleri çeşitli adlarla anılmaktadır. En yaygın GSM’dir.

4.5.1 Cep Telefonu Teknolojileri

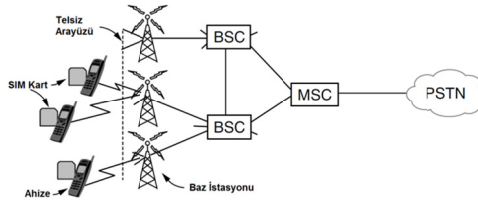
4.5.1.1 2G Teknolojisi

2G teknolojilerinde dünya üzerinde kabul edilmiş ortak bir standart yoktur. Günümüzde, D-AMPS, GSM, CDMA ve PDC olmak üzere dört farklı teknoloji kullanılmaktadır. Bunlardan bazıları pek yaygın değildir. Mesela PDC sadece Japonya’da kullanılmaktadır. Ülkemizde de kullanılan Avrupa standardı GSM’dir. GSM 1980’lerde Avrupa’ya has bir 2G standardı olarak geliştirilmiştir. “Groupe Spécialé Mobile” adındaki telekom grubunun adının kısaltmasıdır. İlk GSM sistemleri 1991’de kullanılmaya başlamış ve hızlı bir başarı göstermiştir.²⁴⁶

GSM ve diğer mobil telefon sistemleri genel olarak 1G sistemlerden kazanılan hücre sistemi, hücreler arası frekansların tekrar kullanımı ve hareketlilik sağlayabilme gibi ortak prensiplere sahiptirler fakat detaylarda farklılıklar gösterirler. Mobil cihaz bu sistemde ahize ve abone-hesap bilgilerinin saklandığı SIM kart denen ayrılabilir bir karttan oluşmuştur. Ahizeyi çalıştıran ağ cihazlarıyla mobil cihazın birbirini tanımlarını sağlayan

²⁴⁶ Tanenbaum Andrew S., 2011, Computer Networks Fifth Edition, Prentice Hall PTR, New Jersey, s.170.

bilgilere sahip olan birim SIM karttır. SIM kart bir ahizeden çıkarılıp başka bir ahizeye takılabilir.²⁴⁷



Şekil 22. GSM Mimarisi

GSM teknolojisi dünya çapında 850, 900, 1800 ve 1900 MHz frekans bantlarını kullanılmaktadır. Daha fazla kullanıcı kapasitesi için geniş bir spektrum ayrılmıştır. GSM frekans bölmeli çift yönlü hücrel bir sistemdir. Her mobil cihaz bir frekanstan görüşmeyi iletirken diğer bir frekanstan alır. GSM’de tek bir frekans çifti birden fazla mobil cihazın kullanımını sağlayabilecek şekilde zaman dilimlerine bölünmüştür. Bunu başarabilmek için GSM kanalları 200-kHz bantlara ayrılmıştır.²⁴⁸

GSM teknolojisinin sahip olduğu zaman yapılandırması sayesinde telefon(mobil cihaz) boş zaman dilimlerinde etrafındaki diğer bazların sinyal değerlerini ölçerek baz istasyonunu bilgilendirir. Baz istasyonu da bu bilgileri telefonun kendi bölgesinden ayrılıp diğerine geçtiğini anlamak ve frekans değişimini yönetmek için kullanır.²⁴⁹

4.5.1.2 2.5G Teknolojisi

2.1, 2.5, 2.9 gibi birçok isimle anılan bu teknoloji grubu 2G ile 3G arasındaki geçiş döneminde kullanılan teknolojilerdir. GSM operatörleri tarafından hızla artan veri trafiğine hızlı bir çözüm bulunması amacıyla kullanılmaya başlamıştır.

“2.5G Nesli” genel olarak 2G şebekelerinin tüm geliştirmelerini ifade eder. Bu geliştirmelerden bazıları planlanan 3G kabiliyetlerinin neredeyse hepsini sağlar. IS-136 sistemleri GPRS ve EDGE’ le, IS-95 sistemleri IS-95B veya CDMA2000 1xRTT geliştirmeleriyle 2.5 G olarak anılmaya başlanmıştır.

²⁴⁷ Tanenbaum, 2011, s.171.

²⁴⁸ Tanenbaum, 2011, s.172.

²⁴⁹ Tanenbaum, 2011, s.174.

GSM şebekelerindeki en büyük sıkıntı düşük veri hızıdır. GSM sistemi 9.6Kbps veri hızı sağlayabilmektedir. Daha sonraları 14.4Kbps hız sağlayan sistemler geliştirilmiş (GSM 1800 MHz) olsa da yaygın olarak kullanılmamıştır.²⁵⁰

2.5G GSM sistemi; HSCSD, GPRS veya EDGE teknolojilerinden en az birini içermektedir.

4.5.1.3 GPRS

GPRS’le birlikte veri hızı teorik olarak 115 Kbps’a kadar ulaşmaktadır. GPRS’in en büyük avantajı sekiz indirme kanallı paket anahtarlamalı bir sistem kullanmasıdır. Bu sayede alıcı kaynaklarını sürekli meşgul etmek yerine sadece veri akışı olduğu zaman kullanmaktadır. Cep telefonu üreticilerinin de tercih etmesinden dolayı birçok GSM operatörü GPRS’i tercih etmiştir. GPRS entegrasyonu HSCSD’ye göre çok daha maliyet gerektirmektedir. Hem sistemde mevcut kullanılan cihazlarda değişiklikler yapılmasını hem de sisteme yeni cihazlar eklenmesini gerektirmektedir. Yine de GPRS 3G sistemlerine geçişte çok ciddi bir atlama taşı olarak görülmektedir.²⁵¹

4.5.1.4 EDGE

Diğer bir geçiş teknolojisi de EDGE’dir. Orijinali “GSM Evrimi İçin Gelişmiş Veri Hızları” iken daha sonraları “Küresel Evrim için Gelişmiş Veri Hızlarının” kısaltması olarak kullanılmıştır.

EDGE teknolojisi 8PSK olarak adlandırılan yeni bir modülasyon düzeni kullanmaktadır. Bu sistem sayesinde standart GSM veri hızı üç kata kadar artırılabilir. Altyapı cihazlarının EDGE için gerekli olan güce dayanması durumunda EDGE sadece baz istasyonlarında yapılacak bir yazılım güncellemesiyle geçilebilecek bir teknolojidir.²⁵²

EDGE GPRS’le beraber kullanıldığında EGPRS olarak adlandırılır ve EGPRS’de en yüksek veri hızı 384 Kbps’dır. EDGE’in HSCSD ile kullanımına da ECSD denir ve standart HSCSD hızının üç katı kadar veri hızı sağlayabilmektedir.²⁵³

²⁵⁰ Korhonen Juha, 2003, Introduction to 3G Mobile Communications Second Edition, Artech House, Norwood, s.5.

²⁵¹ Korhonen, 2003, s.6.

²⁵² Korhonen, 2003, s.6.

²⁵³ Korhonen, 2003, s.7.

4.5.1.5 3G Teknolojisi

Mobil veri iletişimi talebinde artışlar, kullanıcı sayılarının artması ve farklı mobil isteklerin oluşması 3G teknolojilerin kullanımını mecburi kılmıştır.

3G teknolojilere adım atarken artık dünya çapında da ortak standartlar belirlenmeye başlamıştır. IMT-2000²⁵⁴ (International Mobile Telecommunications-2000) olarak adlandırılan ve aslında ITU tarafından tek bir standart olması amacıyla ortaya atılmış “şemsiye özellikler” belirlenmiştir. Her ne kadar bu özellikler teknik ve politik sebeplerden dolayı tek bir standart yapısı olarak hayata geçirilememiş olsa da tüm 3G teknolojilerinde olması gereken temel standartlar olarak kabul görmüştür.²⁵⁵

IMT-2000 şebekelerinin sağlaması amaçlanan temel özellikler ve sağlaması gereken standartların bazıları şunlardır:²⁵⁶

- Yüksek veri hızı (Hareket halinde 144 kbps, açık alanda 384 kbps ve sabit yerde 2 Mbps)
- İnternet erişimi için IP desteği
- İhtiyaca göre dinamik bant genişliği sağlayabilme
- Tek bağlantıyla eş zamanlı farklı servis sağlayabilme
- Sabit hattaki gibi yüksek ses kalitesi
- Dünya çapında ortak frekans kullanımı
- 2G ile beraber çalışabilme
- Uluslararası dolaşım
- Coğrafi konumdan bağımsız hizmet alabilme

Buna bağlı olarak IMT-2000 tarafından 3G cihazları için de bazı anahtar özellikler belirlenmiştir.²⁵⁷

- Dünya çapında ortak, yüksek derecede tasarım
- IMT-2000 ve sabit şebeke hizmetlerinde uyumluluk
- Yüksek kalite
- Tüm dünyada kullanılabilecek küçük cihazlar

²⁵⁴ IMT-2000 adlandırmasında 2000; 2000 yılında servise verilmeye başlanması hedeflendiği, çalışması planlanan frekans olduğu (MHz olarak) ve servis vermesi gereken bant genişliğini(kHz olarak) ifade ettiği için kullanılmıştır.(2,166)

²⁵⁵ Korhonen, 2003, s.13.

²⁵⁶ Martinez Rut Sánchez, 2005, 3G Systems WCDMA (UMTS) & CDMA2000, s. 5.

²⁵⁷ ITU-R, 2000, M.1455-1 No’lu “ Key Characteristics for the International Mobile Telecommunications-2000 (IMT-2000) Radio Interfaces” başlıklı tavsiye kararı, s.1.

- Dünya çapında dolaşım kabiliyeti
- Multimedya desteği

ITU, 1999 Kasım ayında yaptığı toplantıda altyapıları birbirine benzemeyen 5 farklı teknolojiyi IMT-2000 uyumlu olarak ilan etmiştir. Bu tüm önemli teknolojilerin dâhil edildiğini gösteren ve IMT-2000'in aslında tek bir telsiz ara yüzü standardı değil, bir standartlar paketi olduğunu gösteren bir karardır.²⁵⁸

IMT-2000 tarafından uyumlu olarak kabul edilen teknolojiler:

- IMT-DS: IMT Direct Spread (UTRA FDD/WCDMA olarak bilinir)
- IMT-MC: IMT Multicarrier (CDMA2000 olarak bilinir)
- IMT-TC: IMT Time Code (UTRA-TDD/TD-SCDMA olarak bilinir)
- IMT-SC: IMT Single Carrier (UWC-136 olarak bilinir)
- IMT-FT: IMT Frequency Time (DECT olarak bilinir)

İlerleyen zaman içerisinde 3G standartlarını belirlemek amacıyla, temel alınan 2G teknolojilerine göre 3GPP ve 3GPP2 olarak iki farklı grup oluşturulmuştur.²⁵⁹

Bu teknolojilerden sadece CDMA2000 ve UMTS olarak da bilinen WCDMA dünya pazarında hâkim olan iki teknoloji olarak kalmıştır.

4.5.1.6 WCDMA (UMTS- IMT-DS)

WCDMA, CDMA temelli bir teknoloji olup Ericsson firması tarafından geliştirilmiştir. Kullanıcı bilgileri bitleri CDMA yayılım kodlarından türetilen yarı-rastgele bitler (çentikler) ile kullanıcı verileri çarpılarak geniş bir bant üzerinden yayılır. 2Mbps gibi yüksek bir veri hızını sağlayabilmek için değişken bir yayılım faktörü ve Çoklu kod bağlantıların kullanımı desteklenmektedir. Kullandığı 5 MHz bant genişliğinde taşıyıcı kanal başına 3,84Mcp çentik imkânı sağlamaktadır. Geniş taşıyıcı kanal bant genişliği sayesinde yüksek veri hızı ve çoklu yol çeşitliliği gibi performans faydaları sağlamaktadır. Yani operatör sistemine çoklu 5 MHz taşıyıcılar uygulayabilmektedir.²⁶⁰

Devre anahtarlamalı sistemlerin en büyük sakıncası olarak gösterilen iletişim kanallarının veri iletişimi olsa da olmasa da meşgul edilmesi problemi WCDMA'da

²⁵⁸ Korhonen, 2003, s.13.

²⁵⁹ Korhonen, 2003, s.13.

²⁶⁰ Holma Harri, Toskala Antti, 2004, WCDMA for UMTS, Radio Access for Third Generation Mobile Communications Third Edition, John Wiley & Sons, West Sussex, s. 48.

yaşanmamaktadır. WCDMA’da BoD olarak da bilinen veri boyutuna göre bant genişliği ayarlama kabiliyeti oldukça yüksektir. Bir kullanıcının veri hızı 10 ms’lik çerçeve (frame) boyunca sabittir ama aynı kullanıcının her çerçevesinin veri hızı farklı olabilir. Bu hızlı değişken veri hızı şebeke tarafından en uygun veri hizmeti sağlanması için kontrol edilmektedir.²⁶¹

WCDMA’nın telsiz ara yüzü geliştirilmiş CDMA alıcıları (akıllı antenler, çoklu kullanıcı algılama vb.) kavramıyla ifade edilen ve şebekenin kapasitesini ve kapsama alanını geliştirecek seçeneklere uygun şekilde hazırlanmıştır.²⁶²

GSM ile herhangi bir geriye dönük uyumu olmamasına rağmen GSM şebekeleriyle beraber çalışmak üzere tasarlanmıştır. Bununla beraber, bir kullanıcı WCDMA bazından çıkıp herhangi bir görüşme kaybına maruz kalmadan GSM bazına geçiş yapabilir. WCDMA Avrupa Birliği tarafından UMTS adıyla desteklenmiştir.²⁶³

4.5.1.7 Diğer 3G Teknolojileri

Advanced TDMA	IMT-2000 tarafından UWC-136 olarak kabul edilen sistemdir. Kuzey Amerika’da uygulanabilecek altyapısı olmasına rağmen WCDMA’nın tercih edilmesinden dolayı artık desteklenmemektedir.
Hybrid TDMA	Orijinal ETSI UMTS telsiz ara yüzü düzenidir. Desteklenmemektedir.
OFDM	Hiçbir IMT-2000 teknolojisinde uygulanmamıştır. Bazı WLAN uygulamaları kullanılmaktadır. Mobil sistemlerle beraber çalışan WLAN sistemleriyle kullanılma olasılığı hala vardır.

Şekil 23. 3G Teknolojileri

²⁶¹ Holma, 2004, s. 49.

²⁶² Holma, 2004, s.49.

²⁶³ Tanenbaum, 2002, s.167.

4.5.1.8 4G Teknolojiler

Her ne kadar 3G sistemleri geliştirilmiş olsa da hücresel mobil teknolojiler temel olarak ses iletimi için tasarlanmış sistemler oldukları için var olan bant genişliği verimli kullanılamamaktadır. Bundan dolayı veri temelli yeni bir sisteme ihtiyaç duyulmuştur.²⁶⁴

4G kablosuz teknolojisi bu ihtiyaca çözüm olarak geliştirilmiştir. 4G, geniş kapsama alanı ve yüksek veri hızı sağlayan paket anahtarlamalı bir sistemdir. 4G teknolojisinde OFDM, UWB²⁶⁵ ve MIMO²⁶⁶ anten sistemleri kullanılmaktadır. 20 Mbps veri hızı ve mobil hızı 200 km/s olması planlanmaktadır. Çalışma frekans aralığı ise 2-8 GHz'dir. 4G teknolojisi, dünya çapında dolaşım sağlamaktadır.²⁶⁷

ITU-R tarafından 4G teknolojinin sağlaması gereken asgari özellikler IMT-A adıyla şu şekilde belirtilmiştir:²⁶⁸

- Tamamen IP tabanlı, paket anahtarlamalı şebeke
- Yüksek hareketlilik esnasında 100 Mbps ve durağan veya yavaş hareketlilik esnasında 1Gbps veri hızı
- Hücre başına eş zamanlı daha fazla kullanıcı kapasitesi için şebeke kaynaklarının dinamik paylaşımı ve kullanımı
- 5 ile 20 MHz aralığında ölçeklenebilir kanal bant genişliği (opsiyonel olarak 40 MHz'e kadar yükseltilebilir)
- Daha verimli frekans kullanımı
- Heterojen şebekeler arası yumuşak hücre aktarımı
- Dünyada iki nokta arasında en az 100 Mbps veri hızı
- Birden fazla ağ arasında küresel dolaşım
- Mevcut kablosuz standartlarla birlikte çalışabilirlik

2009 Eylül ayında ITU'ya 4G adayı olarak önerilen teknolojiler şunlardır:

- 3GPP tarafından standartlaştırılan LTE-A
- IEEE tarafından standartlaştırılan Wimax

²⁶⁴ Jawwad Ahmad vd., 2003, 4G Wireless Systems, Next-Generation Wireless Working Group, s. 4.

²⁶⁵ UWB, telsiz tayfının çok geniş bir bölümünü kullanarak çok düşük enerji kullanımıyla yüksek bant genişliği iletişimi sağlamak için kullanılması için geliştirilen bir telsiz teknolojisidir.

²⁶⁶ İletişim performansını artırmak için kullanılan akıllı anten sistemidir. Alıcı ve verici olarak çoklu antenlerin birlikte kullanılmasını sağlayan anten sistemidir.

²⁶⁷ Jawwad vd., 2003, s. 3.

²⁶⁸ Roebuck Kevin, 2011, 4G Standard, Emereo Pty Limited, Australia, s. 2.

Mevcut Wimax ve LTE uygulamaları ITU tarafından açıklanan gereksinimlere ulaşmak için geçici bir çözüm olarak görülmektedir. Wimax 2 ve LTE-A ile sonlandırılacaktır. Wimax ve LTE uygulamaları 1Gbps ve 100Mbps gereksinimlerini tam olarak yerine getirememektedir.²⁶⁹

4.5.2 GSM Temel Kavramlar ve Şebeke Elemanları²⁷⁰

GSM mimarisinde *dört* ana bileşenden bahsedilebilir, şöyle ki;

- Cep telefonu (MS – Mobile Station),
- Baz istasyonu (BTS – Base),
- Baz istasyon kontrolörü (BSC – Base Station Controller)
- Santral sistemi (MSC)

4.5.2.1 Cep telefonu (MS: Mobile Station)

İçerisinde SIM kartı barındıran ve GSM iletişimde kullanılan temel cihazdır. Her bir cep telefonunun kendisine ait tekil bir numarası vardır. 15 karakterli bu numara **IMEI** (International Mobile Subscriber Identity) olarak adlandırılır. IMEI numaralarının ilk 14 hanesi o cihaza ait tekil bilgileri içerir. 15. hane ise ilk 14 hanedeki bilgilerin doğrulanması amaçlıdır.

SIM kart ilgili operatör tarafından temin edilen cep telefonunu şebekeye dâhil edilmesi için gerekli bilgileri barındıran akıllı karttır. SIM kart içerisinde; ICCI, IMSI, TMSI, LAI, MSISDN ve Ki bilgileri bulunmaktadır.

ICCI (Integrated Circuit Card Identifier): SIM kartı tanımlayan tekil numara bilgisidir.

IMSI (International Mobile Subscriber Identity): Şebekede aboneyi tanımlayan özel numaradır. Bu sayede abone şebekede tek numarayla değişik servisleri kullanabilmektedir. Bu numara şebekeye ilk girişte kullanılmaktadır.

TMSI (Temporary Mobile Subscriber Identity): Şebekeye kabul edilen cep telefonuna şebeke tarafından atanan bir numara olup şebeke tarafından periyodik olarak

²⁶⁹ Roebuck, 2011, s. 3.

²⁷⁰ Bu Bölüm Vodafone GSM Eğitim Notlarından derlenmiştir.

değiştirilmektedir. Böylece abone bilgileri ve konuşma güvenliği için dinlenmeye karşı ilave bir korunma sağlamaktadır.

LAI (Location Area Identity): Abonenin kendi şebekesi veya tanımlı herhangi bir GSM şebekesindeki hizmet aldığı bölgeyi tanımlar. Bu kod aboneye gelen çağrılar için bağlantı kurulma aşamasında kullanılmaktadır.

Ki: 128 bitlik abone bilgisi ve konuşma güvenliğini sağlamak amacıyla kullanılan bir şifreleme ve sorgulama anahtarıdır. Bu kod her abone için ayrı olup, SIM kart ve AUC'ta kayıtlıdır. Ki kullanılarak MS ile BTS arasında iletilen tüm bilgiler (sinyalleşme ve konuşma) şifreli olarak gönderilir. Şifreleme ve deşifre işlemini sağlayan anahtar kod Ki'dir.

MSISDN (Mobile Station International Services Digital Network): Bu abonenin kullandığı telefon numarasıdır. Ülke kodu, şebeke kodu ve abone telefon numarasının birleşmiş halidir.

4.5.2.2 Baz istasyonu sistemi (BSS: Base Station System)

Baz istasyonu sistemi, şebekede cep telefonu ile MSC arasındaki bağlantıyı sağlayan sayısal ve RF ekipmanlarından oluşmaktadır. BSS cep telefonu ile sayısal hava ortamından (air interface), MSC ile de veri hatları üzerinden bağlantıyı gerçekleştirir.

BSS'in üç temel donanım elemanı vardır:

- Baz istasyonu (BTS)
- Baz istasyonu kontrol birimi (BSC)
- Transcoder (TC)

4.5.2.3 Baz istasyonu (BTS: Base Transceiver Station)

Cep telefonu ile şebeke arasındaki radyo bağlantısı ile ilgili fonksiyonları BTS yerine getirmektedir. Bir BTS ekipmanı bir veya birden fazla hücre (cell) kapsamını sağlayabilir. BTS cihazı:

- Radyo kanal yönetimi,
- Seselelektirikselle formatata dönüştürülmesi ve hava ortamındaki (air interface) iletim formatının şifrelenmesi için gerekli işlemler,

- Radyo frekanslarının gönderimi ve alımı gibi işlevi yerine getirir.

BTS’lerde bulunan hücrelerin kapsama alanlar baz istasyonunun bulunduğu coğrafi konum ve hizmet ettiği bölgedeki muhtemel görüşme yoğunluğuna göre değişiklik göstermektedir. Bir görüşmenin devam ederken başka bir hücreye aktarılması olayı “hand over” olarak adlandırılmaktadır.

4.5.2.4 Baz istasyonu kontrol birimi (BSC: Base Station Controller)

BSC, BSS’in akıllı kısmıdır. Kaynakların yönetimini ve işletme-bakım fonksiyonlarını kontrol eder. Bir BSC birden fazla BTS’i kontrol edebilmektedir. BSC biriminde bağlı bulunan baz istasyonlarının taşıyıcı frekansları, frekans atlama (frequency hopping) listeleri, güç azaltma seviyeleri ve hücrelerin kapsama sınır hesaplarına ait bilgiler tutulmaktadır. BSC’nin şebekede gerçekleştirdiği fonksiyonlar:

- BTS ve TC bağlantısını sağlamak
- Radyo kaynaklarının yönetimi (abone için kanal tahsislerinin yapılması)
- Radyo frekans yönetiminin gerçekleştirilmesi
- Konuşma işlemleri olarak sıralanabilir.

4.5.2.5 Transkoder

GSM sisteminde hava ortamındaki iletimin zorluğu nedeniyle 16 Kbit/s’lik diğer telekom sistemlerinde ise 64 Kbit/s’lik iletim kullanılmaktadır. Transkoder GSM’de kullanılan iletim formatı ile genel telekomünikasyon sistemlerindeki iletim formatı arasındaki dönüşümü sağlamaktadır. Transkoder 16Kbit/s den 64 Kbit/s ve tersi yönde dönüşümü gerçekleştirmektedir.

4.5.2.6 Şebeke Anahtarlama Sistemi (NSS: Network Switching System)

NSS GSM şebekesinin anahtarlama fonksiyonlarını yerine getirir. Abonenin şebeke içinde veya diğer şebekelerle (PSTN ya da diğer GSM şebekeleri) olan bağlantısı NSS üzerinden anahtarlınır. Ayrıca abonelik işlemleri ve abonenin hareketliliği için gerekli veriler NSS’te bulunmaktadır. NSS’in ana bileşenleri şunlardır:

- MSC - Mobile Services Switching Centre

- HLR - Home Location Register
- VLR - Visitor Location Register
- EIR - Equipment Identity Register
- AUC - Authentication Centre
- EC - Echo Celler
- IWF - Interworking Function

4.5.2.7 MSC

MSC NSS alt sisteminin en temel elemanıdır. “Santral” olarak da tabir edilen bu ekipman şebeke içinde ve diğer şebekelerle olan tüm anahtarlama fonksiyonlarını yerine getirir. MS’ten itibaren konuşma bilgisi BSS’ten geçerek MSC’ye gelir ve buradan görüşülmek istenen abonenin bulunduğu yere servis veren BSS gurubuna ya da PSTN şebekeye bağlantısı gerçekleştirilir. Trafik yönlendirmesi ile beraber şu temel fonksiyonları da sağlar:

- BSS kontrolü; trafik kanallarının yönetimi ve tahsis
- Konuşma işlemleri; konuşmanın başlatılması, sonlandırılması, abone mobility işlemleri vs.
- Ücretlendirme
- Anons sistemleri
- Alt servislerle olan bağlantılar; SMS, VMS, WAP vs.

4.5.2.8 HLR

Abone kayıtlarının yapıldığı ve saklandığı kütük dosyalarıdır. Abonelere verilen telefon numaraları HLR’ye kaydedilen numaralardır. Bu numaralar tahsis edildiğinde aboneye ait kimlik bilgisi, ücret tarifeleri, kısıtlamalar ve kullanılacak servisler hakkında bilgiler bu dosyalara kaydedilir. Böylece abone şebekede tanımlanmış olmaktadır. HLR kapasiteleri kayıt edilebilen abone sayısı ile ifade edilirler. Bu bilgiler ile beraber abonenin aktif olarak bulunduğu VLR adresi de HLR’de tutulur ve abone yer değiştirdikçe güncellenir.

4.5.2.9 VLR

VLR aboneye ait aktif işlemleri gerçekleştirmede kullanılan geçici kütüklerdir. Yapı olarak HLR’nin kopyalarıdır. Abone kayıtları sabit dosyalar olan HLR’ye yapılır.

Konuşma işlemleri ve abonenin sorgulama işlemleri bu dosyada bulunan bilgilerle gerçekleştirilmektedir. Abonenin hareketliliği nedeniyle bu bilgilere ulaşmak konusunda bir yük dengesi oluşturmak oldukça güç olmaktadır ve şebekenin performansını etkilemektedir. Abone başka bir bölgeye gittiğinde ona ait bilgileri almak üzere her ihtiyaç olduğunda HLR’ye başvurmak yerine, o bölgeye ait geçici bir kütüğe (VLR) bu bilgiler bir kez kopyalanır. Bu sayede abone o bölgede bulunduğu sürece işlemleri için HLR yerine VLR kullanılarak şebeke sinyalleşme yükü azaltılır ve performansının yüksek olması sağlanır.

VLR’de:

- Abone bilgileri (ücret tarifesı, servisler, kısıtlamalar vs.)
- Abone yer bilgisi (LAI: Location Area Identity)
- Sorgulama bilgileri tutulur. Bu bilgiler ışığında abonelik sorgulaması VLR tarafından yapılır.

VLR’ler de abone sayısı ile ifade edilirler ve genel olarak MSC ile birlikte bulunurlar. Her bir MSC’de yine bir adet VLR bulunmaktadır.

4.5.2.10 EIR

Mobil telefon cihazlarına ait (ME) kayıtların tutulduğu ve kontrol edildiği kütüklerdir. Her telefon cihazının IMEI (International Mobile Equipment Identity) denilen özel bir seri numarası bulunmaktadır. Bu numaralarla telefonlar EIR aracılığıyla kontrol edilirler. Cihazın GSM içinde herhangi bir şebekede kullanımı kısıtlanabilir. Örneğin bir kaçak telefon kara listeye alınır ve bu durumda GSM içinde hiçbir şebekede herhangi bir SIM kartla kullanılmasına izin verilmez.

4.5.2.11 AUC

AUC sorgulama için gerekli parametreleri üretir. Sabit Ki kodu ve rastgele üretilen RAND numarası kullanılarak, sistemde bulunan algoritmalar aracılığıyla SRES – Sign response ve Ki –şifreleme anahtarı üretilir. Bu üç bilgi “triplet” olarak isimlendirilir, sorgulama için VLR’a gönderilir. AUC bu işlemi her abone için ve belirli periyotlarla ya da HLR’nin isteğiyle parametreleri değiştirerek tekrarlar.

4.5.2.12 IWF

GSM şebekesi ile diğer şebekeler arasındaki veri formatında adaptasyonu sağlayan donanım ve yazılımdan oluşan fonksiyonların tamamı IWF olarak isimlendirilmektedir. Bu çoğunlukla yarı bir ekipman olarak değil de MSC'nin bir birimi gibi çalışmaktadır.

4.5.2.13 EC

Sistemde oluşan yankıyı gidermek için kullanılan bir filtre ünitesidir. GSM sisteminde iletimden kaynaklanan gecikmeler nedeniyle oluşan yankı bazen mevcut fonksiyonlar tarafından giderilememektedir. Bu durumda ayrıca bir filtre ünitesine ihtiyaç vardır. Yine özellikle PSTN ile GSM'de kullanılan farklı transmisyon sistemleri nedeniyle bir empedans uyumsuzluğu ve dolayısıyla yankı oluşmaktadır. Bu hissedilir bir yansımadır ve sadece yazılımla bunu gidermek pek mümkün olmamaktadır. Bu nedenle EC genellikle MSC ile PSTN santrali arasına yerleştirilir.

4.6 Mahremiyet ve Gizlilik

Mahremiyet kelime anlamıyla gizli ve özel olma durumudur. Güvenlik açısından ise mahremiyet, bir bilginin herkes tarafından bilinmemesi ve açıklanmasının sahibinin kişisel hak ve çıkarlarına zarar verebilmesi durumudur. Bir diğer ifadeyle, bir bilginin zarar görmesi, yok olması veya farklı ellere geçmesi halinde vatandaşların sağlığına, emniyetine, güvenliğine, ekonomik refahına veya hükümetin etkin ve verimli işleyişine ciddi olumsuz etki edebilmesi halidir.

Son dönemde bilgi teknolojilerinde yaşanan baş döndürücü gelişmeler sonucunda, internet yoluyla iletilen bilgilerin büyük bir kısmını kişisel veriler oluşturmaktadır. Tüm iş ve işlemler elektronik ortama aktarılmış/aktarılmaktadır. Örneğin, dünyada 2,4 milyar internet kullanıcısı vardır ve günlük 144 milyar e-posta gönderilmektedir. Bunun yanı sıra, kişisel, kurumsal ve ulusal açıdan hayati önem taşıyan pek çok bilgi elektronik ortamda bulunmakta olup 634 milyon internet sayfası, 1 milyar aktif Facebook kullanıcısı, 200 milyon aktif Twitter kullanıcısı, 5 milyar telefon kullanıcısı, 1,3 milyar aktif kullanılan akıllı telefon sayısı bulunmaktadır. Ayrıca, ayda 4 milyar saat Youtube'da video seyredilmekte, günlük 300 milyon fotoğraf Facebook'a yüklenmektedir.²⁷¹

²⁷¹ <http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/>, Haziran 2013

Telefon görüşmesinde, e-postalarda, internetten alışveriş yapıldığında, sosyal ağlara girildiğinde kişisel bilgiler paylaşılır ve bize ait özel bilgiler bir yerlerdeki veri tabanlarına kaydedilir. Bu veri tabanlarında saklanan bilgiler analiz edilerek alışkanlıklarımız, davranışlarımız gibi mahrem bilgilerimiz istemediğimiz kişilerin eline geçebilir. Bu bilgiler suçluların yakalanması gibi vakalarda yararlı olabilmekle beraber yanlış kişilerin eline geçmesi durumunda istenmeyen sonuçlara da yol açabilir. Örneğin, ciddi bir hastalığın ilaçlarını aldığımızı öğrenen bir sigorta şirketi hakkımızdaki başka bilgileri de kullanarak bu hastalığa sahip olduğumuza kanaat getirip bizi sigortalamak istemeyebilir. Bankalar, kredi vermeye karar vermek için önceki borçlarımızı ödeyip ödemediğimizin yanında rızamız dışında başka özel bilgilerimizden de faydalanyor olabilirler.

Bazı bilgilerin sadece bize özel kalması olarak tarif edilen kişiye özelliğın sınırlarını çizmek günümüzde hiç de kolay değildir. Özel bilgilerimizi bir taraftan saklamak isterken, bunları paylaşmak durumunda kalacağımız uygulama sayısı da giderek artmaktadır. Örneğin, Akıllı telefonlara indirilen bazı uygulamalar konum gibi bilgileri kullanıcıdan talep etmekte ve kullanıcılar rahatlıkla bu bilgiyi uygulamayı üreten şirketlerle paylaşabilmektedir. Bu servisleri kullandığımız takdirde geçmiş bilgilerimizin kaydının tutulmadığından emin olabilir miyiz?

Bazı kişilerin paylaşmakta sakınca görmediğı bilgileri diğer kişiler sır olarak tutmak isteyebilir. Buna, kullanılan oy bilgisi örnek olarak verilebilir. Kişiyeye özel verilerin kayıt ve takibinde kişinin rızasının olması çok önemlidir. Örneğin, Google'ın Latitude servisinde, sistemden çıkabilir, yer bilgisini paylaşmak istemeyebilir veya başka bir yerde gibi görünebilirsiniz.

Dünyada ve ülkemizde kritik bilgiler ve altyapılar dendiğinde sadece kişisel bilgiler akla gelmemelidir. Daha geniş çerçeveden bakıldığında su, tarım ve gıda, sağlık, enerji, bankacılık ve finans, bayındırlık hizmetleri, ulaşım, sivil yönetim, kamu düzeni, yerel hizmetler, acil hizmetler (sağlık, itfaiye, vb.), bilgi ve iletişim, uzay ve araştırmaları, kimyasal ve nükleer endüstri, askeri iletişim kanalları gibi pek çok farklı kesimde bilgi teknolojileri kullanılmaktadır. Bilgi teknolojilerinin olduğu yerde de bilgi güvenliği özelde kriptoloji bulunmak zorundadır. Kriptoloji temelde kriptografik algoritmalar ve anlık üretilen ve tahmin edilemeyen kriptografik anahtarların kullanımı olarak gösterilebilir.

İletişimin güvenliği o sistemde kullanılan algoritmaların değil o oturumda üretilen anahtarların güvenliğine bağlıdır (Kırşof prensibi).²⁷²

Pek çok insan gündelik hayatlarının her anında bir şekilde özel hayatlarına dair önemli ya da önemsiz bilgilerini bu bilgi sistemleri ile paylaşmaktadırlar. Veri mahremiyeti isteğe bağlı olmamalı ve yasal olarak korunmalıdır. Kuruluşlar veri gizliliği yönetmeliklerine uygun ve veri gizliliği ihlallerini önlemek için hem üretim hem de üretim dışı ortamlarında gerekli prosedürleri bulunmalı ve bu kuruluşlar fiziksel ve en iyi teknik çözümleri uygulamalıdır. (güvenli standartların kullanılması - ISO/IEC 15408 ve 27001)



Verilen çevrimiçi hizmetler, mesafeler uzak olsa dahi insanlar arasındaki iletişimi kolaylaştırmıştır. Ancak, bu hizmetlerin yeni güvenlik problemlerini de beraberinde getirdiği dikkatlerden kaçmaktadır. Bu bilgiler niyeti kötü olan kullanıcılara ulaştığında hiç istenmeyen sonuçlara ulaşmasına sebep olmaktadır. Karşılaşılan bu sorunlar da yine örneğin kriptolama teknikleri gibi yöntemler kullanılarak çözülmeye çalışılmaktadır.

²⁷² A. Kerckhoffs, "La cryptographie militaire", Journal des Sciences Militaires, 9th Series (February 1883), s.161-191.



Bilindiği üzere bir zincir, en zayıf halkası kadar sağlamdır. Bilgi güvenliği konusunda eğitilmemiş veya umursamaz çalışanlar zincirin en zayıf halkası durumundadır. Bu nedenle, bilgi güvenliği kurumlar için çok önemli ve kritik ise kurum çalışanlarının belirli aralıklarla eğitilerek, bu zayıf halkanın güçlendirilmesi gerekmektedir. Bunun yanında, dışardan gelebilecek ataklara karşı “uçtan uca güvenlik” önlemleri almak mümkündür. Uçtan uca güvenlik yerine yukarıdaki şekilde belirtildiği gibi arada farklı bir algoritma kullanılması durumunda güvenlik riski doğabilmektedir, çünkü o noktada bazı şifreli veriler çözüldüğünden saldırı yapılabilmektedir.

Mahremiyet açısından kritik olabilecek veriler aşağıda bir kaç başlık altında sıralanacaktır.

4.6.1 Kişisel Bilgiler

Kişisel bilgiler dendiğinde akla ilk gelecek bilgiler şunlardır: Kimlik bilgileri, adres, iletişim bilgileri (telefon), kişisel fotoğraflar ve videolar, iş, meslek, öğrenim durumu, aile içi mahrem bilgiler. Kişisel bilgilerin tutulduğu bütün kamu kurumları ve özel sektör kuruluşları bu bilgileri güvenli yöntemlerle saklayacağını garanti etmelidir. Bankalardan, sigorta şirketlerine, havayolu şirketlerinden otobüs şirketlerine hatta marketlerde dağıtılan müşteri kartlarına kadar birçok sektörde kişisel bilgiler saklanmaktadır. Bu nedenle yasal bir düzenlemeye gidilmediği müddetçe mahremiyet ülkemizde bir sorun olmaya devam edecektir.

Örneğin, internette çevrimiçi anket yaptırmak isteyen bir web sitesi istemci ve sunucu arasındaki bağlantıyı sağlamak amacıyla “çerezler” kullanmaktadır. Bundan dolayı, tarayıcıda bu çerezlerin kabul edilmesi için tanımlı olması gerekmektedir. Ancak, bu çerezler hiçbir şekilde sizin bilgisayarınızda kişisel ve gizli bilgileri toplamamalıdır.

Bununla birlikte, oturum sona erdiğinde kişisel veya gizli her türlü bilgiyi barındıran çerezler hemen silinmelidir.

4.6.2 TTNET-Phorm Ortaklığı ile Mahremiyet İhlali

TTNET, Phorm ortaklığı kapsamında internet kullanıcılarına ait kişisel bilgileri reklam verenlere satmak amacıyla toplayan gezinti hizmetine bu hizmeti talep etmeyen kullanıcılarını da dahil etmekle suçlanmış ve devam eden süreçte Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından hakkında 1,5 milyon TL para cezası uygulanması kararı alınmıştır. Kullanıcının izni olmaksızın tarayıcısına çerez yerleştiren ve kullanıcının internet alışkanlıklarını bu vesile ile takip eden sistem, daha sonra kullanıcının gezdiği internet sitelerindeki reklamları TTNET'in kendi istediği reklamlar ile değiştirmesine olanak tanıyordu. Karara gerekçe olarak ise Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in "Telekomünikasyonun Gizliliği" başlıklı 8'inci maddesinde yer alan; "Yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının izni olmaksızın, telekomünikasyonun üçüncü şahıs tarafından dinlenmesi, kaydedilmesi, saklanması, kesilmesi veya gözetimi yasaktır..." hükmü gösterilmiştir. Kararda ayrıca gezinti "hizmetinin" talep etmeyen kullanıcıları da kapsamına almasına dikkat çekilmiştir.²⁷³ Bu tür mahremiyeti ihlal eden sistemlerin önüne geçmek için kurumsal bir yapının denetlemelerde bulunması gerekmekte, böylelikle yazılı ve görsel basına sızmamış yasal olmayan olası sistemlerin de önüne geçilebileceği düşünülmektedir.

4.6.3 TürkTrust Hatalı Sertifika Dağıtım

TürkTrust'ın iki müşterisine sağladığı SSL ara sertifikalarının hatalı olduğu ortaya çıkmıştır. Google bu hatayı yayınladıktan sonra Mozilla ve Microsoft şirketleri de konuyla ilgili güvenlik bültenlerinde açıklamalar yayınlamış ve IE, Chrome ve Firefox tarayıcıları yetkisiz sertifikaları bloke etmişlerdir. Bu hatalı sertifikalar "Ortadaki Adam Saldırısı" olarak bilinen saldırı yöntemine olanak sağlamaktaydı. Bu saldırı, bir saldırganın bir ağ üzerinde bilgisayar ile diğer ağ araçları (örn. yönlendirici, modem, sunucu) arasına girerek şifrelenmemiş verileri görebilmesidir. Sahte sertifika, dürüst kullanıcılar güvenli bir biçimde Google veya Gmail web sayfalarına girdiklerini düşünseler bile, belirli bir yönlendirmeye tüm güvenli iletişimin izlenebilmesi imkânını vermektedir. TürkTrust

²⁷³ http://www.btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/TTNET-PHORM.pdf

yetkilileri ilgili sertifikaların hatalı olarak üretildiğini kabul etmiş ve durumun sertifikalar yanlış yerlerde kullanılmadan fark edildiği ve sertifikaların iptal edildiği yönünde açıklama yapmıştır.²⁷⁴

Bu tür bir problemin - ülkemize ait bir web tarayıcı olmadığı için - Chrome, IE, Mozilla gibi web tarayıcıları fark etmeden ülkemiz otoritelerince fark edilmesi mümkün olamamaktadır.

4.6.4 Sağlık Bilgileri

Hekimin mesleğini ve sanatını uygularken hastaları hakkında öğrendiği özel (mahrem) bilgileri, yasal zorunluluk gibi durumlar dışında, saklı tutması gerekmektedir. Sağlıkla ilgili akla ilk gelecek bilgiler şunlardır: gebelik testleri, hastalık geçmişi ve kullanılan ilaçlar, özürllük durumu ve seviyesi, medeni hal, alkol-madde-sigara kullanımı, hastalık şikâyetleri, doktorun hastaya teşhis koyma amaçlı olarak yönelttiği sorular sonucu elde ettiği hastanın öyküsü, hastalıklarla ilgili tetkik sonuçları, 15-49 yaş arası kadınların doğum ve düşük sayıları, kadın sağlığı işlemleri, kullanılan aile planlaması yöntemi, kan grubu, teşhis ve tedavi işlemleri.

Bu bilgilerin kişinin bilgi ve rızası dışında ifşa edilmesinin önlenmesi, ifşası durumunda ise yasal yaptırımı olması gerekmektedir.

4.6.5 Varlık Bilgileri

Gelir ve gider gibi ekonomik durum ile ilgili detaylı bilgiler varlık bilgileri adı altında toplanabilir. Bu bilgilere de erişim sınırlandırılmalıdır. Bu mahrem bilgilerin kötü niyetli kişilerin eline geçmesi durumunda örneğin, bankada yüklü miktarda parası olduğu öğrenilen bir kişi şantaja maruz kalabilir. Benzer şekilde kredi kartı limiti yüksek olan kişilerin kredi kart bilgilerine ulaşılması durumunda bu kişiler hedef haline gelebilir.

4.6.6 Konum/Güzergâh Bilgileri (GPS)

Kişinin bulunduğu konum bilgileri, gittiği yerler ve güzergâhların saklı tutulması gerekmektedir. Akıllı telefonlarla beraber konum bilgileri pek çok uygulama tarafından alınmaktadır. Bu bilgiler de mahrem bilgi olarak kabul edilmekte olup kişinin rızası dışında kullanılmaması gerekmektedir.

²⁷⁴ <https://www.turktrust.com.tr/kamuoyu-aciklamasi.1v2.html>



4.6.7 Teknik Saldırı Yöntemleri ve Amaçları

Teknik olarak bir saldırgan aşağıdaki yöntemleri uygulayarak İnternet yoluyla saldırı yapabilir ve kişisel veya kurumsal gizli bilgileri elde edebilir.

- **Kripto Analiz:** Şifrelenmiş bir metnin şifrelenmemiş düz metin haline getirebilmek için yapılabilecek her türlü kriptografik saldırıları inceleyen bilim dalıdır.
- **Yan Kanal Analizi:**^{275,276} Yan kanal analizinde akıllı kart gibi bir kripto modülünden gizli anahtarı elde etmek için; sistemin kripto işlem gerçekleştirdiği sıradaki güç tüketim karakteristiği, gerçekleştirdiği elektro-manyetik ışıma ya da işlemleri gerçekleştirme süresi gibi yan kanal bilgileri kullanılmaktadır. Örneğin, Basit Güç Analizi (BGA) yan kanal analizinde kullanılan yöntemlerden biri olup bir kripto sisteminde yapılan farklı işlemlerin güç tüketimi eğrisine bakılarak ayırt edilebilmesidir. RSA şifreleme sisteminde kullanılan modüler üs alma işlemlerinde gerçekleştirilen kare alma ve çarpma işlemleri bir birinden ayırt edilebilirse sistem BGA saldırısına açık demektir. Bu sayede gizli RSA anahtarları elde edilebilmektedir.
- **Servis Dışı Bırakma Saldırıları (DoS, DDoS):** Bir sistemin çalışmasını yavaşlatmak, fonksiyonlarının bir ya da birden fazlasını çalışamaz hale getirmek ya da bir sistemi tamamen çökertmek üzere yapılan saldırılara denir. Burada hedef, sistemlerin kaynaklarının tükenmesine veya internet ağ kapasitesinin dolmasına sebep olarak sistemi erişilemez hale getirmektedir.²⁷⁷

²⁷⁵ Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing, NIST, 2005, <http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper19.pdf>

²⁷⁶ Side Channel Attacks, http://en.wikipedia.org/wiki/Side_channel_attack

²⁷⁷ Örnek için bkz. Ian Traynor, The Guardian 17 May 2007: Russia Accused Of Unleashing Cyberwar To Disable Estonia.

- **Oltalama (Phishing):** Gerçek kaynağı belli olmayan fakat güvenilir ve bilinen bir kaynaktan geliyormuş izlenimi vererek –yani bilinen siteleri taklit ederek gerçekleştirilen saldırı türüdür (örn. bankalar, internet üzerinden yapılan kredi kartı ile yapılan işlemler).
- **Sosyal Mühendislik:** İnsanlar arasındaki iletişimi ve insan davranışları analiz ederek açıklıklar tespit edip güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir. En çok kullanılan sosyal mühendislik yöntemlerinin başında e-posta gelmektedir. Hedef kişilere gönderilen e-posta içeriklerinin gerçekçi olması ve e-posta alıcısının eklentiyi açması veya e-posta içeriğindeki adresleri, tarayıcı aracılığı ile açması sonucu bilgisayara zararlı yazılım bulaştırılabilmektedir.
- **Solucan:** Kendisini bir bilgisayardan diğerine kopyalamak için tasarlanan ancak bunu kullanıcı etkileşimi olmadan otomatik olarak yapan bir bilgisayar kodu parçasıdır. Solucan bir kez sisteme girdikten sonra kendi başına ilerleyebilir (örn. İran’ın nükleer sistemine giren Stuxnet solucanı^{278,279} veya 2008 yılından beri aktif olan Conficker gibi).²⁸⁰
- **Brute-Force (Kaba Kuvvet) saldırıları:**²⁸¹ Belli bir şifreleme sistemini kırmak için bir veya birden çok bilginin tüm ihtimallerinin denenerek şifrenin kırılmaya çalışılmasıdır.
- **Truva Atı:** Truva atları yararlı yazılımlar gibi görünen bilgisayar programlarıdır, ancak güvenliğinizi tehlikeye atar ve pek çok zarara yol açarlar. Truva atları, insanların, meşru bir kaynaktan geldiğini düşündükleri bir programı açmaya yönlendirilmeleri yoluyla yayılır ve kişinin bilgisayarında uzaktan yönetim için bir arka kapı açar.
- **Klavye İzleme Yazılımları:** Klavye izleme yazılımları sayesinde klavyeye basılan her tuş kaydedilebilir ve genellikle internet üzerinden saldırganlara gönderilebilir.
- **Casus / Köstebek Yazılımlar:** Potansiyel olarak sistem çalışmalarına zarar veren kodlardır. Küçüklü ya da büyüklü tüm sistemlere zararlı olabilirler (örn. casus

²⁷⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

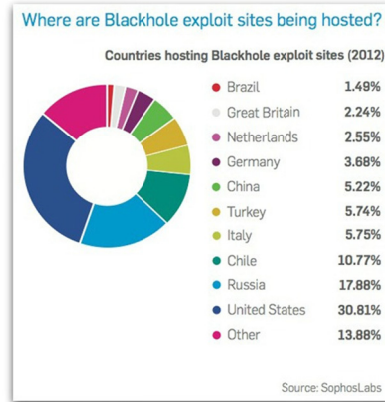
²⁷⁹ <http://www.stuxnet.net/>

²⁸⁰ <http://tech.slashdot.org/story/11/12/02/2224256/was-conficker-stuxnets-trojan>

²⁸¹ Brute-Force Attack, http://en.wikipedia.org/wiki/Brute-force_attack

yazılım yüklenmiş bir bilgisayardan banka şifreleri, e-posta şifreleri, kişisel bilgiler e-posta yoluyla raporlanmış olabilir.)

- **Virüs:** Bir bilgisayardan diğerine yayılan ve bilgisayarın çalışmasını kesintiye uğratan küçük yazılım programıdır. Bir diğer ifadeyle, kendini bir programa veya bir dosyaya iliştirerek bilgisayardan bilgisayara atlayabilen bir bilgisayar kodu parçasıdır. Bir bilgisayar virüsü bilgisayardaki verileri bozabilir veya silebilir, e-posta programını kullanarak diğer bilgisayarlara yayılabilir ve hatta sabit diskteki tüm öğeleri silebilir. Bir e-posta ekinde, bir Web sitesinden yüklediğiniz ücretsiz bir dosyadan veya ortak kullanılan bir disket, CD ya da USB bellekten virüs bulaşabilmektedir.
- **İstem Dışı Elektronik Posta (SPAM):** İnternet üzerinde bir mesajın çok sayıdaki alıcıya, alıcıların isteği dışında gönderilmesidir.
- **İstismar Kiti (Exploit Kit):** Tarayıcıların ve tarayıcı eklentilerinin (Java, Flash Player, PDF Reader vb.) sürümlerini ve açıklıklarını test edip veri tabanında bulunan uygun istismar kodlarını kullanıcıya göndererek tarayıcının veya eklentilerinin istismar edilmesini sağlar. Kullanıcıya hiç fark ettirmeden zararlı bir yazılım indirtip sistemde çalıştırabilen yazılımlardır. (drop-by-download).



Şekil 24. Sophos Labs Araştırma Sonuçları²⁸²

Sophos Labs'ın araştırmasına göre Blackhole isimli kara listede bulunan sitelerin sunucuları en fazla yukarıdaki ülkelerde bulunmaktadır.

²⁸² Sophos Security Threat Report 2013, <http://nakedsecurity.sophos.com/2012/12/04/sophos-security-threat-report>.

- **Ağ Trafiğinin Dinlenmesi:** İki bilgisayar arasında yapılan bilgi alışverişini yakalama olarak adlandırılabilir.
- **Gelişmiş Siber Casusluk Tehdidi (Advanced Persistent Threat):** Bu yöntem, diğer yöntemlerin birkaçının birleştirilmesi ve hedef odaklı olunması olarak açıklanabilir. Bu yöntemde sosyal mühendislik saldırıları ile kurumlara sızılıp, kurumların en kritik bilgileri bile çalınabilmektedir. USB bellek gibi araçların kullanımı ile kapalı ağlardan bilgi sızdırılması, endüstriyel cihazların kontrolünün ele geçirilmesi veya çeşitli tasarım dokümanlarının (yazılım, donanım, ilaç, silah vb.) çalınması en bilinen örneklerdir.

Yukarıda bahsedilen saldırıların pek çok amacı bulunmaktadır. Bunlar kısaca,

- Sisteme yetkisiz erişim
- Sistemi bozmak
- Hizmetleri engellenmek
- Bilgileri değiştirmek
- Bilgileri silmek/yok etmek
- Bilgileri ifşa etmek
- Bilgileri çalmak
- Siber casusluk

şeklinde sıralanabilir.

Hedef sistemlerden çalınan bilgiler kişisel bilgiler, kredi kartı bilgileri olabileceği gibi askeri veya ticari sırlar da olabilmektedir. Çalınan bilgiler kişisel olarak kullanılabildiği gibi kara borsada (underground market) da satılabilmektedir. Örneğin bazı kredi kartlarına ait bilgiler 3-4\$ gibi fiyatlardan satılmaktadır.

Bilgi sistemlerinin güvenliğinin sağlanması için aşağıda verilen konularda çalışmalar yapılmalıdır.

Fiziksel ve Ağ Güvenliği	Donanım Güvenliği	Mobil Cihaz Güvenliği
Haberleşme Güvenliği	Sosyal Ağ Güvenliği	Kritik Altyapı Güvenliği
Yayımlı Güvenliği	İşletim Sistemi Güvenliği	Şifre Güvenliği
Yazılım Güvenliği	Web Teknolojileri Güvenliği	Veri Tabanı Güvenliği
Zararlı Yazılım Analizi		

Kritik altyapılar, devlet kurumlarının ve toplumsal yapının sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasında bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılar olarak sıralanabilir. Kritik altyapıların korunması, gelişmiş ülkelerin önemli gündem maddelerinden birisi olarak karşımıza çıkmaktadır. Bazı ülkeler, kritik altyapıların korunması ile ilgili yasal, teknik, idari, kurumsal ve dokümanter çalışmalarda ciddi yol almışlardır. Ülkemizde de Aralık, 2012 tarihinde Bakanlar Kurulu kararı ile “Siber Güvenlik Kurulu” kurulması kararı alınmış olup Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planına hazırlanmıştır.²⁸³ Bu strateji belgesinin amacı siber dünyada ülkemize yönelik meydana gelebilecek güvenlik ihlallerinin bertaraf edilmesi, engellenmesi, düzeltilmesidir. Dünyada “Siber Savaş” diye tarif edilen savaşların çok basit oluşum veya organizasyonlar yerine çok daha büyük profesyonel organizasyonlarla, oluşumlarla devlet destekleriyle gerçekleştirildiği bilinmektedir. Bu nedenle, hazırlanan bu yol haritası ülkemiz adına çok önemli bir adımdır.

Bu eylem planına göre, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, BTK ve TÜBİTAK’ın sorumluluğunda, Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. Bu kapsamda, Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulması kararı alınmış olup bu hususta TİB görevlendirilmiştir. Mayıs, 2013 tarihi itibarıyla USOM faaliyetine başlamıştır. Başlıca faaliyetler olarak;

- Siber Güvenlik konusunda akademisyen yetiştirilmesi
 - Eylem planına göre siber güvenlik konusunda akademisyenlerin yetiştirilmesi (yüksek lisans ve doktora seviyelerinde burs verilmesi),
- YÖK’te Siber Güvenlik Komisyonunun Kurulması
 - Siber güvenlik altyapısının geliştirilmesi ile ilgili YÖK’te bir komisyon kurulacak, ilgili branşların lisans, lisansüstü ve doktora seviyesi müfredatlarına siber güvenlik ile ilgili derslerin eklenmesi,
 - Siber güvenlik alanında Türkçe kitap, dergi, makale vb. kaynaklarının çoğaltılması,
 - En az iki siber güvenlik yüksek lisans programının açılması,
 - En az bir siber güvenlik doktora programının açılması,

²⁸³ <http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf>

- İlk Orta ve Lise Öğretimde Güvenlik Eğitimlerinin Yaygınlaştırılması
 - İlk, orta ve lise öğretiminde siber güvenlik eğitimleri yaygınlaştırılması,
 - Siber olaylara müdahale merkez ve ekiplerinde çalışan uzmanların eğitimi ve uygulama deneyiminin kazandırılması,
 - Bilgisayar programcılığı meslek liseleri müfredatına siber güvenlik dersi eklenmesi,
 - Müfredatta yer alan bilgisayar derslerinde siber güvenlik konusuna yer verilmesi,
 - FATİH Projesi'ne siber güvenlik eğitimlerinin dâhil edilmesi,
- Üniversitelerde Siber Güvenlik Konusunda Ar-Ge Çalışmaları Yapılması
 - Siber güvenlik konusunda, Ar-Ge laboratuvarları kurulması,
 - Zararlı yazılımları ve bu yazılımların bilişim sistemlerinde yaptığı etkileri belirleyebilecek laboratuvar altyapısı kurulması,
 - Üniversitelerde siber güvenlik konusunda Ar-Ge laboratuvarlarının kurulması teşvik edilecek ve destekleyecek programlar oluşturulması,
 - Eylem planına göre, siber güvenlikte yerli ürün ve çözüm çalışmaları da yapılarak yerli kaynaklardan da yararlanılması,
- Siber Güvenlik Milli Güvenliğe Entegre Edilmesi
 - Siber saldırılar, milli güvenliği tehdit eden saldırılar olarak ulusal siber güvenliğin milli güvenliğe entegrasyonunun sağlanması,
 - Siber ortamda meydana gelebilecek çeşitli olaylarda devreye girecek mekanizmaların mevcut durumunun analizi ve iyileştirilmeleri için gerçekleştirilmesi gereken öncelikli eylemlerin belirlenmesi,
 - Türkiye'ye yönelebilecek olası saldırı senaryolarının ve bunların yol açabileceği etkiler belirlenmesi,
 - Siber ortamda çeşitli siber güvenlik olayları meydana geldiğinde, kurumların sorumluluklarının ve ulusal düzeyde koordinasyonunun nasıl sağlanacağı belirlenmesi, ulusal siber savunma konusunda strateji geliştirilmesi,
- Bilgi Sistemlerinden Üst Düzey Yöneticiler Bilgilendirilmesi
 - Siber güvenlik eğitim altyapısının güçlendirilmesi kapsamında kurumların bilgi sistemlerinden ve siber güvenliğinden sorumlu üst düzey

yöneticilerin bilgilendirilmesi, teknik personelinin eğitilmesi ve eğitime katılan personele sertifika verilmesi,

- Siber güvenlik alanında ulusal ve uluslararası mevzuatın incelenmesi ve ihtiyaç duyulan yasal düzenlemelerin tespit edilmesi,

hedeflenmektedir.

4.7 Veri Güvenliği ve Kriptoloji

Kripto, genel bir ifadeyle mesajların önceden belirlenmiş bir kodlama mekanizması ile gizlenmesidir. Kriptoloji ise şifre bilimidir. Çeşitli iletilerin, yazıların belli bir sisteme veya kurala göre şifrelenmesi, bu mesajların güvenli bir ortamda alıcıya iletilmesi ve iletilmiş şifreli mesajın çözülmesiyle uğraşır.

Temelde dünyada şifreleme sistemlerini kullanan kriptografik yöntemler standarttır (askeri ve gizli uygulamalar bunun dışında tutulabilir). Gizliliği sağlayan ana öge ise kriptografik anahtarlardır. Bu nedenle tüm kullanıcılardan kendilerine ait özel anahtarını gizli tutmaları ve başkalarına vermemeleri beklenir. Şifreye alternatif olarak akıllı kart gibi güvenli modüller kullanılabilir. Aslında güvenlik sistemleri farkında olunmasa da hayatın her alanına girmiştir. Bilgisayar, telefon veya bankamatik kullanan birisi farkında olmadan şifreleme yapıyor demektir. Bankacılık işlemlerinde, kredi kartı ile alışveriş yapıldığında, internette bilet satın alındığında size açık görünen işlemlerin arka kısmında şifreleme yapılmaktadır.



Geçmişte kriptoloji sadece iletişimin gizliliğini korumak için kullanılırdı. Ancak günümüzde kriptoloji sadece iletişimin gizliliği bağlamında değil telefonlardan

bilgisayarlara, taşınabilir belleklerden veri merkezlerine birçok yerde bulunan gizli veya mahrem bilgilerin güvenliğinin de sağlanabilmesi için de gerekmektedir.

Güvenli iletim ve saklamanın yanı sıra kriptoloji, yeni kripto teknikleri kullanılarak kişiye özel kalma ya da bir diğer ifadeyle anonimlik hizmeti sağlayan güvenli hesaplama sistemlerinde de kullanılmaktadır. Örneğin, A ve B bankalarının ticari gizli verileri bulunsun. A ve B bankaları kendilerine özel verilerini birbirleriyle paylaşmak istemesinler, ancak yine de bu verileri kullanarak belirli bir analizi (veri madenciliği) yapmak istesinler.²⁸⁴ Görülüyor ki, veri gizliliği ve güvenli iletim yöntemleri bu problemi kolay ve hızlı bir şekilde çözemeyecektir. Bu tür mahremiyet koruyan ve güvenli hesaplama sistemlerinin gelecekte yaygın olarak kullanılması düşünülmektedir (örn. elektronik para, elektronik seçim, elektronik müzayedede, elektronik noter, şifreli metin arama ve elektronik açık arttırma).²⁸⁵



Bilgi teknolojilerinin güvenliğinin temel gereksinimleri olan veri gizliliği, bütünlük, erişilebilirlik, inkâr edilemezlik, kimlik doğrulama ve erişim denetiminin en net biçimde tanımlanabildiği sistemler veri tabanı sistemleridir.

Veri tabanında tutulan bilgilerin güvenli bir şekilde üretildiğinin, iletildiğinin ve kaydedildiğinin garanti edilmesi gerekmektedir. Daha teknik bir ifadeyle, erişilebilirlik, bütünlük, gizlilik, inkâr edilemezlik ve kimlik doğrulama gibi kriptografik hizmetlerin sağlanabilmesi gerekmektedir. Örneğin, yetkisiz bir kullanıcının bu verilere ulaşamayacağının garanti ve ispat edilmesi gerekmektedir. Bunun yanında, veri tabanına iletilen ve saklanan verilerin hiçbir şekilde yetkili kullanıcıların haberi olmadan değişikliğe uğramayacağının garanti edilmesi gerekmektedir. Son olarak, veri tabanında tutulan

²⁸⁴ Yehuda Lindell and Benny Pinkas. Secure Multiparty Computation for Privacy-Preserving Data Mining, The Journal of Privacy and Confidentiality, 2009.

²⁸⁵ Secure Multi-Party Computation, http://en.wikipedia.org/wiki/Secure_multi-party_computation.

bilgiler istendiği anda erişilebilir olması gerekmektedir. Bu nedenle, bir kuruluş için kendine has veri tabanının yangında kurtarılabilecek ilk IT sistemi olması gerektiği düşünülebilir, zira taşıdığı ve servis ettiği verilerle kuruluşun dışarıdan temin edemeyeceği, yeniden yapılandıramayacağı tek bileşendir.

Günümüzde veri tabanı sistemleri taşıdığı verinin önemi ve bu alanda uzun yıllardır yapılan çalışmalar sebebiyle en sağlam çalışması gereken sistemlerdir. Bu sistemlerin düzgün bir şekilde 7/24 esasına göre çalışması için güvenli altyapılar üzerine kurulup doğru bir şekilde yapılandırılması ve güvenli bir şekilde yönetilmesi gerekmektedir.



4.7.1 Veri Tabanı Güvenliği

Veri tabanı sistemleri bilgi çağının en önemli bileşenlerinden biridir ve her kurum için hayati önem taşırlar. Veri tabanı güvenliği kurumların elektronik bilgilerinin hızla artması ve regülasyonların zorunlulukları nedeniyle önemini arttırmıştır. Veri güvenliği, verinin bozulmaması, veriye doğru kişinin eriştiğinden emin olunması, verinin gizliliğinin korunması konularını kapsar. Diğer bir deyişle verinin güvenliğinin sağlanması için gizlilik, erişilebilirlik ve bütünlük hizmetleri göz önünde bulundurulmalıdır.

Günümüzde her vatandaşın özel veya kamu kuruluşlarıyla ilişkileri bulunmaktadır. GSM şirketleriyle ve internet servis sağlayıcılarıyla kişisel bilgiler ve iletişim bilgileri, Sosyal güvenlik kurumlarıyla ile kişisel bilgiler ve ödeme bilgileri, tapu kadastro müdürlükleriyle mal varlığı bilgileri, belediyelerle fatura bilgileri, emniyet müdürlükleriyle kişisel bilgiler ve pasaport bilgileri, yine nüfus müdürlükleriyle ve işyerleriyle kişisel bilgilerimizi paylaşılmaktadır. Kişisel bilgilerin paylaşıldığı kurum/kuruluş sayısı arttıkça ortaya çıkan risk de o nispette artmaktadır. Şöyle ki, bazı kuruluşlar bilgilerin muhafazası konusunda daha hassas davranırken bazı kuruluşlarca yeterli hassasiyetin gösterilmemesi durumunda bu bilgiler rahatlıkla saldırganların eline geçebilecektir. Mevcut durum yerine kurulacak bir otoritenin tüm kişisel bilgileri en yüksek güvenli bir şekilde saklamaya

yetkili ve sorumlu olmasının, özel veya kamu kurumlarından gelen istekleri kriptografik olarak mahremiyeti ihlal etmeden sağlayabilmesinin daha ileri seviyede koruma sağlayacağı değerlendirilmektedir.

Veri tabanı sistemlerinin erişilebilirlik hizmetini engelleyecek temel nedenler aşağıdaki gibi özetlenebilir:

- Yedekleme ve kurtarma politikalarının belirlenmemesi/testlerinin gerçekleştirilmemesi,
- Veri tabanı şemasındaki tasarım hatalarından dolayı veri tabanının yavaş servis sağlaması ve/veya hiç servis sağlayamaması,
- Veri tabanına tasarım ve/veya yazılım zafiyetleri sebebiyle verebilecek hizmet engelleme (DoS) saldırıları,

Bilişim sistemlerini oluşturan altyapı, donanım, yazılım ve uygulamalara bir saldırganın izlemesi öngörülen yöntemler kullanılarak yapılan saldırı ve müdahaleler sonucunda güvenlik açıklarının tespit edilip bu zafiyetler kullanılarak sistemlere sızılmaya çalışılması, bu açıkların nelere sebep olabileceğinin incelenmesi ve sonuçların raporlanmasına Sızma (Penetrasyon) Testi denir. Bu testler veri tabanı yönetim sistemi yazılımlarında bulunabilecek açıklar ve bu açıkların sebep olduğu zafiyetlerin testini de içermektedir. Sunulan sızma test hizmetleri arasında: Web uygulaması testleri, DNS servisi testleri, kablosuz ağ sızma testleri, mobil cihaz güvenlik testleri, ATM sızma testleri, iç ağ sızma testleri, sosyal mühendislik testleri, sunucu ve servis genel güvenlik testleri, ağ ve iletişim cihazları güvenlik testleri ve değerlendirmeleri, güvenlik duvarı (firewall) ve IDS/IPS cihazları güvenlik testleri ve değerlendirmeleri, sanallaştırma ortamı güvenlik testleri, domain ve PC güvenlik testleri, veri tabanı güvenlik testleri ve değerlendirmeleri, DoS/DDoS testleri bulunmaktadır.

Saldırı Önleme Sistemleri, saldırı tespit ve önleme sistemleri olarak da bilinen ağ ve/veya sistemi kötü niyetli aktivitelerden korumak için, trafiği izleyen ağ güvenlik cihazlarıdır. Siber saldırı önleme sistemleri (Intrusion-Detection System - IDS), ağ üzerindeki trafiği sürekli olarak izleyen ve şüpheli bir paketle karşılaştığında (türüne ve ayarlarına göre) bu paketi kaydeden, ağ yöneticisine alarm gönderen ve güvenlik duvarı üzerindeki ilgili trafiği kapatarak ağ güvenliğini sağlayan cihaz ya da yazılımlardır. Bu sistemin temel görevi kötü niyetli aktiviteleri belirlemek, kötü niyetli saldırıları durdurmak ve saldırının türünü rapor etmektir.

4.7.2 Bulut Bilişim Güvenliği



Şekil 25. Bulut Bilişim

Bulut bilişim (Cloud computing), bilişim aygıtları arasında ortak bilgi paylaşımını sağlayan hizmetlere verilen genel addır. Burada “Bulut” sözcüğü dosyaların sağlandığı konumu işaret etmektedir. Hotmail, Yahoo Mail, Google Mail, Ubuntu, Dropbox, Picasa, Flickr, Google Docs vb. hizmetler düşünüldüğünde Bulut Bilişimin çoktan birçok kimsenin hayatında yerini aldığı görülmektedir. Bulut bilişim ile internet erişimi olan bir bilgisayardan istenen verilere erişilip normal bir bilgisayarda yapılabilecek tüm işlemler - yüksek işlem kapasitesi gerektirebilecek işlemler de dâhil - yapılabilmektedir. Daha genel ifadeyle bulut bilişim, temel kaynaktaki yazılım ve bilgilerin paylaşımı sağlanarak, mevcut bilişim hizmetinin; bilgisayarlar ve diğer aygıtların - elektrik dağıtıcılarına benzer bir biçimde - bilişim ağı (örneğin internet) üzerinden kullanılmasıdır. Bulut bilişim ile beraber düşük donanım ve yazılım maliyeti, gelişmiş performans, anında yazılım güncelleme, sınırsız depolama/yedekleme kapasitesi, artırılmış veri gizliliği ve güvenliği, farklı işletim sistemleri arasında sorunsuz geçiş gibi pek çok yenilik sunulmaktadır.



Klasik bir algı olarak işleme ve saklama konumlarının aynı aygıtta bulunması durumu klişeleşmiştir. Ancak günümüzde artan saklama boyutu ihtiyaçları, saklama ortamlarını bulutlara yani saklama ve altyapı hizmeti barındıran hizmetlere doğru kaydırmaktadır. Bu değişimin öncüsü, internet sağlayıcıları tarafından yedekleme amacıyla sunulan bulut uygulamalar olmuştur.



Bulut bilişim muhtemel faydalarının yanında, veriler hangi noktalarda saklanacak ve işleneceği, üçüncü şahısların bu bilgilere erişiminin nasıl düzenleneceği ve en önemlisi bilgilerin saklandığı yer ile ilgili nasıl bir hukuki düzenleme getirilmesi gerektiği şeklinde pek çok soruyu da beraberinde getirmektedir.

4.7.3 Kamu Kurumlarının Ortak Ağ ve Veri Tabanı

4.7.3.1 Dünyadaki Uygulamalar ve Hâlihazırda Ülkemizdeki Durum

Bulut bilişim konusunda Cisco, HP, IBM, NetApp, EMC ve Microsoft gibi uluslararası şirketlerin yatırımları her geçen gün artmaktadır. Örneğin, Microsoft Windows işletim sisteminin internet üzerinden çalışmasını hedeflemektedir. Google gibi uluslararası bilişim şirketleri ise; Google Docs gibi çevrim içi bilgi işleme özelliği sunan uygulamalar geliştirmiştir. Ayrıca; Amazon, Microsoft ve Intel gibi büyük teknoloji firmaları da; bu teknolojiyi bilişim tüketicilerine sunmuşlardır.

Ülkemizde ise Turkcell, Türk Telekom, Avea, Vodafone Türkiye ve TTNET şirketleri KOBİ'lere yönelik bulut bilişim hizmetleri sunmaktadırlar.

4.7.3.2 Bilim ve Teknoloji Yüksek Kurulu Kararları

Türkiye'de bilim politikalarının oluşturulmasında en yüksek karar mercii olan Bilim ve Teknoloji Yüksek Kurulu'nun (BTYK) 25. toplantısında Ulusal Veri Merkezi Çalışmalarının yapılması hedeflenmiş, bu kapsamda kamu kurumlarının veri merkezlerinin birleştirilmesine yönelik hukuki, teknik ve idari yapılanma modelinin oluşturulması ve Türkiye Kamu Entegre Veri Merkezi'nin kurulması çalışmalarının yapılmasına karar verilmiştir.²⁸⁶

Ülkemizde kurumlar e-Devlet hizmetlerini verebilmek için kendi altyapılarını geliştirmektedirler. Diğer taraftan dünyadaki örnekler incelendiğinde veri merkezlerinin birleştirilmesine dair eğilim gözlemlenmektedir. Örneğin Güney Kore'nin 48 merkezî kamu idaresinin bilgi sistemleri 2 ayrı şehirde konumlandırılacak şekilde tek bir veri merkezinde birleştirilmiştir. Bu sayede yedeklilik, felaket kurtarma merkezi, siber güvenlik, iş sürekliliği, kamu bulutu, etkin işletme maliyeti, kurumlar arası veri paylaşımı gibi isteklerin tamaminin yerine getirilmesi amaçlanmıştır.

ABD, bulut bilişim ve ortak veri merkezi yaklaşımlarıyla 2015 yılına kadar 800'den fazla veri merkezini kapatmayı planlamakta, bu kapsamda 2015 yılı sonu itibarıyla 3 Milyar ABD Doları tasarruf etmeyi öngörmektedir. Ülkemizde de idari ihtiyaçlar, mali tasarruf ve siber güvenlik gereksinimleri doğrultusunda, halen her kurumda müstakil olarak işletilmekte olan veri merkezlerinin tek bir çatı altında birleştirilerek Türkiye Kamu Entegre Veri Merkezi'nin kurulmasının önem arz ettiği değerlendirilmektedir.

²⁸⁶ http://www.tubitak.gov.tr/sites/default/files/62_2013_104.pdf.

BEŞİNCİ BÖLÜM

SONUÇ VE ÖNERİLER

20. yüzyılın ikinci yarısından sonra, teknolojinin her alanında baş döndürücü bir hızla meydana gelen gelişmeler, kişinin vazgeçilmez ve en temel hakları olan özel hayatın ve haberleşme özgürlüğünün gizliliğini tehdit eder hale gelmiştir.

Hayatımızın vazgeçilmezleri haline gelen cep telefonu, internet, radyo ve televizyon gibi kitle iletişim araçları, bir yandan hayatı kolaylaştırmakta, bir yandan da bu araçlar kullanılarak en gizli alanlara kolaylıkla müdahale edilmekte ya da insanlar haberleşme gizlilik ve hürriyetlerinden haberleri dahi olmadan mahrum bırakılabilmektedir. Bunun yanı sıra kişilerin ya da devlet kurumlarının özel alanlarını koruma konusunda gösterdikleri ihmal bu duruma eklendiğinde ortaya temel hak ve hürriyetleri tehdit eden bir tablo çıkmaktadır.

Haberleşme ve bilgi güvenliği ile ilgili en ufak bir zafiyet, en yüksek düzeyde güvenlik açığını beraberinde getirmektedir. Bütün bunlar ise haberleşme özgürlüğü ve özel hayatın gizliliğine yönelik her türlü saldırıya karşı önleyici tedbir alınması gerekliliğini ortaya koyduğu gibi, çağımızın en temel hak ve hürriyetleri arasında sıralanan bu kavramlara yönelik somut saldırıların da bazen en ağır şekilde cezalandırılması gerektiğini de açığa çıkarmıştır. Toplumun ve devlet kurumlarının bu saldırılara karşı etkili bir biçimde korunması gerekliliği her gün kendisini biraz daha fazla hissettirmektedir. Bilinmelidir ki hukuk devleti olmanın başlıca yolu, temel hak ve hürriyetleri güvence altına alabilmekten geçmektedir.

Bütün bu değerlendirmeler, özel hayatın ve haberleşmenin gizliliği ile korunması hakkının önemini ortaya koymaktadır. Ancak temel hak ve özgürlüklerden olan haberleşme özgürlüğü ve özel hayatın gizliliğine, Anayasa'nın 22'nci ve 13'üncü maddeleri ile Avrupa İnsan Hakları Sözleşmesi'nin 8'inci maddesi uyarınca, millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması nedenlerinden biri veya birkaçına bağlı olarak, ancak kanunla ve demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine uyulmak şartıyla müdahale söz konusu olabilmelidir. İşte özel hayatın gizliliğinin, haberleşmenin gizliliği ile özgürlüğünün korunması ve güvence altına alınması yönünden hâlihazırdaki yasal, idari, teknik ve bilimsel mekanizmaların araştırılması, bu konularda ortaya çıkmış eksiklerin belirlenip tedbirlerin alınması, bu hakkın sahip ve öznesi konumunda olan kişi ya da kurumların daha bilinçli hale getirilmesi için nasıl bir

çalışma yapılması gerektiği sorunu, Türkiye Büyük Millet Meclisinde haberleşme özgürlüğüne ve özel hayatın gizliliğine yönelik ihlallerin tespiti ve önlenmesine ilişkin tedbirlerin belirlenmesi amacıyla bir Meclis Araştırması Komisyonu kurulmasına sebep teşkil etmiştir.

Yukarıda belirtilen amaçları gerçekleştirmek üzere Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan Meclis Araştırması Komisyonumuz, oldukça yoğun bir çalışma temposu ile, İktisat hükümlerinin öngördüğü zaman dilimi içerisinde yaptığı çalışmalar sonucunda, her ülkede olabileceği gibi, ülkemizde de haberleşme özgürlüğüne ve özel hayatın gizliliğine yönelen somut, şahsi, bazen de organize tehditlerin var olabildiğini tespit etmiş ancak kamuoyunda yerleşmiş olan **“hepimiz dinleniyor ve izleniyoruz”** algısının teknik olarak mümkün olamayacağı sonucuna da ulaşmıştır.

Komisyonumuzca, yargı kurumlarınca yürütülmekte olan ve kamuoyunun yakından takip ettiği özel hayatın gizliliğine yönelik ihlallere ilişkin somut bazı davalardan olan Cumhuriyet Halk Partisi eski Genel Başkanı Deniz Baykal, Milliyetçi Hareket Partisi milletvekili adayları ve Adalet ve Kalkınma Partisi Genel Başkanı ve Başbakan Recep Tayyip Erdoğan’ın yasa dışı dinlenmesi ve izlenmesi hakkındaki soruşturma ve kovuşturmalara ilişkin Anayasa’nın 138’inci maddesinin üçüncü fıkrasında ifadesini bulan *“görülmekte olan bir dava hakkında Yasama Meclisinde yargı yetkisinin kullanılması ile ilgili soru sorulamayacağı, görüşme yapılamayacağı veya herhangi bir beyanda bulunulamayacağı”* hükmü gereğince herhangi bir araştırma yapılmamıştır.

Ülkemizde dinleme ve izleme cihazları, piyasada rahat biçimde tedavül edebilmekte, üretimi, satılmaları, taşınmaları, bulundurulmaları yasal olarak herhangi bir izne ya da ruhsata tabi kılınmayan eşya görünümü arz etmektedir. Ayrıca, ülkemizde dinleme ve izleme cihazları ile ilgili ithalat rejimi denetiminin oldukça zayıf olduğu, üretim ve ithalat rejimlerinin kayıtsızlığı ve denetimsizliği yüzünden, bahsi geçen bu cihazların gerçek kullanım amacı dışında beyan edilen başka bir isimle ya da tamamen kaçak yollarla ülkemize sokuldukları izlenmektedir.

Yürürlükteki ceza hukukumuzda, özel hayat ve haberleşmenin gizliliği kavramlarının, sadece özel olarak dinleme, izleme kast ve amacına dönük olarak üretilmiş cihazlarla değil, cep telefonu, kamera, bilgisayar gibi asıl olarak başka amaçlarla bulundurulmuş tüm teknolojik cihazlar aracılığıyla ihlal edilmesi, cihazlar arasında ayrım

yapılmaksızın suçtur ve TCK'nın 132'nci ve devamındaki diğer maddeleri çerçevesinde cezayı gerektirmektedir.

Kamuoyunda dinleme ve izleme cihazlarının yasa dışı amaçlarla kullanımının önüne geçebilme düşüncesinden hareketle, bunların üretim veya ithalinin tamamen yasaklanması hatta bu eylemler için hürriyeti bağlayıcı ceza ya da para cezalarının getirilmesi gerektiği yönünde fikirler bulunduğu görülse de, bazı durumlarda her yönüyle yasal nitelik arz eden kameralı, ses kaydı yapabilen cep telefonu ve benzeri cihazların da suç işleme kast ve iradesi ile birleştğinde, rahatlıkla haberleşme özgürlüğü ve özel hayatın gizliliğine yönelik ciddi bir tehdide dönüşebildiği görüldüğünden; bu cihazların üretimi, ithali, bulundurulması, sevki ile ilgili olarak bu cihazların beyan edilen amaçlara uygun kullanılıp kullanılmadığı ile ilgili bir denetim mekanizmasının hayata geçirilmesinin uygun olacağı değerlendirilmiştir.

Toplumu oluşturan bireylerin mahrem alanlarının ihlali suretiyle gerçekleştirilen eylemlerin zaten niteliği gereği gizlice işlendiği bilinmekte, şikâyet şartı yokluğu, delil yokluğu ya da yetersizliği, mağdurun işlenen suçtan habersiz olması gibi çok farklı sebeplerle ancak çok azının yargı kurumlarının önüne getirilebildiği görülmektedir. Bu yönüyle sadece yasal teminatları geliştirmek yerine, ilave olarak özel hayat ve haberleşmenin gizliliği ve özgürlüğü kavramlarının en temel toplumsal bir değer olarak kabulü için daha kapsamlı çalışmalar yapılması gerekmektedir.

Komisyon çalışmaları sonucunda, aşağıda hukuki ve teknik olmak üzere iki ayrı başlık altında sıralanan somut önerilerin hayata geçirilmesinin, ülkemizde yaşanan haberleşme özgürlüğüne ve özel hayatın gizliliğine yönelik ihlallerin önlenmesi noktasında hayati önem arz etmekte olduğu değerlendirilmiştir.

5.1 Hukuki Öneriler

1. Kişisel verilerin korunması hakkındaki kanun tasarısı taslağının bir an önce yasalaşması gerekmektedir.

28 Ocak 1981 tarihinde imzaya açılmış olan ve 1985 yılında yürürlüğe giren 108 sayılı Otomatik Olarak İşlenen Kişisel Veriler Bakımından Bireylerin Korunması Hakkında Sözleşme, Türkiye tarafından imzalanmış, ancak onaylanamamıştır. Çünkü Türkiye'nin bu Sözleşmeyi onaylanabilmesi için Sözleşmeye imza atan devletin öngörülen ilkeler çerçevesinde bir kanun kabul ederek iç hukukunda yürürlüğe koyması zorunludur.

Söz konusu uluslararası Sözleşmenin amacı; sözleşmeyi imzalayan devletlerin sınırları dâhilinde tüm vatandaşların, ulus ve ikametleri her ne olursa olsun, hak ve özgürlükleri ile kişiye ait otomatik işleme girmiş tüm kişisel bilgileri ekseninde, herkesin özel yaşamını korumaktır (Madde 1). Sözleşmeye göre; "kişisel bilgi", kişi hakkında belirlenmiş veya belirlenebilecek her türlü bilgidir. Kişisel bilgilerle ilgili işlemler denilince de kişiler hakkında veri depolanması, bu veriler üzerinde mantıksal veya matematiksel işlemler yapılması (işlenmesi), kişilerin bu verilerinin düzeltilmesi veya silinmesi ya da yeniden yapılandırılması veya yayılması olarak anlaşılmaktadır. (Madde 2)

Avrupa Konseyinin “24 Ekim 1995 Tarihli Kişisel Nitelikli Verilerin Değerlendirilmesi ve Bu Verilerin Serbest Dolaşımına Karşı Gerçek Kişilerin Korunması Üzerine 95/46 Sayılı Direktifi de bu konuda önem arz eden uluslararası düzenlemelerdendir. Yine Bilişim teknolojisinin hızlı gelişimi nedeniyle bu Direktifi takiben yetersizliklerin önlenmesi amacıyla 2002 yılında; “Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması”na ilişkin 2002/58/EC sayılı Direktif kabul edilmiştir.

Türkiye tarafından uyum mevzuatı çerçevesinde “Kişisel Verilerin Korunması Hakkında Kanun Tasarısı” hazırlanarak Bakanlar Kuruluna sevk edilmiş, 7.4.2008 tarihinde kabul edilerek TBMM Başkanlığına 22.04.2008 tarihinde gönderilmiştir. Ancak 23. Yasama Döneminde görüşülemeyen kanun tasarısı kadük olmuştur.

Buna göre; Kişisel Verilerin Korunması ile ilgili 95/46 sayılı Direktif ile 108 sayılı Sözleşme dikkate alınarak, iç hukukumuzda uyarlanıp bir “Tasarı” hazırlanmışsa da, 1981 yılından itibaren kişisel verilerin gizliği hakkında bir kanun kabul etmek suretiyle sorun çözülmüş değildir. Hülasa iç hukukumuzda her ne kadar Kişisel Verilerin Korunması kavramı, “anayasal ve cezai koruma” altına alınmış olsa da, ülkemiz yönünden kişisel verilerle ilgili “özel bir kanun” yoktur. Bu nedenle kişisel verilerin korunması hakkındaki kanun tasarısı taslağının bir an önce yasalaşması gerekmektedir.

2. Türkiye Büyük Millet Meclisi Genel Kurul gündeminde 240 sıra sayısı ile yer alan “Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı”nın yasalaşmasına öncelik verilmelidir.

Bilgi teknolojilerine ait ürünler ve bilgi toplumu hizmetleri modern bireyin günlük hayatını çepeçevre kuşatmış bulunmakta ve başta bilgisayarlar olmak üzere, internete bağlanabilen cep telefonları, çeşitli kamu hizmetlerinin bilişim ağları üzerinden

verilebilmesi, modern hayatta insanlığın yaşamını kolaylaştırmaktadır. Modern hayatta bireylerin yaşamını kolaylaştıran bu teknolojik ürünlerin ticaretinin çoğunlukla elektronik ortam üzerinden gerçekleştirildiği gerçeği karşısında bu alan yapılacak yasal düzenlemenin son derece önemli olduğu görülmektedir.

Dinleme ve izleme cihazları ticaretinin de diğer teknolojik ürünlerde olduğu gibi ağırlıklı olarak internet üzerinden yapıldığı görülmektedir. Bu bağlamda elektronik ticareti düzenleyen bir kanun çıkarılmasının dinleme ve izleme cihazlarının alım-satımına da sınırlandırma getireceği değerlendirildiğinden Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı’nın bir an önce yasalaştırılması gerekmektedir.

3. Dedektiflik kurumunun TBMM gündemine yeniden taşınarak yasal bir altyapıya ve standartlara kavuşturulması ve bu konuda mesleki standartlar belirlenmesi gerekmektedir.

Günümüzde artık birçok ülkede bu hizmetler, bazılarında özel bir dedektiflik/araştırma yasası, bir kısmında ise ticaret yasasına göre kurulan şirketler tarafından yürütülmektedir. Çıkış itibarıyla aynı dönem ve tarihe rastladıkları için de birçok ülkede “özel güvenlik ve özel dedektiflik” aynı yasa içinde düzenlenmiş, öz olarak da şirket kuruluş, ABD, Fransa, İspanya’da olduğu gibi ruhsata bağlanma ve kurucularda aranan şartlar aynı olmakla sadece faaliyet alanları farklı belirtilmekle yetinilmiştir.

Ülkemizde ise, 20.01.1994 tarihinde TBMM’de 3963 sayılı “Özel Dedektifler Kanunu” çıkartılmışsa da, 4 Şubat 1994 tarihinde dönemin Cumhurbaşkanı tarafından Anayasa’nın 89’uncu maddesi gereği bir defa daha görüşülmek üzere TBMM’ne iade edilmiş, geri gönderme tezkeresi, 17.03.1995 tarih ve İçişleri Komisyonunda görüşülerek gerekli düzeltmeler yapılmış olmakla birlikte TBMM’de tekrar gündeme alınmadığı için yasalaşamamıştır.

Bu gün ülke genelinde özellikle internet üzerinden yapılan sorgu ile, bu alanda birçok özel dedektiflik şirketine ait sitenin bulunduğu görülecektir. Bu şirketlerin hizmet verdikleri alanlar incelendiğinde, “eş takibi”, “evlilik öncesi araştırma”, “adres araştırması”, “dinleme ve izleme cihazlarının tespiti ve bunlara karşı öneyici teknolojilerin geliştirilmesi”, “dolandırıcılıklarda fail tespiti”, “öğrenci takibi”, “kayıp şahıs takibi”, “borçlu takibi” gibi birçok farklı alanda çalıştıkları görülmektedir.

Yukarıda sözü edilen faaliyet alanları incelendiğinde, dedektiflik şirketi adı altında yapılan bu firmaların, toplumumuzda var olan sosyal ve hukuki bazı ihtiyaçların devlet otoritesi ve müdahalesi dışında daha hızlı, sorunsuz çözebilme arzu ve isteği sebebiyle varlık kazandıkları, kimi faaliyet alanlarının Anayasa ve kanunlarda ifadesini bulan temel hak ve özgürlüklere, haberleşme ve özel hayatın gizliliği ilkelerine uygun olabileceği, ancak örneğin “evlilik öncesi araştırma”, “adres araştırması” gibi bazı faaliyet alanlarının ise özel hayatın gizliliği ilkesini açık biçimde ihlal edecekleri, ancak son tahlilde, ülkemizde “dedektiflik” kurumunun yasal bir alt yapıya kavuşturulmadan yapılacak tüm değerlendirme ve yorumların “afaki” olarak kalacağı tartışmasıdır.

Bu sebeplerle, İçişleri Bakanlığı ve Emniyet Genel Müdürlüğünün, konu ile ilgili farklı ülkelerin bu konudaki uygulamaları da incelenmek suretiyle güncel bir çalışma yapması sağlandıktan sonra, dedektiflik kurumunun TBMM gündemine yeniden taşınarak yasal bir altyapıya ve standartlara kavuşturulması, oluşturulacak standartlara uygun olmayan “dedektiflik” kurumlarının bir suç örgütü gibi çalışabilecekleri dikkate alınarak, faaliyetlerinin derhal yasaklanması şarttır.

4. İzleme ve dinleme cihazlarının üretimi, ithali, bulundurulması, sevki ile ilgili olarak İçişleri; Ulaştırma, Denizcilik ve Haberleşme; Bilim, Sanayi ve Teknoloji ile Gümrük ve Ticaret Bakanlıklarının bu cihazların beyan edilen amaçlara uygun kullanılıp kullanılmadığı ile ilgili bir denetim mekanizması ya da duruma göre diğer bazı tedbirlerin yanında “ruhsat” modeli ile ilgili tedbir ve önlemleri hayata geçirmeleri gerekmektedir.

Bilindiği gibi ülkemizde dinleme ve izleme cihazları, piyasada rahat biçimde tedavül edebilmekte, üretimi, satılmaları, taşınmaları, bulundurulmaları yasal olarak herhangi bir izne ya da ruhsata tabi kılınmayan eşya görünümü arz etmektedir.

Ayrıca, ülkemizde dinleme ve izleme cihazları ile ilgili ithalat rejimi denetiminin oldukça zayıf olduğu, üretim ve ithalat rejimlerinin kayıtsızlığı ve denetimsizliği yüzünden, bahsi geçen bu cihazların gerçek kullanım amacı dışında beyan edilen başka bir isimle ya da tamamen kaçak yollarla ülkemize sokuldukları izlenmektedir.

Mevcut sorunun çözülebilmesi için gümrüklerde bu konuda görev üstlenecek yeterli uzman istihdamının sağlanması, dinleme ve izleme cihazlarının gerçek işlevlerinin ne olduğunun belirlenerek, ülkeye giriş sırasında belirli kıstasların ve denetimlerin geliştirilmesi gerektiği, üretilen veya ithal edilen bu türden elektronik cihazların

uluslararası standartlara, kendi alt yapımıza, sistemlerimize uygunluğunun ve bu cihazların beyan edilen amaçlara uygun kullanılıp kullanılmadığı ile ilgili denetim mekanizması getirilmesi gerektiği, bu sayede kayıt dışı işlemlerin de kontrol altına alınabileceği düşünülmektedir.

Buna karşın kamuoyunda dinleme ve izleme cihazlarının yasa dışı amaçlarla kullanımının önüne geçebilme düşüncesinden hareketle, bunların üretim veya ithalinin tamamen yasaklanması hatta bu eylemlere karşılıklı hürriyeti bağlayıcı ceza ya da para cezalarının getirilmesi gerektiği yönünde fikirler bulunduğu görülse de, bazı durumlarda her yönüyle yasal nitelik arz eden kameralı, ses kaydı yapabilen cep telefonu ve benzeri cihazların da suç işleme kast ve iradesi ile birleştiğinde, rahatlıkla haberleşme özgürlüğü ve özel hayatın gizliliğine yönelen ciddi bir tehdide dönüşebildiği, kaldı ki nasıl bir tabanca, tüfek gibi ateşli niteliği haiz insan hayatı gibi en önemli değer yönünden tehlikelilik arz eden silahların da tüm bu niteliklerine rağmen, meşru müdafaa ve diğer bazı hukuka uygunluk sebepleri ile kullanılabildikleri gözetilerek üretim ve ithallerinin sıkı belli kurallar çerçevesinde gerçekleştirilebildikleri, bu anlayış ve çerçeveden bakıldığında pek tabidir ki dinleme ve izleme cihazlarının da her ne kadar bunca yasa dışı fonksiyonlarına rağmen, bazen de evlilik ve boşanma hukuku gibi alanlarda, başka türlü ortaya konması mümkün olmayan bazı olguların ispatı ile ilgili bu sefer de yasal fonksiyonlar üstlenebildikleri müşahade olunabilmektedir.

Nitekim Yargıtay uygulamalarında da, bazen şeklen hukuka aykırı gibi görünen dinleme ve izleme cihazları ile kaydedilen bazı ses ya da görüntü kayıtlarının, elde edilen yöntemlerine bakılmaksızın hukuka uygun olduklarına ilişkin oldukça isabetli kararlara yer verildiği, bu bağlamda Yargıtayın 2013 yılı içerisinde ulusal basına da konu olan bir boşanma davasının yerel ilk derece mahkemesinin davanın reddine dair verdiği kararın temyizi üzerine verdiği kararında, koca tarafından eşinin bilgisi dışında evine ses ve görüntü kayıt cihazı yerleştirerek kendisini aldattığına dair kayıtların bulunduğu CD'yi yasal delil olarak kabul etmeyen yerel mahkemenin kararını “eşinin sadakatinden kuşkulanan tarafın, her ikisinin de ortak mekânı olan konutta, eşinin bilgisi dışında ses ve görüntü kayıt cihazı yerleştirerek, eşinin aleni olmayan konuşmalarını kaydetmesinde, özel hayatın gizliliğinin ihlali ile hukuka aykırılık bulunduğu kabul edilemeyeceği” gerekçesiyle bozularak, belli bazı hukuki şartlar çerçevesinde izleme ve dinleme cihazları ile “yasal delil” elde etmeye cevaz verildiği gözlenmektedir.

Yine Yargıtay Ceza Genel Kurulunun 2013 yılı içerisinde verdiği bir kararında, şikâyetçi işadınının irtikâp suçu işlendiğini kanıtlamak için mahkeme kararı olmadan dinleme ve izleme cihazıyla yaptığı ses ve görüntü kaydının, yasal olmayan delil niteliği taşıdığı gerekçesiyle Yargıtay 5. Ceza Dairesince sanıkla ilgili beraat kararı verilmesine rağmen, kararın Yargıtay Cumhuriyet Savcısı ve mağdur işadınınca temyizi sonrasında, söz konusu kayıtların yasal delil olduğuna hükmedilerek Yargıtay 5. Ceza Dairesinin beraat kararının bozulduğu ve cezalandırma kararı verilmesine hükmedildiği görülmektedir.

Aslında Yargıtayın yukarıda bahsi geçen uygulamalarında vurgulanan husus, genel bir hukuki kaideye işaretle, aniden ve fiili bir durum olarak gerçekleşen bazı hukuki olguların ispatına ilişkin delillerin, hukuk nezdinde şeklen yasaya aykırı gibi görünen yollarla elde edilseler de, elde ediliş kast ve kullanım amaçları itibarıyla meşru bir amaç hedeflenmiş ise, yine eğer bu delilleri elde edenlerden o anda başka türlü delil elde etmeleri de akla, mantığa ters ise, delilin artık yasal olduğunun kabulü gerektiğidir.

Sonuç olarak, yürürlükteki ceza hukukumuzda, özel hayat ve haberleşmenin gizliliği kavramlarının, sadece özel olarak dinleme, izleme kast ve amacına dönük olarak üretilmiş cihazlarla değil, cep telefonu, kamera, bilgisayar gibi asıl olarak başka amaçlarla bulundurulmuş tüm teknolojik cihazlar aracılığıyla ihlal edilmesi, cihazlar arasında ayırım yapılmaksızın suçtur ve TCK'nın 132'nci ve devamındaki diğer maddeler çerçevesinde cezayı gerektirmektedir. Günümüzde artık kabul etmelidir ki faildeki suç işleme kast ve iradesi altında özel hayatın gizliliğini ihlal edebilecek en tehlikeli tehditlerden birisi, akla fikre gelmeyen teknolojik yetenekleri haiz cep telefonlarıdır. O halde, özel hayat kavramına yönelik tehdidi, ihlal sırasında kullanılan cihazın özel olarak dinleme ve izlemeye hasredilip edilmemesine bakmadan cezalandırmak gerekmektedir. İhlal edilen ve korunması artırılması gereken kavram, özel hayatın gizliliği olmakla, bu eylemin cezasının artırılması ya da tayin edilecek cezalarla ilgili kişiselleştirme tedbirlerine yönelik önerilere başka bir maddede değinileceğinden, burada daha fazla üzerinde durulmasına gerek duyulmamıştır.

Bu çerçeveden bakıldığında dinleme ve izleme cihazlarının tamamen yasaklanması veya bunları üreten, ithal eden, bulunduranlara ceza getirilmesinin mevcut sorunu çözemeyeceği, ceza verme mantığından hareket edildiğinde, bu cihazların bazı şartlarda üstlenebilecekleri faydalı hukuki-fiili fonksiyonların da engellenebileceği, bu fikirden

hareketle yukarıda da sözü edildiği gibi üretilen veya ithal edilen bu türden elektronik cihazların uluslararası standartlara, kendi alt yapımıza, sistemlerimize uygunluğunun ve bu cihazların beyan edilen amaçlara uygun kullanılıp kullanılmadığı ile ilgili bir denetim mekanizması, hatta belki de öyle ya da böyle yukarıda üzerinde durulduğu kadarıyla savunulabilir hukuki menfaatin bulunabileceği özel durumlarda ihtiyaç duyanların bu cihazları edinebilmelerine yönelik bir tür “ruhsat” model ve tedbirinin getirilmesinin uygun olabileceği kanaatine ulaşılmıştır.

Dinleme ve izleme cihazlarının ithalat, üretim ya da duruma göre “ruhsat” modeli ile ilgili tedbir ve önlemlerin, İçişleri; Ulaştırma, Denizcilik ve Haberleşme; Bilim, Sanayi ve Teknoloji ile Gümrük ve Ticaret bakanlıklarının müşterek çalışmasıyla yürütülmesi gerektiği, ayrıca Bilgi Teknolojileri Kurumu bünyesinde çalışan Piyasa Gözetim ve Denetim Laboratuvarının bu süreçte aktif bir rol ve çaba üstlenmesi, cihazların denetimi için gümrüklerde bilişim uzmanlarının istihdam edilmesi gerektiği değerlendirilmektedir.

5. Ceza Muhakemesi Kanunu’nun 134 ile 140’ıncı maddeleri arasında düzenlenen ceza usul hukuku ile ilgili tüm işlemlere dair kararların, ihdas olunacak özel yetkili hâkimliklerce verilmesi ve izlenmesi için yasal düzenlemeye ihtiyaç bulunmaktadır.

Kamuoyunda mevcut “yasa dışı dinleme” ile ilgili kaygı ve korkunun yoğunluk düzeyi gözetildiğinde, Ceza Muhakemesi Kanunu’nun 134 ile 140’ıncı maddeleri arasında düzenlenen bilgisayarlar da yapılacak arama, el koyma, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, kararların yerine getirilmesi, iletişim içeriklerinin yok edilmesi, tesadüfen elde edilen deliller, gizli soruşturmacı ve teknik araçlarla izleme işlemleriyle ilgili görev yapacak olan, konusunda uzman, müstakil ve müstemir yetkili özel hâkimliklerin kurulması, bu mahkemelerin personelinin titizlikle ve bu konuda uzman kişilerden seçilmesi ve tüm bu ceza usul hukuku işlemlerinin konusunda uzmanlık sahibi olacak hâkimlerce gerçekleştirilmesi, bu hâkimliklerin ise denetimi ile ilgili özel prosedürlerin öngörülmesi, artık bir zorunluluk olarak görülmelidir.

Ayrıca müstemir yetkili bu hâkimliklerin, zabıta birimlerinde bulunan iletişimin tespiti sırasında kullanılan odalarda görev yapan polis-jandarma görevlilerinin disiplin amiri sıfatını taşıması ve bu personelin özel olarak seçilmesi, dinleme odalarına giriş çıkışların yeterli teknolojik karmaşıklıkla içeren özel şifreli kapılar aracılığıyla yapılması,

ve tüm bunların tamamen müstemir yetkili hâkimin kontrolünde olması gerektiği ve sıralanan hususlarda yasal düzenlemelere ihtiyaç bulunduğu anlaşılmaktadır.

6. Ceza Muhakemesi Kanunu’nun 134 ile 140’ıncı maddeleri arasında düzenlenen ceza usul hukuku ile ilgili tüm işlemlere dair kararların mağduru olduğunu iddia edenlere tazminat talebi hakkı getirilmelidir.

Ceza Muhakemesi Kanunu’nda, haksız tutukluluk ya da elkoyma tedbirleri sonucu mağdur olanların, 141’inci maddede maddi ve manevi tazminat talebinde bulunabilmesi ile doğrudan devletin sorumluluğunun kabul edildiği, ancak her nedense telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, kararların yerine getirilmesi, iletişim içeriklerinin yok edilmesi, tesadüfen elde edilen deliller, gizli soruşturmacı ve teknik araçlarla izleme işlemleriyle ilgili böyle bir tazminat sorumluluğu öngörülmediği bilinmektedir.

Yukarıda sayılan haksız tutukluluk ve elkoyma tedbirleri dışındaki diğer tedbirlerin haksız olarak tatbikinden de ciddi maddi ya da manevi zararların doğabileceği gözetilerek, Ceza Muhakemesi Kanunu’na ilave bir düzenlemeyle, devletin “telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, kararların yerine getirilmesi, iletişim içeriklerinin yok edilmesi, tesadüfen elde edilen deliller, gizli soruşturmacı ve teknik araçlarla izleme” işlemlerde hak kaybının olması ve kişilik haklarına açıkça saldırının gerçekleşmiş olması hallerinde tazminin sorumlu olması esası getirilmelidir.

7. Ceza Muhakemesi Kanunu’nun 135’inci maddesine kaybolan, öldüğünden şüphe edilen ya da bir suç neticesinde özgürlüğünden mahrum bırakıldığı değerlendirilen kişilerin sinyal bilgilerinin değerlendirilebileceğine dair hüküm konmalıdır.

Ceza Muhakemesi Kanunu’nun 135’inci maddesinin iletişimin tespiti, dinlenmesi ve kayda alınmasıyla ilgili esasları düzenlediği, ancak kaybolan, ölen, öldüğü ya da bir suç neticesi özgürlüğünden mahrum bırakıldığı değerlendirilen kişilerin yerinin tespiti veya benzer nitelikte özel bazı durumlarda sinyal bilgilerinin değerlendirilmesi ile ilgili herhangi bir konuya yer verilmediği görülmektedir. Mevcut yasal zemin çerçevesinde, her ne kadar zabıta ve soruşturma makamlarınca ilgililere yardım sağlandığı haricen bilinse de, bu konuda hâlihazırda mevcut yasal bir standardın bulunmadığı gözden uzak tutulmamalıdır.

Yukarıda sayılan kimi hallerde belki de ortada somut bir suç şüphesi bulunduğu kesinlik kazanmasa da, toplum menfaat ve düzenini yakından ilgilendiren bu konuda bir

düzenleme yapılarak, belli standartlar dâhilinde soruşturma makamlarınca sinyal bilgilerinin değerlendirilebilmesi ve zor durumda bulunan, ölen, ya da ölümünden şüphelenilen kişilere ulaşılmaya çalışılması bir gerekliliktir.

İletişimin dinlenmesi, kaydedilmesi, tespiti ve sinyal bilgilerinin değerlendirilmesi tedbirlerinin amacı suçla ilgili olarak delil elde edilmesidir. CMK'nın 135'inci maddesinin dördüncü fıkrasında düzenlenen mobil telefonun yerinin tespiti tedbirinin amacı ise şüpheli veya sanığın yakalanmasıdır. Amacı farklı olan bu denetim şeklinin ayrı bir maddede düzenlenmesi ve bu tedbire başvuru koşullarının da açık bir şekilde belirtilmesi yararlı olacaktır.

8. Türk Ceza Kanunu'nun özel hayata ve hayatın gizli alanına karşı suçlar bölümünde yer alan suçlara dair cezalarla ilgili olarak, cezaların artırılması yoluna gidilebileceği gibi seçenek yaptırımlar, erteleme ve hükmün açıklanmasının geri bırakılması tedbirlerinin uygulanmamasına ya da bu konuda kısıtlayıcı tedbirlere ilişkin hükümlere yer verilebilir.

Toplumlar karmaşık yapılı modern tiplere doğru geliştikçe, hukuk sistemlerindeki cezalandırıcı kuralların, tüm kurallara oranı azalmak, buna karşılık iade edici/tazmini nitelikteki hukuk kurallarının tüm kurallara oranı ise gittikçe büyümektedir.

Nitekim Yeni Türk Ceza Siyaseti ışığında yerleşmeye başlayan yaptırım modelinin de "tazmin edici adalet", yani failin cezasının şiddetlendirilmesinin değil, mağdurun yarasının sarılmasını referans aldığı söylenebilir.

Tazmin edici adalet yaklaşımı, geleneksel yaptırım sistemine göre; suç mağdurlarına el uzatılması, yardım sağlanması, tazmin şartının suçlunun kendisine bir şey yapılması yerine onun bir şeyler yaparak suç sonrası ortaya çıkan olumsuz durumun iyileştirilmesine katkı yapabilmesi, bütçe giderlerinde önemli ölçüde tasarruf sağlanabilmesi ilkeleri çerçevesinde farklılaşmaktadır.

Tüm bunlara karşın rasyonel bir ceza siyaseti, kimi durumlarda suçun ciddiyet göstergesine toplumda yerleşik algı doğrultusunda yalnızca hürriyeti bağlayıcı ceza niteliği ile vurgu yapılabileceğinden hareketle, mücadeleye rağmen baş gelinemeyen ya da ağır nitelik arz eden suç ve suçlu tiplerine karşı "tazmin edici adalet" ilkelerinden uzaklaşarak, hürriyeti bağlayıcı ceza ile cevap verilmesi gerektiğini emreder. Nitekim bizim ceza

hukukumuz da dâhil olmak üzere birçok modern ceza yasaları bu yaklaşım tarzı doğrultusunda ortaya çıkan ağır ya da hafif birçok hürriyeti bağlayıcı cezalarla doludur.

Toplumuzda yasa dışı dinleme ve izlemelerle, haberleşme gizliliği ile özgürlüğüne yönelik tehdit içeren somut eylemlerin bulunduğu yönünde çok açık bazı bulgu ve emareler olduğundandır ki bu konuda TBMM bünyesinde bir araştırma komisyonu kurulması gerekliliği hâsıl olmuştur. Öyleyse, sözü edilen eylemleri işleyen faillerin cezalandırılması ve tayin edilecek cezaların şahsileştirilmesiyle ilgili TCK ve CMK’da mevcut “erteleme”, “seçenek bazı yaptırımlara çevirme” ve “hükümün açıklanmasının geri bırakılması” ile ilgili yasal tedbirlerin yeniden gözden geçirilmesinin, gerekirse bu suçlar yönünden bu tedbirlere gidilmesinin kısıtlanması ya da tamamen kaldırılması yönünde yasal değişikliklere gidilmesinin yerinde olacağı düşünülmektedir.

Bununla birlikte özellikle iletişimin denetlenmesi tedbirinin uygulamasında, soruşturma ve kovuşturma aşamasında görev alan kişilerin bu suçu işlemesi halinde cezalarında yapılan artırımın daha fazla olması bu fillerin caydırıcılığı konusunda daha etkili olacaktır.

9. Ceza Muhakemesi Kanunu’nun 138’inci maddesinin ikinci fıkrasının değiştirilerek, Polis Vazife ve Salahiyet Kanunu’nun ek 7’nci maddesinin ikinci fıkrası ile 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu’nun ek 5’nci maddesine hüküm eklenerek, tesadüfen delil elde edildiğinde derhal Cumhuriyet savcılığına bildirme ve delilin bizzat cumhuriyet savcılığınca muhafaza altına alınması yükümlülüğü getirilmesi gerekmektedir.

Ceza Muhakemesi Kanunu’nun 138’inci maddesinin ikinci fıkrasında, ilgili zabıta birimlerince telekomünikasyon yoluyla yapılan iletişimin denetlenmesi esnasında yapılmakta olan soruşturma ile ilgisi bulunmayan ve ancak, 135’inci maddenin altıncı fıkrasında sıralanan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edildiğinde, delilin zabıta makamlarınca muhafaza altına alınarak durumun Cumhuriyet savcısına derhal bildirileceğine ilişkin hükme yer verilmiştir.

Ancak, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi konusunda kamuoyunda hâlihazırda mevcut algı ve konunun özel önemi dikkate alınarak, Ceza Muhakemesi Kanunu’nun 138’inci maddesinin ikinci fıkrasında, soruşturma sürecinde bu nitelikte tesadüfi delil elde edildiğinde hemen ve derhal Cumhuriyet savcısına bilgi verilerek delilin kolluk güçlerince değil, bizzat Cumhuriyet savcısı tarafından muhafaza

altına alınmasının sağlanması yönünde değişiklik yapılması, yine aynı sakinca ve gerekçelerle Polis Vazife ve Salahiyet Kanunu'nun ek 7'nci maddesi ile 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun ek 5'inci maddesine, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi esnasında yapılmakta olan soruşturma ile ilgisi bulunmayan ve ancak, 135'inci maddenin altıncı fıkrasında sıralanan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edildiğinde hemen ve derhal Cumhuriyet savcısına bilgi verilerek delilin kolluk güçlerince değil, bizzat Cumhuriyet savcısı tarafından muhafaza altına alınmasının sağlanması yönünde hüküm ilave edilmelidir.

Bu konuda Yargıtay kararlarında kolluğun tesadüfen delil elde ettiğinde kendiliğinden muhafaza altına aldığı, savcıya veya hâkime haber vermediğinden bazı dosyalarda bozma kararı verildiği görülmektedir. Bu tarz kanununa aykırı sonuçların önüne geçilmesi bakımından kolluğun dinleme sırasında tesadüfen başka bir suç işlendiğini haber aldığına durumu derhal savcıya bildirmelidir. Savcı gerekli görmesi halinde delilin muhafaza altına alınmasına, elkonulmasına veya iletişimin bu yeni suç için de denetlenmesine dair karar almak üzere hâkime başvurup başvurmamayı takdir etmelidir. Böylece kolluğun kendiliğinden işlem yaparak telafisi mümkün olmayan sonuçlar doğmasının önüne geçilmesi amaçlanmaktadır.

Örneğin uyuşturucu veya uyarıcı madde imal ve ticareti (Madde 188) suçundan dinleme yapılırken adam öldürmeye dair delil elde edildiğinde kolluk bu suçtan dinlemeye kendiliğinden devam etmeyecek savcıya durumu bildirecektir. Savcılık gerekli görürse iletişimin denetlenmesine dair karar alacak veya adam öldürmeye dair bir delile ulaşılmışsa (mesela suçta kullanılan silah) elkoyma prosedürünü uygulayacaktır.

Bu konuda kanunda veya ikincil mevzuatta yapılacak bir değişiklik yanlış uygulamaların önüne geçecektir.

10. Özel hayatın gizliliğini ihlal edebilecek bilgilerin, adli soruşturma ve kovuşturma dosyalarında yer almasının kısıtlanması ile ilgili idari ve yasal tedbirler alınmalıdır.

Avrupa İnsan Hakları Mahkemesi, tedbirin uygulanması sonucu yapılan kayıtların gizliliği ve korunması ile ilgili koşulların belirli olmamasını AİHS'nin 8'inci maddesinin

ihlali olarak değerlendirmektedir.²⁸⁷ Mevzuatımızda, tedbir kararlarının uygulanması aşamasında ve uygulanmasından sonra tedbirin uygulanması sonucu elde edilip, ilgili kolluk birimlerinde muhafaza edilen veya tedbirin sona ermesini müteakip Cumhuriyet Başsavcılıklarına ve mahkemelere teslim edilen kayıtların ne şekilde korunması gerektiğine dair yeterli hükümler bulunmaması nedeniyle yapılacak bir başvuru halinde AİHM'nin Türkiye aleyhine benzer bir karar vermesi kuvvetle muhtemeldir²⁸⁸. Bu nedenle tedbir sırasında ve sonucunda elde edilecek verilerin nasıl nerede kimler tarafından muhafaza edileceği mevzuatta ayrıntılı bir şekilde düzenlenmelidir.

Ayrıca iletişimin denetlenmesi tedbirinde elde edilen tüm veriler dosyaya dâhil edilmektedir. Fiziken dosya içerisinde muhafaza edilmese de bu kayıtlar dosyanın bir parçasıdır. Bu kayıtlar içerisinde delil niteliği taşıyan kayıtların yanında hiç bir delil niteliği olmayan tamamen özel hayatı ilgilendiren mahrem bilgiler de yer almaktadır. İleride gelebilecek itiraz ve savunmalarda bu kısma da atıf yapılabileceği düşüncesiyle bu kayıtlar yok edilmemekte, delil olabilme ihtimaline karşı dosyada muhafaza edilmektedir. Soruşturma aşamasında gizlilik kararı alınarak bu kayıtların öğrenilmesi kısmen engellenebilirse de kovuşturma aşamasında bu mümkün olmamaktadır. Alenileşen yargılama sırasında taraflar delil olan kayıtlar yanında tarafların mahrem bilgilerine de vakıf olabilmektedirler. Bu durumun önüne geçilmesi amacıyla savcının iddiasını dayandırdığı deliller haricinde kalan bilgilerin dosyadan ayrılması gerekmektedir. Bu ayrılan özel bilgilerin şüpheli veya sanık rızası olmadan dosyaya dâhil edilmemeli ve ilerde delil olabilme ihtimaline karşı emanet gibi özel ve güvenli bir yerde muhafaza edilmelidir. Bu kayıtların açıklanmasına talep üzerine ve dosya etkisi olacağı görülmesi durumunda yine hâkim karar vermelidir. Uygun görülmesi durumunda bu aşamanın başlaması soruşturma da çekilebilir. Savcı tarafından şüpheli lehine veya aleyhine hiçbir atıf yapılmayan bu kayıtların hiç bir kimse tarafından öğrenilememesi yargılamanın amacına da uygun olacaktır.

²⁸⁷ Kruslin/Fransa, pg.35; <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=kruslin&sessionid=1650805&skin=hudoc-en>. (Erişim tarihi: 22.3.2007).

Aynı yönde bkz. Huvig/Fransa, pg.34 <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=huvig&sessionid=1650896&skin=hudoc-en> (Erişim tarihi: 22.3.2007).

²⁸⁸ Kaymaz, s. 368-370.

11. Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi ile ilgili tüm işlemlerde işlem sonrası yapılacak geri bildirimlerin hem fiilen dinlenen şahsa hem de hat sahiplerine yapılması ile ilgili yasal tedbirler alınmalıdır.

Bilindiği gibi ülkemizde çok farklı sebeplerle telekomünikasyon araçlarına dair hatların kayıtlı olundukları kişilerle bunları fiilen kullanan ve istifade eden kişiler farklı kişiler olabilmektedir. Bu sebeple uygulamada fiilen dinlenen kişi ile hat sahibi olan kişi farklı olduğunda bir takım tereddütler oluşmakta, adli soruşturma ve kovuşturma makamlarınca birçok zorlukla karşılaşılabilmektedir.

CMK'nın 137'nci maddesinin dördüncü fıkrasında "Tespit ve dinlemeye ilişkin kayıtların yok edilmesi halinde soruşturma evresinin bitiminden itibaren, en geç on beş gün içinde, Cumhuriyet Başsavcılığı, tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgisine yazılı olarak bilgi verir." hükmüne yer verilmiş olmasına rağmen uygulamada zaman zaman dinlenen kişilere geri bildirimde bulunulduğu ancak hat sahiplerine bilgi verilmediği ya da tam tersi durumların yaşandığı görülmektedir. Bilgilendirme ve itiraz mekanizmasının daha iyi çalışabilmesi açısından ilgililerin kimler olması gerektiği konusunda ikincil mevzuatla bir düzenleme yapılması gerekmektedir.

12. İnternet üzerinden yapılan iletişimin denetlenmesi bakımından ayrıntılı düzenlemelerin yapılması, denetimin esas ve usulleri ile sınırlarının belirlenmesi ve haberleşme hürriyeti ile özel hayatın gizliliğinin korunmasına yönelik ilave hükümlerin öngörülmesi gerekmektedir.

İnternet üzerinden yapılan iletişim gittikçe yaygınlaşmakta ve her geçen gün yeni iletişim biçimleri ortaya çıkmaktadır. İnternete giren kişi, arkasından kişiliği hakkında çok zengin ve detaylı bilgiler bırakır. Kişilerin internet üzerindeki hareketlerinin izlenmesi ile kişilik profilinin çıkarılması imkânı mevcuttur. İnternet üzerinden yapılan iletişimin denetimi diğer yöntemlere göre daha az riskli, kolay ve etkili olduğundan internet üzerinden yapılan iletişimin denetlenmesi yoluna daha çok başvurulmaktadır. O nedenle, internet üzerinden yapılan iletişimin denetlenmesi özel hayatın gizliliğini daha çok tehdit etmekte, bu denetim kötüye kullanılmaya daha elverişli görünmektedir. Bu itibarla, internet üzerinden yapılan iletişimin denetlenmesi bakımından ayrıntılı düzenlemelerin yapılması, denetimin esas ve usulleri ile sınırlarının belirlenmesi ve özel hayatın gizliliğinin korunmasına yönelik ilave hükümlerin öngörülmesi lazımdır. Özellikle internet ortamında gönderilen elektronik postanın hangi aşamada elde edilmesinin mümkün olduğu,

sistem üzerinde depolanmış bilgilere erişimin esas ve usullerinin tespit edilmesi büyük önem taşımaktadır.

13. Ceza Muhakemesi Kanunu’nun 135’inci maddesinde sayılan katalog suçların yeniden değerlendirilmesi uygun olacaktır.

Katalog kapsamındaki suçlar esas itibarıyla oranlılık ilkesine uygun olarak belirlenmiştir. Bazı suçların katalog suçlar kapsamından çıkarılmasının düşünülebileceği gibi, başka türlü delil elde edilmesinin güç olduğu iletişim araçlarıyla işlenen, iletişim araç ve ortamlarının suç aracı olarak kullanıldığı suçların, örneğin telefonla veya elektronik posta ile işlenen çocuk pornografisi, özel hayata ve hayatın gizli alanına karşı suçlardan olan haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğini ihlal gibi suçların katalog kapsamına alınması yerinde olacaktır.

14. Soruşturma ve kovuşturma organlarının tedbirin uygulanması suretiyle elde etmiş olduğu delillerin diğer soruşturma ve kovuşturma organlarıyla paylaşılmasının esas ve usullerine ilişkin yasal bir düzenleme yapılması gerekmektedir.

Soruşturma ve kovuşturma organlarının tedbirin uygulanması suretiyle elde etmiş olduğu delillerin diğer soruşturma ve kovuşturma organlarıyla paylaşılmasının esas ve usullerine ilişkin bir düzenlemenin bulunmaması nedeniyle uygulamada tedbirin uygulanması suretiyle elde edilen delillerin başka soruşturma ve kovuşturma organlarıyla paylaşımı konusunda tereddütler bulunmaktadır. Uygulamadaki tereddütlerin ortadan kaldırılması bakımından kanunda bu hususta açık bir düzenleme yapılmalıdır.

15. Telekomünikasyon yoluyla yapılan iletişimin denetlenmesiyle ilgili tedbir kararlarına ilişkin ayrıntılı bilgi ve analizlerin kamuoyunun bilgisine sunulmalıdır.

Toplumumuzda yaygın ve biraz da bulaşıcı bir kanaatle herkesin dinlendiği şeklinde bir algı oluşmakta ve bu durum özellikle konjonktürel bazı dinleme olaylarının kamuoyunu meşgul ettiği dönemlerde iletişim araçlarının kullanımına karşı önemli bir güven kaybına, derin bir şüphe ve hatta evhama dönüşmektedir.

Bu bakımdan, pek çok demokratik ülkede örnekleri görüldüğü üzere, kamuoyu güveninin tesis edilebilmesini teminen, şeffaflık ve hesap verebilirlik ilkelerinin gereği olarak, iletişimin denetlenmesi tedbirini uygulayan kurumlarınca tedbir kararları ve

uygulama sonuçlarına ilişkin istatistiki verileri içeren yıllık raporlar hazırlanarak kamuoyunun bilgisine sunması yararlı olacaktır.

Bu değerlendirme raporlarında, iletişimin denetlenmesi kararlarının sayısı, hukuka aykırı olarak verilen kararlar, tedbir kararlarına karşı yapılan itirazlar ile kabul veya reddedilen itiraz sayısı, tedbir kararlarının katalog suçlar ve talepte bulunan güvenlik kurumları bakımından analizi, uygulanan kararların başarı durumu, suç delili elde edilen ve elde edilmeyen tedbir kararlarının sayısı, elde edilen delillere göre aydınlatılan suç sayıları, elde edilen delillere dayalı olarak verilen tutuklama ve mahkûmiyet karar sayıları ve genel olarak tedbirin önemine ve suçla mücadelede etkinliğine ilişkin genel bir değerlendirme yer almalıdır.

İletişimin denetlenmesine ilişkin ayrıntılı bilgi ve analizlerin kamuoyunun bilgisine sunulmasının, hem tedbir kararını veren hâkimleri hem de ilgili kolluk birimlerini daha özenli hareket etmeye zorlayacağı, ayrıca raporlama sürecinin tedbire karar veren ve uygulayan merciler için geri besleme ve bir çeşit denetim işlevi göreceği açıktır.

Ayrıca, iletişimin denetlenmesi uygulamalarının suçla mücadelede etkinliğinin istatistiki veriler ışığında ortaya konulması ve analiz edilmesi, haberleşme hürriyetine ağır müdahale oluşturan telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbirine ilişkin yasal normların hürriyetlerin sınırlandırılmasında orantılılık ilkesine, başka bir anlatımla hürriyetlere müdahale ile amaca ulaşmak için başvuru araçlarının elverişlilik, gereklilik ve ölçülülük kriterlerine, uygunluğunun değerlendirilebilmesi bakımından büyük önem taşımaktadır. Zira, herhangi bir yasa hükmünün doğurduğu etki ve sonuçların objektif ve somut bir şekilde ölçülememesi veya belirlenememesi halinde, sağlıklı bir değerlendirme yapılması ve isabetli kararlar alınması güçleşecektir.

Bu itibarla, hukuka aykırı dinleme iddialarının sık sık gündeme geldiği, konuyla ilgili pek çok spekülasyonun yapıldığı ülkemizde, özgürlükler ile güvenlik dengesinin demokratik toplum düzeninin gereklerine uygun olarak isabetle kurulabilmesini teminen yapılacak yasama faaliyetleri bakımından da iletişimin denetlenmesine ilişkin yıllık raporların önemli bir gösterge olacağı düşünülmektedir.

Böyle bir raporlama faaliyeti için herhangi bir yasal engel bulunmamakta olup ikincil mevzuatta gerekli düzenlemenin yapılması yeterli olacaktır.

16. Ceza Muhakemesi Kanunu’nun 137’nci maddesinin üçüncü fıkrasında yer alan iletişimin tespitine dair kayıtların imhasına dair hükümlerin, beraat veya mahkûmiyet durumunda nasıl davranılacağını da içerecek biçimde daha geniş şekilde düzenlenmesi yararlı olacaktır.

CMK’nın 137’nci maddesinin üçüncü fıkrasına göre, kovuşturmaya yer olmadığına karar verilmesi ve Cumhuriyet savcısının gecikmesinde sakınca olan hallerde vermiş olduğu kararın hâkim tarafından onaylanmaması halinde tedbire son verilerek yapılan kayıtların en geç on gün içinde imha edilmesi lazımdır. CMK’nın 135’inci maddesinin ikinci fıkrasında, şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişiminin kayda alınamayacağı belirtildikten sonra, “kayda alma gerçekleşikten sonra bu durumun anlaşılması hâlinde, alınan kayıtlar derhâl yok edilir” denilmektedir.

Kayıtların imha edilmesi için kamu adına kovuşturma yapmaya yer olmadığına ilişkin kararın kesinleşmesinin beklenmemesi isabetli değildir. Zira CMK’nın 173’üncü maddesinin birinci fıkrasına göre suçtan zarar görenin, kovuşturmaya yer olmadığına dair kararın kendisine tebliğ edildiği tarihten itibaren on beş gün içinde, bu kararı veren Cumhuriyet savcısının yargı çevresinde görev yaptığı ağır ceza mahkemesine en yakın ağır ceza mahkemesi başkanına itiraz etme hakkı vardır. İtirazı değerlendiren mahkeme başkanının itirazı yerinde bulması halinde Cumhuriyet savcısının kamu davası açmak dışında bir seçeneği yoktur. Denetim sonucu yapılan kayıtlar ve tespitler daha önce imha edilmiş olduğundan bu kayıtların soruşturmada ve kovuşturmada delil olarak kullanılması mümkün olmayacaktır. Kararın kesinleşmesi beklenmeden kayıtların imha edilmesi ile kamu adına kovuşturma yapmaya yer olmadığına dair karara yapılan itirazı değerlendiren en yakın ağır ceza mahkemesi başkanının da karar verirken bu kayıtlardan yararlanmasının önüne geçilmiş olacaktır. O nedenle, CMK’nın 137’nci maddesinin üçüncü fıkrasındaki bu hüküm değiştirilmelidir.

Avrupa İnsan Hakları Mahkemesi, tedbirin uygulanması sonucu yapılan kayıtların gizliliği ve korunması ile ilgili koşulların belirli olmamasını AİHS’nin 8’inci maddesinin ihlali olarak değerlendirmektedir. Mevzuatımızda, tedbir kararlarının uygulanması aşamasında ve uygulanmasından sonra tedbirin uygulanması sonucu elde edilip, ilgili kolluk birimlerinde muhafaza edilen veya tedbirin sona ermesini müteakip Cumhuriyet Başsavcılıklarına ve mahkemelere teslim edilen kayıtların ne şekilde korunması

gerektiğine dair yeterli hükümler bulunmaması nedeniyle yapılacak bir başvuru halinde AİHM’nin Türkiye aleyhine benzer bir karar vermesi kuvvetle muhtemeldir.

İmha yükümlülüğü bulunan hallerin CMK’nın 135’nci maddesinin ikinci fıkrası ve 137’nci maddesinin üçüncü fıkrasında belirlenen hallerle sınırlanması isabetli değildir. Beraat kararı veya mahkûmiyet kararı verilen hallerde kayıtların süresiz olarak saklanması düşünülemeyeceğine göre, belli bir süre sonra bu kayıtların imha edilmesi lazımdır. Yapılacak düzenlemede beraat veya mahkûmiyet hükmü verilen hallerde kayıtların ne zaman imha edileceğine dair hükümlere yer verilmesi yararlı olacaktır.

17. Telekomünikasyon yoluyla yapılan iletişimin denetlenmesiyle ilgili talepte bulunan, karar veren, verilen kararları uygulayan ve tüm sıralanan safahatta rol üstlenen kamu görevlilerinin periyodik olarak eğitilmeleri daha isabetli karar ve işlemlere vesile olacaktır.

Teknik boyutu da olan telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri ve bu kapsamdaki denetim şekilleri itiraz mercileri tarafından da yeterince bilinmediği için uygulamada amaca uygun olmayan ve başvurulması imkânı bulunmayan iletişimin denetlenmesi kararları verilmekte ve usulüne uygun olmayan bu tür kararlar uygulanabilmektedir.

İtiraz mercilerinin de bu denetim şekilleri hakkında yeterli bir bilgiye sahip bulunmamaları nedeniyle bir mahkemenin vermiş olduğu karara karşı bir üst mahkemeye itiraz edilmesi, hukuka aykırılığın ortadan kaldırılması bakımından yeterli bir hukuksal güvence oluşturmamaktadır. O nedenle, bu tedbirin teknik ve hukuksal boyutları konusunda hâkim ve Cumhuriyet savcıları eğitilmelidir.

18. İletişim ortamına girilmesi, iletişimin okunması, izlenmesi veya herhangi bir şekilde elde edilmesi de telekomünikasyon yoluyla yapılan iletişimin denetimi kapsamında düzenlenmelidir.

CMK’nın 135’inci maddesinde iletişimin içeriğinin öğrenilmesi yöntemi olarak iletişimin dinlenmesi ve kaydedilmesine yer verildiği halde, iletişimin okunması ve izlenmesine yer verilmemesidir. E-mail de denilen elektronik posta veya elektronik mektup; “telekomünikasyon hizmetini kullanan tarafından toplanacağı ana kadar şebekede veya alıcının terminal cihazında depolanabilir nitelikteki şebeke üzerinden gönderilen yazılı, sesli, görüntülü mesaj” anlamına gelir. SMS (Short Message Service) ise, mobil

telefonlarla gönderilen kısa mesajlara denilmektedir. Kuşkusuz ki SMS veya elektronik posta yoluyla yapılan iletişim de telekomünikasyon yoluyla yapılan iletişim kapsamındadır. Ancak kanunumuzdaki düzenleme nedeniyle SMS ve elektronik posta (e-mail) gibi iletişim türlerinin CMK'nın 135'inci maddesindeki telekomünikasyon yoluyla yapılan iletişimin denetimi kapsamında yer alıp almadığı hususunda tereddütler ortaya çıkabilir. Çünkü CMK'nın 135'inci maddesinde iletişimin tespiti, dinlenmesi ve kaydedilmesinden söz edildiği halde okunmasından söz edilmemiştir, oysa SMS ve elektronik posta ile yapılan iletişim ancak okunabilir. Maddenin gerekçesinden, internet üzerinden sözlü ve/veya görüntülü yapılan iletişim veya elektronik posta ile yapılan iletişimin içeriği hakkında bilgi edinilmesinin, iletişimin kaydedilmesi kapsamında değerlendirildiği; internet üzerinden sesli ve/veya görüntülü iletişim ile elektronik posta yoluyla yapılan iletişimin ancak kayıt edildikten sonra içeriği hakkında bilgi edinilebileceği görüşünden hareket ettiği anlaşılmaktadır. Ancak, iletişim, kayıt edilmeden de okunabilir, görülebilir ve izlenebilir. O nedenle, iletişim ortamına girilmesi, iletişimin okunması, izlenmesi veya herhangi bir şekilde elde edilmesi de telekomünikasyon yoluyla yapılan iletişimin denetimi kapsamında düzenlenmelidir.

19. Dünyada siber güvenliği tehdit altında bulunan ilk on ülke içinde bulunmamız sebebiyle siber güvenlik uygulama eylem planının hazırlanması, bir yandan da siber güvenlik ile ilgili yasal düzenlemenin bitirilerek devlete ait verilerin tek bir veri merkezinde toplanması sağlanmalıdır.

Siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünü olan siber güvenlik, kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen veya saklanan bilgilerin tümünü kapsamakta olduğundan, bilgi güvenliği ve siber güvenlik konusunda üst düzey çalışılma yapılması gerekmektedir.

Konuyla ilgili olarak, Bakanlar Kurulu'nun, "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"ı 20.10.2012 tarihli Resmi Gazete'de yayımlanarak yürürlüğü girmiş olup, bu kararlar kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğin korunmasına

yönelik tedbirlerin alınması ve bilgi-iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esaslar düzenlenmiş, kamu kurum ve kuruluşlarının ulusal siber güvenliğin sağlanması amacıyla Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yayımlanan plan, program, usul, esas ve standartlara uyacakları belirtilmiş olmakla birlikte; teknolojinin geldiği nokta ve uluslararası siber saldırı tehditleri de göz önüne alınarak, siber güvenlik konusunda Türkiye’de yetkili ve sorumlu bir kurum oluşturulması önem arz etmekte olup, oluşturulacak bu kurum tarafından siber güvenlik uygulama eylem planının hazırlanması, bir yandan da Siber güvenlik ile ilgili yasal düzenlemenin bitirilerek devlete ait verilerin tek bir veri merkezinde toplanması sağlanmalıdır.

20. Yurt dışında bulunan içerik ve yer sağlayıcıların Türkiye’de temsilcilik ve irtibat bürolarının oluşturulması gerekmektedir.

Kamuoyunda “üçüncü yargı paketi” olarak bilinen 2.7.2012 tarih ve 6352 sayılı Kanun ile 5237 sayılı Kanunun 132, 133 ve 134 üncü maddelerinde yapılan değişikliklerle, “İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.” cümlesi eklenmiştir. Bu suretle, hukuka aykırı olarak ifşa edilmiş olan haberleşme içeriklerinin basın ve yayın yoluyla yayımlanması halinde de, faillerin bu fıkra hükmüne göre cezalandırılmasına imkân tanınmıştır. Ancak bu düzenleme yurtdışı kaynaklı sitelerin bu tarz suçları işlemesi konusunda caydırıcı olamamaktadır. Cezalandırma yoluna gidilmesi uzun zaman almakta ve bazı durumlarda yurt dışında suç olmaması nedeniyle cezalandırılmamaktadır. Bununla birlikte bu tarz yayınların sadece suç unsuru içeren içeriklerine erişimin engellenmesi de teknik olarak mümkün değildir. Sitenin tamamına yurt içinden erişiminin engellenmesi kamuoyu tarafından abartılı bulunmaktadır. Bunun önüne geçilmesi amacıyla yurt dışı kaynaklı olarak Facebook ve Twitter gibi sosyal paylaşım, YouTube gibi video paylaşım ve Google gibi arama motoru hizmeti sunan firmaların ülkemizde sunucuları bulunmadığından Türkiye’deki faaliyetleri nedeniyle IP adreslerinin paylaşımı ve kişilik haklarının korunmasını teminen içeriğin çıkarılması gibi konularda işbirliğinin sağlanması, bunların Türkiye’de yetkili temsilcilik ve irtibat bürolarının oluşturulması ve bu amaçla uluslararası girişimlerde bulunulması gerekmektedir.

Söz konusu uluslararası şirketlerin ülkemizde yapmış olduğu faaliyetler nedeniyle çok büyük gelir elde etmelerine karşılık vermiş oldukları hizmetlerin kötüye kullanımı nedeniyle oluşan toplumsal zararlar ile ülkemiz karşı karşıya kalmaktadır. Ayrıca bu

firmaların ülkemizde temsilciliklerinin bulunmaması, elde ettikleri gelirlerin vergilendirilememesi sonucunu doğurmakta ve ülkemiz açısından büyük bir vergi kaybına neden olmaktadır.

Sonuç olarak bu firmaların ülkemizde yetkili temsilcilik kurmaları, hukuka aykırı içeriklerin kısa sürede kaldırılabilmesine imkân sağlayacak aynı zamanda da vergi kayıplarının önüne geçilerek ekonomik olarak ülkemize katkı sağlayacaktır.

21. Ulusal Bilgi Güvenliğinin Sağlanmasına Dair Çalışmaların Hızlandırılması Gerekmemektedir.

Kamu kurumlarında tutulan bilgilerin güvenliği konusunda gerekli tedbirlerin alınmadığı görülmektedir. Son derece önemli bilgilerin depolandığı kurumların her birinin bilgi güvenliği konusunda aynı donanımına sahip olduğunu söylemek güçtür. Bu konuda son teknolojiye uygun bir koruma standardının sağlanması gerekmektedir.

Ayrıca Ülkemiz genelinde bulunan tüm kamu kuruluşlarında bulunan bilgilerin korunması belli bir standarda kavuşturulması amacıyla yapılacak çalışmalara hız verilmelidir.

22. Suçla mücadelede suç işlemeye yönelik motivasyonu etkili biçimde azaltarak katkı sağlayan alarm izleme merkezleri ve kent güvenliği yönetim sistemi (KGYS-MOBESE) ile ilgili yasal altyapı ve standartlar getirilmelidir.

Güvenli kent olgusu, insanlık tarihinde uygarlığın her zaman kabul gören bir ölçütü olmuştur. Ülkemizde kentleşme olgusunun hız kazanmasıyla birlikte, güvenlik sorunu kamuoyunu giderek daha çok meşgul etmeye başlamış, kapkaç, gasp, dolandırıcılık, cinsel taciz, cinayet gibi, günlük yaşamda etkisi daha kolay hissedilen suçlardaki artış, toplumdaki tedirginliği artırmıştır. Elbette ki suçsuz bir toplum hayalden başka bir şey değildir. Ancak bu toplumsal tedirginliğin güvenlik hizmetleriyle görevli devlet kurumlarını suçun henüz işlenmeden önlenmesi, işlenen suçların faillerinin daha hızlı biçimde takip edilerek adalet önüne çıkarılması ve hatta faillerin adli hatalara mahal vermeden saptanabilmesi yönünde yeni arayışlara sevk etmesini pek tabii bir sonuç olarak görmek gerekmektedir.

Suçlularla mücadelede bu yeni arayışların ürünü olarak karşımıza çıkan KGYS (MOBESE) ve Alarm İzleme Merkezleri, özellikle büyükşehirlerimizde, gerek suçlular gerekse potansiyel suçlular açısından riski artıran ve suç işlemeye yönelik motivasyonları

azaltan önemli faktörlerdendir. Son yıllarda işlenen birçok suçun faillerinin (MOBESE) yardımıyla saptandığı inkâr edilmez bir gerçektir.

Alarm İzleme Merkezleri, konut, işyeri ve tesislerin güvenliğini sağlamak amacıyla, teknik donanım kullanarak bunları izleyen, alarm sistemleri aracılığıyla sürekli olarak yapılan izleme sırasında gelen ihbarları değerlendiren ve teknik bakımdan doğrulanan ihbarları sorumluluk bölgesindeki genel kolluğa bildiren özel güvenlik kuruluşlarıdır.

Alarm İzleme Merkezlerini kurma ve işletme için yeterlilik belgesi valiliklerce verildiğinden, valiliklerin ilgili birimlerince başvuru yapan merkezle alakalı gerekli inceleme ve soruşturmalar yapılmakta ve mevzuatta belirtilen tüm şartları yerine getiren işletmelere merkez kurma izni ve yeterlilik belgeleri verilebilmektedir.

Türkiye’de elektronik güvenlik sistemleri sektöründe yasal düzenleme bulunmadığı için, alarm sistemleri haricinde kamera kayıt sistemlerinin kurulması ve satışı herhangi bir izin belgesine gerek olmadan yapılabilmektedir. Özellikle alışveriş merkezleri, metrolar, otobüs terminalleri ve garlar gibi kamuya açık alanlarda kamera kayıt sistemlerinin kurulması, kaydedilen verilerin saklanması ve daha sonra imhası konularında bir düzenleme olmaması kişi hak ve özgürlükleri açısından ciddi endişelere neden olmaktadır. Ayrıca bu konuda yurtdışından getirilen cihazlar hususunda da belirlenmiş bir standart olmadığı için her türlü cihazın ithalatı yapılmaktadır.

Öncelikle elektronik güvenlik sistemleriyle ilgili tanımlama yapılmalı, çıkarılacak düzenlemeyle bu cihazların üretimi, ithalatı ve satışı ile sistemlerin kurulması konularında bir standardizasyon getirilmelidir.

Türk Standartları Enstitüsü (TSE) tarafından bu sistemlere ilişkin mutlaka yeni standartlar belirlenmeli ve bu standartlar dışındaki ürünlerin Türkiye’ye girmesi önlenmelidir. Buna paralel olarak, bu tür cihazların yurda girişi sırasında daha etkin denetim yapılabilmesi için ihtisas gümrükleri kurulmalıdır.

Üçüncü şahısların ve özel güvenlik kuruluşlarının güvenlik amaçlı elde ettikleri ses ve görüntü sistemlerindeki kaydedilmiş verilere de, sadece gereken şartların oluşması durumunda Yasada belirtilecek yetkililerin emriyle el konulabilmesi şartı getirilmeli ayrıca bu tip görüntülerin özel hayatın gizliliğini tehdit edecek biçimde internet ortamından yayınlanması engellenmelidir.

Özel kişiler tarafından kurulan ve kullanılan güvenlik kameralarının başkalarının özel hayatına müdahale etmelerinin önüne geçilmesi amacıyla kameraların nerelere, hangi

açıyla, kimler tarafından kurulabileceği, kayıtların nasıl, hangi şartlarda, kimler için, hangi amaçlarla kullanılabileceği gibi konuların ayrıntılı bir şekilde düzenlenmesi gerekmektedir. Ayrıca bu sistemlerin standartlarının ve denetiminin de hükme bağlanması gerekmektedir.

Elbette ki bunca sosyal ve adli faydaları bulunmasına rağmen güvenlik hizmetleri ifa eden devlet birimlerinin (MOBESE) aracılığı ile yapılan izleme ve takip yetkisini doğrudan doğruya ve tartışmasız biçimde herhangi bir yasadan aldığı söylenemez. 2559 sayılı Polis Vazife ve Salahiyet Kanunu ve ilgili kanunlarla suçun işlenmesinden önce önlenmesi konusunda polise yetkiler verildiğinden ve KGYS (MOBESE) sistemi de günün ihtiyaç ve koşullarına göre kolluk faaliyeti olarak değerlendirildiğinden kamu güvenliği ve düzeni, suç delillerinin elde edilmesi ve faillerinin yakalanması amaçlarına hizmet eden KGYS sistemi (MOBESE) ile ilgili olarak; kameraların halkın yoğun olarak bulunduğu kamuya açık alanlarda kurulmakta olduğu ve MOBESE kameralarından yapılan izlemelerin belli çevre veya bireylere yönelik olmayıp, genel maksatlı izleme yapılmakta olduğu bilinmekle beraber; hukukun düzenlediği her şeyin mutlaka hayatta var olduğu, ancak hukuken düzenlenmeyen birçok şeyin hayatta ve pratikte olabileceği kuralı karşımıza çıkmakta, KGYS (MOBESE) sisteminin yasal bir çerçeveye oturtulması gerekmektedir.

Birçok olayın önlenmesi ve adli olaylarda faillerin yakalanmasında çok önemli bir role sahip MOBESE ve Alarm İzleme Merkezleri için bir kanun hazırlanmalı ve hazırlanacak olan özel kanunda; Anayasa'nın 13'üncü maddesine göre temel hak ve özgürlüklere müdahale niteliği taşıyabilecek hususların da düzenlenmesi gerekmektedir. Demokrasilerde yurttaşların idareden, adil, tarafsız ve öngörülebilir muamele bekleme hakkı vardır. Bu nedenle, bu kanuni düzenlemenin yeterli derecede detaylı, anlaşılabilir ve net olması gerekir. Ayrıca kanunun, bu kayıtların kötüye kullanılmaması için yeterli koruyucu düzenlemeler içermesi gerekir.

Bu kanuni düzenlemede İçişleri Bakanlığı tarafından yürütülen “Mülkiye Müfettişlerinin İnsan Hakları Alanında Teftiş Bilgi Deneyim ve Kapasitelerinin Artırılması” amacıyla yürütülen proje çerçevesinde hazırlanan “İnsan Hakları Prensipleri Işığında Kolluk Uygulamalarının Denetimi” adlı çalışmada da belirtildiği üzere; tutulan kayıtların ancak belirli bir süre tutulmasını öngörmeli (örneğin 48 saat, 96 saat, bir hafta gibi...), bu süreler sonunda kayıtların yok edilmesi gerektiği belirtilmeli, kayıtların bir suçu aydınlatmada kullanılmak istenmesi halinde, kanunun öngöreceği merciden yazılı talep istenmesi sağlanmalıdır.

Yapılacak kanuni düzenlemede ayrıca izlenen caddelerde herkesin görebileceği yerlerde kayıt yapıldığına dair okunaklı bir levha bulundurulması gerektiğine işaret edilmeli, kamuya açık alanlarda izleme yapılacak yerler, o yerin en büyük mülki amirinin onayı ile tespit ve ilan olunmalıdır.

Kayıtların medyayla veya başka bir merci ile paylaşılması durumunda ilgisi olmayan üçüncü şahısların yüzlerinin mozaiklenmesi sağlanmalıdır.

MOBESE kameralarında ses kayıt özelliği olmamalı, hareketli kameraların pencere gibi özel alanlara karşılık gelen yerlerde görüntü perdelemesi yapılmalı, ayrıca MOBESE sistem odasında gerekli güvenlik tedbirleri alınmalı, giriş çıkışlar kameralar ve kapı kontrol sistemleriyle sürekli denetim altında tutulmalıdır. İlgisiz kişilerin sistem odasına ve bilgisayarlara giriş yapması engellenmelidir.

İngiltere’de olduğu gibi kamuya açık alanlardaki (alışveriş merkezleri, metrolar, otobüs terminalleri, garlar vb.) kamera sistemlerinin MOBESE sistemleri ile entegre edilerek, elde edilen kayıtların tek merkezde toplanması sağlanabilirse elektronik güvenlik sistemleri üzerinde etkin bir denetimin gerçekleştirilmesi mümkün olacaktır.

23. Müdafî ile gerçekleştirilen iletişimin denetlenmesiyle ilgili CMK’nın 136’nı maddesinin, “şüpheli veya sanığın müdafî ile kurduğu iletişimin, kullanılan telekomünikasyon aracına bağlı olmaksızın dinlenemeyeceği, kayıt altına alınamayacağı ve sinyal bilgilerinin değerlendirilemeyeceği” esasına göre yeniden düzenlenmesi uygun olacaktır.

Ceza yargılamasında savunma makamını temsil eden ve adil yargılamanın vazgeçilmez unsurlarından olan müdafîye şüpheli veya sanığın savunmasını layıkıyla ve gereği gibi yapabilmesi için bazı imtiyazlar tanınmış, böylece mesleki sırların ve savunma hakkının korunması amaçlanmıştır. Müdafî ile şüpheli veya sanık arasındaki görüşmelerin mahremiyetinin sağlanabilmesi için Ceza Muhakemesi Kanunun 46’nı maddesinde müdafilerin mesleki uğraşları nedeniyle öğrendiği bilgiler bakımından tanıklık yapmaktan çekinebilecekleri, ilgilinin muvafakat etmesine rağmen tanıklık yapmak zorunda olmadıkları, Kanunun 126’nı maddesinde tanıklıktan çekilme hakkı alanlarla şüpheli veya sanık arasındaki mektup ve belgelere el konulamayacağı, 154’üncü maddede şüpheli veya sanığın vekâletname aranmaksızın müdafî ile her zaman ve konuşmaları başkalarının duyamayacağı bir ortamda görüşebileceği hüküm altına alınmıştır.

Bu bağlamda, Ceza Muhakemesi Kanunu’nun 136’ncı maddesinde de “şüpheli veya sanığa yüklenen suç dolayısıyla müdafinin (şüpheli veya sanığın avukatının) bürosu, konutu ve yerleşim yerindeki telekomünikasyon araçları hakkında, 135’inci madde hükmünün uygulanmayacağı” hükmü yer almıştır. Ancak, müdafilik sıfatıyla kurulan iletişim bakımından getirilen yasak mutlak bir yasak olmayıp, yalnızca avukatın müdafiliğini yaptığı şüpheli veya sanığa yüklenen suçla sınırlı olarak ve müdafinin sadece bürosu, konutu ve işyerinde bulunan telekomünikasyon araçları bakımından geçerlidir. Dolayısıyla müdafinin şüpheli veya sanıkla cep telefonu, araç veya uydu telefonlarıyla kurduğu iletişimin dinlenmesi, kayda alınması, iletişimin tespiti ve sinyal bilgilerinin değerlendirilmesi hususunda yasal bir engel bulunmamaktadır. Günümüzde iletişim araçlarının kullanımında cep telefonlarının kullanım kolaylığı ve yaygınlığı dikkate alındığında Ceza Muhakemesi Kanunu’nun 136’ncı maddesinde yer alan düzenlemenin bu haliyle, savunma hakkının korunması bakımından müdafiyeye sağlanan korumanın eksik kaldığı ve yeterli bir güvence sağlamadığı değerlendirilmektedir.

Açıklanan nedenlerle, anılan yasa maddesinin “şüpheli veya sanığın müdafii ile kurduğu iletişimin, kullanılan telekomünikasyon aracına bağlı olmaksızın dinlenemeyeceği, kayıt altına alınamayacağı ve sinyal bilgilerinin değerlendirilemeyeceği” esasına göre yeniden düzenlenmesi gerektiği, bu çerçevede CMK’nın 136’ncı maddesinin “şüpheli veya sanığa yüklenen suç dolayısıyla müdafii hakkında, dördüncü fıkra hükmü hariç olmak üzere, 135’inci madde hükmü uygulanmaz” şeklinde değiştirilmesinin yerinde olacağı değerlendirilmiştir.

24. Telekomünikasyon İletişim Başkanlığının kuruluş ve görevlerini düzenleyen 2559 sayılı Polis Vazife ve Salahiyetleri Kanunu’nun ek 7’nci maddesine Telekomünikasyon İletişim Başkanlığının itiraz yetkisine dair bir hüküm konulmalıdır.

Ceza Muhakemesi Kanununda iletişimin denetlenmesine ilişkin verilen kararlara itiraz esas ve usulüyle ilgili özel bir hüküm bulunmamakla beraber, itiraz konusu Ceza Muhakemesi Kanunun 267’nci ve devamı maddelerinde olağan kanun yollarından birisi olarak ayrıca düzenlenmiştir. CMK’nın “Kanun yollarına başvurma hakkı” başlıklı 260’ıncı maddesinde “hâkim ve mahkeme kararlarına karşı Cumhuriyet savcısı, şüpheli, sanık ve bu Kanuna göre katılan sıfatını almış olanlar ile katılma isteği karara bağlanmamış, reddedilmiş veya katılan sıfatını alabilecek surette suçtan zarar görmüş bulunanlar için” kanun yollarının açık olduğu hükme bağlanarak itiraz edebilecek ilgililer

sayılarak belirtilmiştir. Diğer yandan Telekomünikasyon İletişim Başkanlığının kuruluş ve görevlerini düzenleyen 5397 sayılı Kanunla 2559 sayılı Polis Vazife ve Salahiyetleri Kanunu’nun ek 7’nci maddesine eklenen hükümler içerisinde de TİB’e itiraz yetkisi veren bir hüküm bulunmamaktadır.

14.01.2007 tarihli Resmi Gazete’de yayımlanarak yürürlüğe giren Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik’in 10’uncu maddesinin birinci fıkrasında ise, iletişimin denetlenmesine ilişkin kararlara karşı Cumhuriyet savcısı, şüpheli, sanık, katılan, suçtan zarar gören, müdafî, vekil, şüpheli veya sanığın yasal temsilcisi ve eşinin yanı sıra TİB’in de itiraz edilebileceği hükme bağlanmıştır. Uygulamada bu yönetmelik hükmüne dayanılarak TİB tarafından itiraz yoluna başvurulmaktadır.

Benzer biçimde, 10.11.2005 tarihli Resmi Gazete’de yayımlanarak yürürlüğe giren Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik’in düzenleyen 17’nci maddesinin c bendinde Başkanlığa, “iletişimin denetlenmesi taleplerinin bu Yönetmeliğe ve diğer ilgili mevzuata uygun olup olmadığını inceleyerek gerektiğinde yetkili mercilere başvuruda bulunmak” görevi verilmiştir.

Ancak, Telekomünikasyon İletişim Başkanlığının itiraz yoluna başvurma yetkisinin açık bir yasal dayanağının bulunmadığı, itiraz başvurularının yönetmelik hükümlerine dayalı olarak uygulandığı anlaşılmaktadır. Nitekim Telekomünikasyon İletişim Başkanlığı’nın açık bir yasal düzenleme olmaksızın yönetmelik hükümlerine dayanarak hâkim kararlarına karşı itiraz yoluna başvurma yetkisinin bulunmadığı gerekçesiyle, uygulamada bazı mahkemelerin TİB tarafından yapılan itirazları reddettikleri görülmektedir.

Bu arada belirtmek gerekir ki; iletişimin denetlenmesine ilişkin tedbir kararlarının gizlilik ilkesi içerisinde uygulanması gerektiğinden, tedbir kararının ilgililerinden şüpheli veya sanık ile bunların müdafileri, yasal temsilcileri ve eşleri ya da katılan, suçtan zarar görenler ile bunların vekillerinin iletişimin denetlenmesi kararından haberdar olamayacakları ortadadır. Dolayısıyla CMK’nın 260’ncı maddesinde itiraz hakkı tanınan kişilerin iletişimin denetlenmesi kararına karşı fiilen kanun yoluna başvurmaları mümkün

olamayacaktır. Ceza Muhakemesi Kanunun 137’nci maddesine göre tedbirin uygulandığı ilgiliye tedbirin uygulamasına son verildikten sonra bildirilmesi gerektiğinden bu aşamada ilgilisi tarafından yapılacak itirazın da anlamı olmayacaktır.

Bu itibarla, Telekomünikasyon İletişim Başkanlığının iletişimin denetlenmesi kararlarına karşı itiraz edebilmesi son derece önemlidir. Kuruluş amacı, iletişime yapılacak müdahalelilerin tek elden yürütülmesi, uygulama birliğinin sağlanması ve keyfiliğin önlenmesi olan Telekomünikasyon İletişim Başkanlığının iletişimin denetlenmesi kararlarına itiraz yetkisi, iletişimin denetlenmesi tedbirinin hukuka uygun olarak işletilebilmesi bakımından büyük önem arz etmektedir. Nitekim kurulduğu günden bu yana TİB’in yapmış olduğu itirazların önemli bir bölümü mahkemelerce kabul edilerek verilen kararlar iptal edilmiştir.

Dolayısıyla, kişi hak ve hürriyetlerin ve özel hayatın gizliliğine müdahale edilmesine neden olan iletişimin denetlenmesi tedbirine müteallik işlemler sürecinin tamamıyla açık yasal düzenlemelere ve yetkiye dayanması gerektiği ilkesinden hareketle, TİB’in kuruluş ve görevlerini düzenleyen 2559 sayılı Polis Vazife ve Salahiyetleri Kanunu’nun ek 7’nci maddesine Telekomünikasyon İletişim Başkanlığının itiraz yetkisine dair bir hüküm konulmalıdır.

25. Ceza Muhakemesi Kanunu’nun mülga 250, 251 ve 252’nci maddelerine atıf yapan kanunlarda değişiklik yapılarak bu atıfların Terörle Mücadele Kanunu’nun 10’uncu maddesi ile uyumlu hale getirilmelidir.

Ceza Muhakemesi Kanunu’nun özel yetkili mahkemeleri düzenleyen 250, 251 ve 252’nci maddeleri kamuoyunda “üçüncü yargı paketi” olarak bilinen 2.7.2012 tarih ve 6352 sayılı Kanunun 105’inci maddesiyle yürürlükten kaldırılmıştır. Bunun yerine TMK’nun 10’uncu maddesi ile yeni bir mahkeme sistemi kurulmuştur. Her ne kadar 6352 sayılı Kanunun geçici 2’nci maddesinin yedinci fıkrasında, “*mevzuatta Ceza Muhakemesi Kanununun 250 nci maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemelerine yapılmış olan atıfların, Terörle Mücadele Kanununun 10 uncu maddesinin birinci fıkrasında belirtilen ağır ceza mahkemelerine yapılmış sayılacağı*” hükme bağlanmışsa da; bu konuda ortaya çıkabilecek yorum farklılıklarını ve yanlış anlamaları ortadan kaldırmak amacıyla CMK’nın mülga 250, 251 ve 252’nci maddelerine atıf yapan kanunlardaki düzenlemelerin değiştirilerek TMK’nın 10’uncu maddesiyle uyumlu hale getirilmesi gerekmektedir.

26. Polis Vazife ve Salahiyetleri Kanunun ek 7’nci maddesi uyarınca Telekomünikasyon İletişim Başkanında görev yapan Millî İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı temsilcilerinin çalışma ilişkisi hakkında ikincil mevzuatta düzenleme yapılmalıdır.

Polis Vazife ve Salahiyetleri Kanunun ek 7’nci maddesinde Telekomünikasyon İletişim Başkanlığında Millî İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığının ilgili birimlerinden birer temsilci bulunacağı hükme bağlanmış, 10.11.2005 tarihli Resmi Gazete’de yayımlanarak yürürlüğe giren Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik’in 16’ncı maddesinin son fıkrasında da sözü edilen Millî İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı temsilcilerinin Başkanlıktaki görevleri esnasında Başkanın talimatlarına ve Başkanlık tarafından belirlenen kurum içi düzenlemelere riayet edecekleri hüküm altına alınmıştır.

Mevcut haliyle TİB’de görev yapan Millî İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı temsilcilerinin statüleri, bağlılık ve disiplin ilişkilerinin mevzuatta açık bir şekilde düzenlenmediği ve çalışma ilişkileri bakımından belirsizlik olduğu görülmektedir. Bu bağlamda, bu temsilcilerin çalışma ilişkisinin ikincil mevzuatta açıkça düzenlenmesi sağlanmalıdır.

27. Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı istihbarat birimlerinin İçişleri Bakanlığı Mülkiye Teftiş Kurulu, Milli İstihbarat Teşkilatı birimlerinin de Başbakanlık Teftiş Kurulu tarafından denetimi sağlanmalıdır.

Devletler açısından suçlarla mücadelede istihbarat önemlidir ama insan haklarının korunması daha da önemlidir. 3152 sayılı İçişleri Bakanlığı Teşkilat Kanunu’nda Bakanlığın görevleri arasında; “Anayasada yazılı hak ve hürriyetleri korumak” görevi bulunmaktadır. Bu görev kapsamında insan hakları prensipleri ışığında bütün kolluk uygulamalarında olduğu gibi istihbarat faaliyetlerinin de etkili bir şekilde denetlenmesi gerekmektedir.

Ülkemizde kolluk istihbarat birimleri üzerindeki idari denetimlere ilişkin olarak, 3152 sayılı İçişleri Bakanlığı Teşkilat Kanununun Teftiş Kurulu Başkanlığı başlıklı 15’inci maddesinde Teftiş Kurulu Başkanlığının Bakanın emri veya onayı üzerine yapacağı

görevler belirlenmiştir. Bu görevlerden birincisi; *“Bakanlığın merkez birimlerinin, bağlı kuruluşların, il ve ilçelerin ve mahalli idarelerle, bunlara bağlı ve bunların kurdukları veya özel kanunlarla kurulmuş birlik, işletme, müessese ve teşebbüslerin işlem ve hesaplarını teftiş etmek ve denetlemek, inceleme ve soruşturma yapmak,”* şeklinde belirlenmiştir. Benzer düzenleme İçişleri Bakanlığı Teftiş Kurulu Tüzüğü’nde de yer almıştır.

Kanunun bu maddesine ve Tüzüğe göre Mülkiye Teftiş Kurulunun Bakanın onayı üzerine Bağlı Kuruluşların tüm iş ve işlemlerini denetlemekle yetkili ve görevli olduğu görülmektedir. Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı İçişleri Bakanlığının bağlı kuruluşları arasındadır.

Yetkili kurumlar tarafından önleme ve istihbarat amaçlı uygulanan tedbirlere ilişkin işlemlerde kurumların uymaları gerekli olan hususların denetlenmesi konusu, bazı kanunlarda değişiklik yapan 5397 sayılı Kanun’da düzenlenmiştir. Bu Kanun hükümlerine göre; yetkili kurumların (Emniyet ve Jandarma Teşkilatı için) sıralı amirler, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve ilgili Bakanlık müfettişleri tarafından MİT için ise sıralı Kurum amirleri Başbakanlık teftiş elemanları tarafından denetleneceği hüküm altına alınmıştır.

Denetim sayesinde sadece, kolluk ve istihbarat birimlerinin şeffaflığı ve hesap verilebilirliği garanti altına alınmakla kalmaz, hukukun üstünlüğüne ve dolayısıyla kişi hak ve özgürlüklerine ve meslek ahlakına saygılı kalması da sağlanır. Türkiye’de iç denetim kolluğun kendi amirleri tarafından sağlanırken, dış denetim ise mülki idare amirleri, mülkiye müfettişleri ve yargı yoluyla gerçekleştirilir.

Jandarma ve Emniyet birimleri mülkiye müfettişleri tarafından üç yılda bir düzenli olarak teftiş edilirken, kolluğun istihbarat birimlerinin denetimi Bakanlık makamından özel onay alınarak yapılabilir. Gerek merkez teşkilatındaki Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı İstihbarat Daire Başkanlıklarının, gerekse taşra teşkilatındaki şube müdürlüklerinin iş ve işlemlerinin denetim ve teftişine yönelik olarak, hem hukuken kendilerine verilen görevleri belirtilen mevzuat içerisinde usul yönünden uygun olarak yerine getirip getirmediklerinin hem de hesap verebilirlik ve şeffaflık açısından hukuka uygun davranıp davranmadıklarının belli süreler içerisinde etkin olarak denetlenmesinin, hiçbir iş ve işlemin hangi gerekçe ile olursa olsun denetim dışında

birakılmamasının, iş ve işlemlerin hukuka ve yürürlükteki mevzuata uygun olarak yapılıp yapılmadığının denetlenmesi için, İçişleri Bakanlığı Makamınca mülkiye müfettişlerine belirli dönemlerde kolluğun istihbarat birimleri için denetim onayı verilmesinin uygun olacağı düşünülmektedir. Bu sayede komisyonumuzun amacı olan haberleşme özgürlüğüne ve özel hayatın gizliliğine yönelik olarak da kolluk istihbarat birimleri üzerinde sivil denetim birimi olan Mülkiye Teftiş Kurulunun denetim ve teftişi sağlanmış olacaktır.

28. Önleme amaçlı iletişimin denetlenmesi tedbirinin uygulanmasında görev alan kurumların çalışma esaslarını düzenleyen kanunların çağın gereklerine uygun olarak yenilenmesi gerekmektedir.

Küreselleşen dünyaya uyum sağlamak isteyen ulusal ve uluslararası seviyedeki kurumların hemen hepsi hızla kabuk değiştirmektedir. Gelişen teknoloji ile birlikte artık istihbarat teknikleri de değişmekte, elektronik, elektromanyetik, siber ve teknolojik istihbarat sahasındaki yeniliklerin yakından takip edebilmesi kaçınılmaz bir zorunluluk olarak karşımıza çıkmaktadır.

Bütün bu teknolojik gelişmeler ışığında ve ileri demokrasilerden ileri istihbarat çıkar mantığı doğrultusunda, Önleme Amaçlı İletişimin Denetlenmesi Tedbirinin Uygulanmasında Görev Alan Kurumların Çalışma Esaslarını Düzenleyen Kanunların çağın gereklerine uygun olarak yenilenmesi gerekmektedir.

5.2 Teknik Öneriler

Her geçen gün yeni bir teknolojinin ortaya çıkması hayatımızı kolaylaştırmasının yanında dezavantajları, mahremiyet ihlalleri ve suiistimallere açık olmayı da beraberinde getirmektedir. Yasa dışı dinleme faaliyetlerini engellemek amacıyla gerekli tedbirler alınmakla birlikte, her gün yenilenen teknolojik gelişmeler dikkate alındığında yasa dışı dinleme faaliyetlerinin tamamen engellenmesi imkan dâhilinde görülmemektedir. Ayrıca sürekli başkaları tarafından üretilen teknolojileri tüketen bir toplum olunması durumunda da yukarıda bahsedilen sakıncaların yaşanmasının devam edeceği çok açıktır.

Komisyonumuzun çalışmaları esnasında tespit edilen teknik öneriler aşağıda sıralanmıştır:

1. Gerek akıllı telefonlardaki casus yazılım, gerekse kişisel bilgisayarlardaki virüs, internet dolandırıcılığı, kimlik avları, zarar verici virüsler, hacker'lık, DDoS saldırıları vb.

gerek mahremiyeti ihlal gerekse haberleşme özgürlüğüne müdahaleye sebep verecek durumların teknoloji, kanun, yönetmelik ve benzeri düzenlemelerle engellenmesi bir noktaya kadar etkili olacaktır. Ancak hiçbir zaman kesin çözüm olmayacak bu konudaki en etkili çözüm kullanıcıların bilinçlendirilmesi, “teknoloji okuryazarlığı”nın toplumda bilinirliğinin artırılması ve gerekli eğitim programlarının düzenlenmesi ve eğitici duyuruların yapılmasıdır. Ayrıca, vatandaşlarımızın kendi kişisel mahremiyetlerini koruma açısından kendilerine düşeni yapacak şekilde bilinçlendirilmelidir.

Bu bağlamda başta çocuklar ve gençler olmak üzere, internet kullanıcıların kullandıkları parolaları kimseyle paylaşmamaları, tahmin edilebilecek parolaları kullanmamaları, parolaların tekrar elde edilmesi için sorulan güvenlik sorularının kolay olmaması, internet ortamında paylaştıkları kişisel bilgilerin doğurduğu risklerin önlenmesi ve bunlarla karşılaşmaları halinde izlenmesi gereken yollar hakkında bilinçlendirilmelidirler.

2. Kişisel verilerin korunması ve kurumlar arası veri paylaşımına ilişkin mevzuat hazırlanmalı, veri sahipliği tanımlanmalı ve hangi verilerin kimler tarafından üretileceği ve paylaşılacağı usul ve esasları oluşturulmalıdır. Bu verilerin nasıl korunması gerektiği gibi hususlarda da kamuoyunun ve kullanıcıların bilinçlendirilmesi sağlanmalıdır.

3. Dinleme ve izleme yetkisi bulunan kuruluşlar ve GSM operatörlerinde çalışanlar sistemlere ulaşmadan önce belirli süreç ve eğitimden geçirilmelidir. Bu kişilere özel kimlikler verilmeli, kimlik doğrulama yöntemleri kullanılarak erişime izin verilmelidir (elektronik imza, parola, parmak izi veya avuç gibi biyometrik veri). Tüm loglar kayıt altına alınmalı ve hiçbir şekilde silinememelidir. Ayrıca elektronik imzalarının da kayıtlarda bulunması gerekmektedir.

4. Nüfus, sağlık, mal varlığı gibi kritik verilerin yer aldığı veri tabanları şifreli olarak tutulmalı (Donanım Güvenlik Modülü gibi cihazlar kullanılarak) ve kriptolanması konularında son teknolojiler uygulanmalıdır. Ayrıca çalışanlar hiçbir şekilde kolaylıkla bu veri merkezlerine ulaşamamalıdır. Verilere ulaşmak zorunda kaldığında çoklu erişim kuralları getirilmeli, kontrollü bir şekilde (örn. iki faktörlü doğrulama) ve yetkili kişiler girebilmelidir. Yapılan girişler ve sorgular loglanmalı, elektronik imza kullanılmalı ve hiçbir şekilde silinememelidir.

5. Kişisel bilgilere yetkisiz ve kötü niyetli kullanıcı veya gruplar tarafından erişilmesi durumunda baskı, şiddet ve şantaj yaparak haksız bir kazanç ve menfaat elde edilebilir.

Örneğin, sağlık verileri göz önüne alındığında sigorta ve ilaç firmaları için altın değerindedir. Bu bilgiler kullanılarak ve yasal boşluktan faydalanılarak toplum düzeninin bozulmasına sebep olabilir. Bu nedenle, ülkemizde kişisel bilgileri-verileri koruma kanununun bulunması gerekmektedir. Bilgilerimizin yasal olarak güvence altında tutulması gerekmekte olup hiçbir şekilde alınamaması, bir maddi para ya da hizmet karşılığında satılamaması ve yetkisiz bir şekilde dağıtılmaması gerekmektedir. Bunun yanında, bu bilgilerin teknik olarak verilerin güvenli tutulduğu ilgili kamu ve özel sektör bilgi merkezlerinin araştırılması ve sızma testleri gibi güvenlik kontrollerinin yapılıyor olması gerekmektedir.

6. Gizli veya Kişisel verilerin işlenmesi gerektiği durumlarda dünyada uygulanan standart mekanizmalar kullanılarak anonimleştirme yapılması, yani gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi gerekmektedir. Bu verilerin otomatik veya otomatik olmayan araçlarla tamamen veya kısmen elde edilmesi, toplanması, kaydedilmesi, depolanması, muhafaza edilmesi, paylaşılması, silinmesi, yok edilmesi, değiştirilmesi, yeniden düzenlenmesi, tehlike altındaki kişilere veya veri sorumlusuna açıklanması, yayımlanması, elde edilebilir hale getirilmesi, sınıflandırılması veya kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem güvenli bir şekilde yapılması gerekmektedir.

7. Özel sektör, üniversiteler, kamu ve sivil toplum işbirliği modelinin oluşturulmasıyla bir ulusal güvenlik otoritesi oluşturulması ve bu otoritenin özel/kamu kurum ve kuruluşlarda denetimlerin yapılmasıyla ülke olarak çok daha iyi bir seviyeye ulaşılabilir. Bunun yanında, güvenlik zincirinde en zayıf halka bireyler olduğundan toplumsal bilinç artırılabilir, bu sayede özel şirketler veya kamu kurumları bilgi güvenliği kültürünün geliştirilmiş olacak ve bu konuya daha ciddi yaklaşıacaklardır. Ayrıca, Türkiye olarak özellikle siber tehditlere yönelik yeniden yapılanmaya ihtiyaç duyulmakta ve bu kapsamda teknik olarak uluslararası düzeyde ciddi siber savunma gücünü barındıran kurumsal bir yapıya ihtiyaç olduğu düşünülmektedir. Ülkemizde böyle bir yapının bulunmamasından dolayıdır ki kurumlarımıza karşı, devletin çok ciddi önemli bilgilerine karşı güvenlik noktasında savunma zafiyetlerimiz olduğu düşünülmektedir. Bu tür bir otoritenin kurulmasıyla aynı zamanda İnternet kullanıcılarının kişisel mahremiyet ve siber ortamdaki kimliğin sınırlarından sorumlu olmalı ve medya üzerinden farkındalık oluşturmalıdır. Bunun yanında, Siber Güvenlik Strateji Belgesi'nin hemen sonrasında Siber Güvenlik Uygulama Eylem Planının hazırlanması gerekir. Bu eylem planı doğrultusunda da

kurumsal anlamda, yasal anlamda, teknik anlamda altyapıların bir an önce faaliyete geçirilmesi gerekmektedir.

Ayrıca siber tehditlerin doğrudan hedefi haline gelen ve zarar görmesi halinde toplumsal düzeni bozabilecek kritik altyapıların tespiti ile bilgi teknolojilerinin kullanımından kaynaklanan risklerin analizinin yapılması, olası risklerin kapatılması için gerekli karşı önlemlerin belirlenmesi ve uygulanması gerekmektedir.

8. Kritik altyapılara yönelik saldırıların birçoğunu engellemek için milli bir anti-virüs programı geliştirilmesi, yüklenmesi ve bunun düzenli bir şekilde güncellenmesiyle giderilebilir. Uluslararası çevrelerde kabul görmüş kabiliyette bir Milli anti-virüs ve güvenlik duvarı (firewall) yazılımının geliştirilmesi gerekmektedir.

9. Bulut bilişim ve barındırma hizmetlerinin gelişimi ve fırsatlarından ulusal düzeyde azami olarak istifade edilebilmesi için; hizmet alıcıların ve sağlayıcıların sorumluluklarının netleştirilmesi, kişisel verilerin gizliliğinin korunmasına ilişkin düzenlemelerin yapılması, ülkemizde ve dünyadaki bulut bilişim uygulamaları incelenerek ülkemiz için uygun stratejilerin belirlenmesi amacıyla ilgili kurumların (BTK, TÜBİTAK vb.) çalışması gerekmekte ve en uygun teknik ve yasal çözümlerin üretilmesi gerekmektedir.

10. Bilgi Güvenliği konuları altında ulusal çapta yapılan çalışmalara destek verilmesi ve projeler oluşturulması için stratejik yol haritaları belirlenmesi, güvenlik çözümleri üretici firmaların ve kurumlarla Ar-Ge ekiplerinin işbirliği içinde çalışması, bilgi ve tecrübe paylaşım sağlayacak imkânların sağlanması gerekmektedir.

11. Farklı kurumların güvenlik hassasiyetleri birbirinden farklı olabilmektedir. Bu nedenle, tüm kamu/özel kurum ve kuruluşlarda aynı kişisel bilgilerin bulunmasının yerine, merkezi ve güvenli bir veri tabanında sorgulamalarda bulunulabilmesine olanak sağlanması, silinemeyecek seviyede erişim kayıtlarının tutulması ve bu kayıtların denetlenmesiyle kişisel bilgilere rahat bir şekilde ulaşılması engellenmesi gerekmektedir.

12. Rol tabanlı kimlik doğrulama mahremiyeti sağlamada kullanılan bir yöntem olup yetkiye yeteri kadar bilgi verilmesi şeklinde tarif edilebilir. Bu bağlamda elektronik kimlik kartlarına mahremiyeti koruyan rol tabanlı sistemler eklenebilir. Sözgelimi kişi seçmen olduğunu ispat için adres bilgisini gösteren bir elektronik sertifika Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nden alınabilir ve bu sertifikayla vatandaş örneğin anket/referandum yapılacak bir belediye sınırları içerisinde olduğunu ispat edebilir. Böylece, adres bilgisi

dışında hiçbir bilgi sistem tarafından bilenemeyecek ve kişinin oy mahremiyeti sağlanabilecektir.

13. Elektronik haberleşme sektöründeki işletmecilerin haberleşmenin gizliliği ve güvenliğini sağlamak üzere gerekli tüm önlemleri alması, buna yönelik izinsiz erişimleri önlemek için gerekli teknik yazılım ve donanım yatırımlarını yapması, ilgili logların tutulması ve kayıt altına alınması gerekmektedir.

14. Tüketimi hızla artan mobil elektronik haberleşme cihazları başta olmak üzere telekomünikasyon alt yapısında kullanılan cihaz, donanım, santral, bilişim teknolojisi ürünlerini, gömülü sistemler ve yazılımların milli olmasının teşvik edilmesi, bunları üreten firmaların desteklenmesi ve bu konuda yapılan AR-GE faaliyetleri teşvik edilmesi gerekmektedir.

15. Bilgi kaçaklarının önlenmesi hususunda kurum ve kuruluş personellerinin eğitim ve akreditasyonuna yönelik faaliyetler yapılmalı, yine bu bağlamda kritik tesislerin binaların inşaat aşamasından itibaren kontrollerinin sıkı tutulmalı, binalar dışarıya elektromanyetik sızmaları engelleyecek şekilde tasarlanmalı ve gerekli önlemler alınmalıdır.

16. Elektronik Haberleşme sektöründe kritik veri veya sistemlere ulaşabilecek kişilerin belli periyotlarda güvenilirlik soruşturmasının yapılması, sistem yetki ve erişim haklarının düzenli olarak kontrol edilmesi, gereksiz hakların alınması, girişlerin biyometrik tanımlama sistemleri ile yapılması, güvenliğin artırılması için pin, elektronik imza kullanılmalıdır. Ayrıca bu sistemlerin bulunduğu mekânlar 7/24 kamera ile izlenmeli ve giriş çıkışların kaydedilmelidir.

17. Ülkemizdeki farklı amaçlarla oluşturulan bütün güvenlik kameralarının (Karayolları, Belediyeler ve Kent güvenlik merkezleri gibi) MOBESE sistemi ile entegre edilmesi, bunların kayıtlarının bir merkezde toplanması, elde edilen kayıtların farklı amaçlarla kullanılmasının engellenmesi, devletin bu tür suçlarla mücadelede hassas ve takipçi olduğu kanısı kamuoyuna yaygın olarak yerleştirilmelidir. Güvenlik kamerası kayıt yapılan yerlerde mutlaka çekim yapıldığını belirten göze çarpan uyarılar bulunmalıdır. Bulundurmayanlar hakkında cezai müeyyide getirilmelidir.

18. MOBESE görüntülerinin kamuoyu ve kişilerle paylaşılması noktasında düzenlemeler yapılmalı, özellikle trafik kazası görüntüleri kamuoyunu bilinçlendirmeye matuf sadece bir kamu spotu çerçevesinde yer ve zaman belirtmeden yayınlanabilmelidir.

19. Akıllı telefonlarda kullanılan çeşitli casus yazılımların reklam ve satışının yasaklanması, bu tür yazılımları yükleyen ve haberleşme özgürlüğü ve iletişimin gizliliğine yasa dışı şekilde müdahalelere uygulanan yaptırımlar ağırlaştırılmalıdır.

20. GSM böcek üretmek için kullanılan GSM devrelerinin yolcu bagajlarında yurda sokulduğu ve bu böceklerin yurtiçinde imal edildiği, daha sonra bu cihazların IMEI klonlama yöntemi ile yurtiçi şebekelere uyumlu hâle getirildiği, ayrıca eski bir cep telefonunun içeriğinin de bir dinleme cihazına dönüştürülebileceği, yine doğrudan ithal edilen GSM dinleme cihazlarının da klonlanarak satıldığı düşünüldüğünde ikinci el ve hurda cep telefonların imhası ile ilgili bir düzenleme yapılması gerekir.

21. Telekomünikasyon şirketlerinin altyapılarını millileştirmeleri doğrultusunda teşvikler verilerek milli Telekom sektörü oluşturulmalı ve bu alanda dışa bağımlılık azaltılmalıdır.

22. Dünya genelindeki açık kaynak kodlu yazılım birikiminden yararlanmak adına açık kaynak kodlu yazılım geliştirilmesi ve kullanımının yaygınlaştırılması teşvik edilmelidir.

23. Bilişim ve elektronik haberleşme hukukunun bağımsız bir bilim dalı olarak kabul edilmesi ve bu konuya yükseköğretim müfredatında yer verilmesi ve bu konuda lisans ve lisansüstü programların açılması önerilmektedir.

24. Kamuoyunu yanıltma ve toplumda kargaşa oluşturma amaçlı haberlere karşı doğru ve hızlı karşılık verilebilmesini teminen, kamu kurumlarının sosyal medyada resmi hesaplarıyla yer alması ve kritik toplumsal olaylarda kamuoyunu doğru bilgilendirebilecek yapıların kurulması tavsiye edilmektedir.

KARAR CETVELİ



TÜRKİYE BÜYÜK MİLLET MECLİSİ

Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan Meclis Araştırması

Komisyonu

(10/74, 471, 472, 473, 474, 475)

Esas No : 53668891

12.06.2013

Karar No: 3

KARAR

“Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi” amacıyla kurulan, 10/74, 471, 472, 473, 474, 475 Esas Numaralı Meclis Araştırması Komisyonunun, yaptığı araştırma ve incelemeler sonucu düzenlemiş olduğu bu Rapor, Genel Kurula sunulmak üzere Yüksek Başkanlığa saygı ile arz olunur.

Yusuf BAŞER
Yozgat Milletvekili
Başkan

Hamza DAĞ
İzmir Milletvekili
Başkanvekili

Yılmaz TUNÇ
Bartın Milletvekili
Sözcü

Mihrimah Belma
SATIR
İstanbul Milletvekili
Kâtip

Namık HAVUTÇA
Balıkesir Milletvekili
Üye
(Muhalefet şerhim
ektedir.)

Ali ERCOŞKUN
Bolu Milletvekili
Üye

Bilal UÇAR
Denizli Milletvekili
Üye

İlhan CİHANER
Denizli Milletvekili
Üye
(Muhalefet şerhim
ektedir.)

Enver ERDEM
Elazığ Milletvekili
Üye
(Muhalefet şerhim
ektedir.)

Şuay ALPAY
Elazığ Milletvekili
Üye

Atila KAYA
İstanbul Milletvekili
Üye
(Muhalefet şerhim
ektedir.)

Şirin ÜNAL
İstanbul Milletvekili
Üye

Erdal AKSÜNGER
İzmir Milletvekili
Üye
(Muhalefet şerhim
ektedir.)

Mehmet Siyam
KESİMOĞLU
Kırklareli Milletvekili
Üye
(Muhalefet şerhim
ektedir.)

Hasip KAPLAN
Şırnak Milletvekili
Üye
(Ayrışık oyum ekedir.)

Fatih ÇİFTÇİ
Van Milletvekili
Üye

MUHALEFET ŞERHLERİ

Balıkesir Milletvekili Namık Havutça, Denizli Milletvekili İlhan Cihaner ve Kırklareli Milletvekili Mehmet Siyam Kesimoğlu’nun Muhalefet ve Ek Katkı Şerhi

Giriş ve Araştırma Komisyonlarının Çalışma Süresi ve Biçimi

TBMM’deki dört partinin önergeleriyle kurulan Komisyonumuz hakkında öncelikle şunu belirtmek bir görevdir: Komisyonumuz çalışmalarına büyük bir anlayış ve içtenlik içinde başlamıştır. Bunda o zamanki komisyon başkanımız, AKP Tokat Milletvekili Sayın Zeyid Aslan’ın tutumunun önemli katkısı olmuştur. Malum ve meşum hadise olana kadar iktidar-muhalefet ayrımı yapmadan herkesin görüşlerine kulak vermiş ve iyi niyet göstermiştir.

Bu nedenle kendisine teşekkür etmek kadirşinaslığın bir gereği, ama milletvekilimiz Kamer Genç’e söylediklerinin kabul edilemez olduğunu ve komisyon üyesi tüm CHP milletvekilleri olarak bu tavrı şiddetle kınadığımızı belirtmek de TBMM’ye saygımızın gereğidir.

Bu olaydan sonra sayın Aslan komisyon üyeliğinden ve başkanlığından ayrılmış, ondan sonra da komisyonumuz yalnızca rutin bir toplantı dışında hiç çalışmamış, Komisyonumuza başvuran şikayetçiler dinlenmemiştir. Rapor sürecinin 4. ayın sonundan başlaması gerekirken Komisyon son bir ayını yalnızca raporunu yazmaya ayırmıştır. Bundan sonra kurulacak araştırma komisyonlarının çalışmalarına yol gösterebilmek amacıyla bunun özellikle belirtilmesine gerek görülmüştür. Araştırma komisyonlarının uzatılan görev süresi rapor yazımı için değil, araştırmalarını devam ettirmeleri içindir.

Komisyonun kuruluşuna mecliste grubu bulunan tüm partiler katkı verdiği halde Başkan, başkanvekili ve sözcüsü İktidar partisi tarafından belirlenmiştir. Bu durum çalışmaların da (kimlerin dinleneceği, uzmanların belirlenmesi, çalışma yöntem ve süresi, vs.) İktidar partisi tarafından domine edilmesi sonucunu doğurmuştur.

Çok önemli olabilecek bazı araştırma talepleri/işlemleri Anayasa’nın 138. maddesi (görülmekte olan bir dava hakkında Yasama Meclisinde yargı yetkisinin kullanılması ile ilgili soru sorulamayacağı, görüşme yapılamayacağı, görüşme yapılamayacağı veya herhangi bir beyanda bulunulamayacağı) bahane edilerek yapılmamıştır. Oysa kısa adlarıyla hatırlayacak olursak, Darbeleri Araştırma, Uludere, Susurluk, Faili Meçhul Siyasi

Cinayetleri araştırma Komisyonları gibi, soruşturma ve davaları devam eden olay ve olgularla ilgili komisyonlar kurulmuş ve bazı önemli sonuçlara ulaşmıştır.

Komisyonun çalışma ziyaretleri “tutanağa” bağlanmamıştır. Bu nedenle “tüm yurttaşların iletişimlerinin tespit edildiğine” dair beyanlar gibi çok önemli bazı soru ve cevaplar kayıt altına alınamamıştır.

İlgili kurum ve kuruluşların komisyon nezdinde dinlenen temsilcileri sınırlı bilgi ve yetkiye sahip oldukları için bazı konular aydınlatılamamıştır.

Araştırma konusu ihlaller ağırlıklı olarak kamu gücünü kullanan (ya da göz yumulan) kişilerce yapılabileceği tartışmasız bir gerçek iken, çalışmalarda bu birimler (seçilen uzmanlar, görüşler, vs.) referans alınmıştır.

Son olarak şu da belirtilmelidir ki, Komisyonumuz bazı oturumlarda hiç gerekmediği halde, iktidar partisinin çoğunluğu ile toplantıların “gizli” yapılmasına karar vermişse de, ne toplantıya katılanlar bu güvence ile daha çok bilgi aktarmış, ne de toplantıda konuşulanların gizli kalması sağlanabilmiştir. Komisyonumuza dinleme ve izleme konusunda verilen teknik bilgiler, 2009’da eski Genel Sekreterimiz Sayın Sav’ın telefonunun yasa dışı dinlenmesine ilişkin olarak kurulan Meclis Araştırma Komisyonu’na verilen bilgilerin ötesine geçememiştir. Bu nedenle “devlet sırrı” gibi gerçekten gizlilik gereken oturumlar dışında, araştırma komisyonları gizli toplantı yapmamalıdır.

Bu arada hem yasaya en uygun biçimde kayıt tutan ve hem de bu bilgileri bizimle açık yüreklilikle paylaşan Jandarma İstihbaratı olmuştur. Kendilerine bu nedenle ayrıca teşekkür ederiz.

Komisyon, Kuruluş Nedeni Olan Olayların Sorumlularını Ortaya Çıkaramamıştır. Bunun İçin Soruşturma Komisyonu Kurulmalıdır.

Komisyonumuzun çalışmaları sonucunda Türkiye’de komisyon başkanımız, alt komisyon başkanımız dâhil, biz milletvekilleri dahil herkesin dinlendiği gerçeği bir kez daha ortaya çıkmıştır. Emniyet İstihbarat Daire Başkan Yardımcısı; “bunlar oluyor, bakın fiyatlarını bile belirlemişler, SMS takibi 350 lira, SMS ortam dinleme 600 lira, SMS ortam dinleme ve canlı telefon dinlemeleri için 500 lira istenildiği öğrenildi” diyerek durumu bütün çıplaklığıyla ortaya koymuştur.

Ancak, bunların faillerinin bulunmasına yönelik hiçbir çalışma yapılmamış, bunun için çok önemli bilgileri paylaşabileceği açık Eski Emniyet Müdürü ve Emniyet İstihbarat

biriminin kurucusu sayılan Hanefi Avcı komisyon tarafından dinlenmemiş, komisyona bu konuda bilgi veren Eski İstihbaratçıların görüşleri ve çözüm önerileri rapora aktarılmamıştır.

Başbakanının evindeki çalışma ofisinden böcek çıktığı -bu yüzden komisyonumuzun adı da basında “böcek komisyonu” olarak kalmıştır-, ana muhalefet partisi genel başkanının, diğer muhalefet partisinin genel başkan yardımcılarının, milletvekillerinin özel yaşama ilişkin görüntülerinin yayınlandığı bir ülkede, bunların ortaya çıkarılması amacıyla kurulan komisyon, bu alanda hiçbir ilerleme sağlayamamış ve raporunda da buna ilişkin hiçbir husus yer almamıştır.

ABD’de yaşayan eski bir istihbaratçının Türkiye’ye gelip yine eski bir istihbaratçı eliyle bir çiftlikte dinleme ve izleme için özel ekipler yetiştirdiği, bu ekiplerin evlere, ofisleri, işyerlerine dinleme ve izleme sistemleri yerleştirmeye çalıştığı, Emniyet ya da Savcılık’taki ifadelerin ilgili kişi daha mahkemeye sevk edilmişken basına sızdırıldığı, DGM savcısının kayıtlarının internete düştüğü, Kara Harp Okulu Komutanının, Genelkurmay Elektronik Sistemler Komutanının, Deniz Kuvvetleri Komutanlığı Eğitim ve Öğretim Komutanının ve Genelkurmay Başkanı’nın “sızmalara karşı” konuşmasının ses kayıtlarının yayınlandığı bir ülkede, konunun yalnızca “araştırma” ile yetinilmesi doğru değildir.

Komisyon Raporu’nda Hukuki Düzenlemeler Hakkındaki Önerilere İlişkin Görüşlerimiz

Komisyon raporunda 28 hukuksal düzenleme önerisi bulunmaktadır. Bunların büyük bölümü komisyonumuzun kuruluş aşamasından itibaren üzerinde fikir birliği oluşan, dünyanın başka ülkelerinde de örnekleri bilinen önerilerdir. Bunları teker teker ele almak yerine CHP’li komisyon üyeleri olarak şu genel ilkeyi kayıtlara geçiriyoruz:

Bu düzenlemelerin tümü, özgürlükleri geliştiren ve hakları sağlam güvencelere kavuşturan bir anlayışla yapıldığı takdirde yanındayız, aksi takdirde karşındayız.

Rapor tarihinde İstanbul Gezi Parkı’nda verilen ve bütün dünyanın haklı takdir desteğini kazanan hak ve özgürlük mücadelesine karşı -Komisyonun CHP’li üyeleri olarak, “toplumsal medyayla örgütlenen ayaklanma” olarak insanlık ve bilim tarihine geçen bu eylemi gerçekleştirenleri saygıyla selamlıyor, hükümetin kullandığı şiddeti nefretle kınıyoruz- Sayın Erdoğan’ın ve AKP hükümetinin antidemokratik tavrı, Komisyon

Raporu’nda yer alan bazı önerilerin tam tersi biçimde, özel yaşamı daha da zapt ü rapt’a alan, haberleşme özgürlüğünü ve diğer temel hak ve özgürlükleri kısıtlayan biçimde kullanılabileceğinin işaretlerini vermektedir.

İktidarın komisyon raporunda yer alan kimi düzenleme önerilerini bu amaçla kullanma olasılığına peşinen dikkat çekiyor ve herkesi uyarıyoruz.

Gerek mecliste yapılan toplantılarda, gerekse çalışma ziyaretlerinde elde edilen bilgilerin rapora yansıtılmadığı görülmektedir. Şu örnek çarpıcıdır; MİT ve Emniyet Genel Müdürlüğünün ülkemizdeki tüm telefonların **“iletişim tespiti” bilgilerini periyodik olarak aldıkları**, görevlilerce ifade edilmişti. Ancak rapor, kamuoyundaki “...’hepimiz dinleniyor ve *izleniyoruz*’ algısının teknik olarak **mümkün olamayacağı** sonucuna da ulaşmıştır” diyebilmiştir.

Rapor, teknik ve hukuki durumun **“çok eksik”** bir fotoğrafını çekmekten ileri gitmemiştir.

Özellikle ihlallerin ağırlıklı kaynağı “idare” olduğu halde gene idareye bağlı denetim mekanizmasının (Mülkiye Teftiş Kurulu(!), Başbakanlık Teftiş Kurulu) öngörülmesi tüm raporu anlamsız hale getirmektedir.

Emekli istihbarat daire başkanlarının çok önemli tespitleri adeta görmezden gelinmiştir.

Sonuç olarak; rapor tespit ve önerileriyle kuruluş amacına yaklaşamamıştır.

Dinleme ve İzleme Çalışmaları Bağımsız Bir Komisyon Tarafından Denetlenmelidir.

Resmi kurumların verdiği bilgiye göre, bu ülkede hiç yasa dışı dinleme izleme yapılmamaktadır.

AKP’nin kurduğu TİB, kendisinin yalnızca aracılık görevi yaptığını, dinlemeleri ilgili istihbarat birimlerinin personelince yapıldığını belirtmekte; ilgili kurumlar MİT, Emniyet İstihbarat ve Jandarma İstihbarat, iletişim bağı TİB’in kurduğunu kendilerinin bir payı olmadığını savunmuşlardır.

Ancak gözlemimiz odur ki, iktidar ya da onu kullananlar, TİB ve Emniyet üzerinden yine uygun gördüğü dinlemeleri yapmaktadır. Bunun göstergesi, TİB’in dinleme kararlarına yaptığı itirazlardır. TİB, Jandarma İstihbaratı’nın dinleme kararlarına itiraz

etmekte, ama Emniyet’in dinleme isteklerine itiraz etmemektedir. Bu, iyi bilinmesi ve niçin böyle olduğu üzerine de düşünülmesi gereken bir durumdur. TİB ve Emniyet arasındaki bu bağlantının nedenini ve bir cemaatle bağlantısı olup olmadığını ortaya çıkarmak gerekmektedir.

Dinlemelerle ilgili diğer bir eksiklik, dinleme hakkındaki mahkeme kararlarındaki özensizliktir. Hâkimlerimiz, dinleme kararı verirken, önlerine gelen liste ile olay-kışı bağlantısını ve kışı-telefon numarası bağlantısını iyice araştırmak ve ona göre karar vermek zorundadırlar.

Adalet Bakanlığı, defalarca sormamıza karşın, dinleme talebi reddedilmiş karar sayısını komisyona bildirememiştir.

Komisyonun kurulma gerekçesini oluşturan ihlallerin en önemli ayağı yargıya dair uygulamalardır. Hem yasal dinlemelerin hukuka aykırı kullanımı hem de yasa dışı dinleme ve izlemelerin etkin soruşturulmaması bir vakıa iken talep etmemize rağmen, Cumhuriyet savcılıkları ve mahkemelerin çalışma koşulları, sorunları, görüş, önerileri tespit edilmemiştir. Hatta yeterli istatistiki bilgiler bile toplanmamıştır.

HSYK ve Adalet Bakanlığının ilgili birimlerinden bilgi alınmamıştır.

Araştırma komisyonuna çok önemli katkı sunacakları tartışmasız olan bazı kişiler taleplerimize rağmen çağırılmamıştır.

Tüm ısrarlarımıza rağmen, adli dinlemelerin ve izlemelerin icra edildiğı birimler - anlaşılmaz bir şekilde- araştırma konusu bırakılmıştır. Emniyet ve Jandarmanın yalnızca “önleyici dinlemeden” sorumlu “istihbarat” birimleri incelenmiştir.

“Dinleme” konusunda ülkeler arasında uygulamalar farklıdır; bazı ülkelerde “teknik dinleme”ye ya son çare olarak başvurulmakta ya da dinleme sonucunda elde edilen bilgiler yargılama aşamasında delil olarak kullanılamamaktadır, bazı ülkelerde ise parlamenterler hiçbir biçimde dinlenememektedir. Biz komisyonun CHP’li üyeleri olarak, parlamenterlerin yasa ile böyle bir zırha kavuşturulmasının, gerçeklere gözünü kapamak anlamına geldiğini, aslolanın her yurttaşın haberleşme özgürlüğünün yasal güvenceye kavuşturulduğu bir düzenin kurulması olduğunu düşünüyoruz.

Diğer ülke örnekleri göz önüne alınarak Türkiye’nin de ya dinlemenin “son çare” olarak kullanıldığı ya da dinlemelerin yargılamada hiçbir bakımdan delil olarak kabul edilmediğı bu iki sistemden birini seçmesi gerektiğine inanıyoruz.

Komisyon Raporu’nun Hukuki Önerileri’nin 15. maddesinde yer alan “Telekomünikasyon yoluyla yapılan iletişimin denetlenmesiyle ilgili tedbir kararlarına ilişkin ayrıntılı bilgi ve analizlerin kamuoyu bilgisine sunulma” önerisi bir çözüm gibi görünse de, bu açıdan yetersizdir: Yalnızca bilgilerin kamuoyuyla paylaşılacağıının bilinmesi bu birimlere yeterli yaptırım olmayacaktır.

Yapılan faaliyetlerin, daha sonra TBMM çatısı altında, içinde milletvekillerinden başka meslek odalarının ve demokratik kitle örgütlerinin temsilcilerinin de yer alacağı bir kurul tarafından denetleneceğinin bilinmesi, ihlalleri büyük oranda azaltacaktır.

Bu nedenle TBMM çatısı altında bir denetleme komisyonu kurulmasını öneriyoruz.

AKP’nin amacı, Uludere Araştırma Komisyonu’nda olduğu gibi konuyu kapatmak değilse;

1- Bu araştırma komisyonu, bir soruşturma komisyonuna dönüştürülmelidir.

2- Devletin resmi kurumlarınca yapılan bütün dinleme ve izlemeler başka ülkelerde olduğu gibi, TBMM’de kurulacak bir komisyon tarafından denetlenmelidir.

Mehmet Siyam KESİMOĞLU
Kırklareli Milletvekili

İlhan CİHANER
Denizli Milletvekili

Namık HAVUTÇA
Balıkesir Milletvekili

İzmir Milletvekili Erdal Aksünger'in Muhalefet Şerhi

TBMM’de grubu bulunan Siyasi Parti Gruplarının önerisiyle 12 Şubat 2013 tarihinde kurulan komisyonda ilerleyen süreçte ise çalışmalarının daha verimli olması için Hukuk ve Teknik olarak iki alt komisyon kurulmuştur. Süreçte komisyon çalışmaları başlangıçta komisyonun kuruluş amaçlarına göre çalışmış, daha sonrasında ise komisyon üyelerin talepleriyle değil, alt komisyon başkanlarının kişisel programlarına göre çalışmalarını sürdürmek zorunda kalmıştır.

Haberleşme Özgürlüğüne ve Özel Hayatın Gizliliğine Yönelik İhlallerin Tespiti ve Önlenmesine İlişkin Tedbirlerin Belirlenmesi Amacıyla Kurulan Meclis Araştırma Komisyonunca hazırlanmış olan raporda farklı bir Türkiye varmış gibi, sanki Türkiye’de bugüne kadar yasa dışı dinleme ve izleme hiç olmamış, bu nedenle kişiler ve kurumlar haksız yere mağduriyetler yaşamamış gibi, yeni hiç olmamış, yaşanmamış bir konu üzerinde çalışılıyormuş izlenimini veriliyor.

Taslak raporun yaklaşık 180 sayfalık bölümü Uluslararası Hukuk, Anayasa ve Türkiye’deki yasaların mevcut düzenlemeleri hakkında bilgilere yer verilmesine rağmen, son bölümde yer alan sonuç ve öneriler bölümü komisyon üyelerinin görüş ve önerilerinin tamamına yer verilmemiş, sadece Komisyon başkanlık heyetinin kabulüne göre rapor dizayn edilmiştir.

Hazırlanan Taslak raporda Komisyona bilgi veren ve komisyonun ziyaret ettiği kurum ve kuruluşların sunumları ve verdikleri cevaplar yer almamış, daha sonra sunum ve cevaplar özet olarak rapora konulmuştur.

Rapor Komisyonun 4 ay çalıştığı söyleniyor. Ancak komisyon bu kadar süre çalışmamış, çalışmaların devamı için ek süre alınacağı beklenirken, Son 1 aylık süre uzatımı rapor yazım süresi için kullanılmıştır. Çalışmalar sırasında 2 haftadan fazla bir sürede alt komisyon başkanlarının programları gerekçe gösterilerek çalışma yapılmamış, neredeyse 1,5 aylık bir süre heba edilmiş, **komisyon çalışmalarını engellenmiş ve kamuoyundan kaçırılmıştır.**

Adli olarak dinleme ve izleme yapmaya yetkili kuruluşlar yaptıkları dinlemeleri ilgili yasa hükmüne göre yapmadıkları, özellikle dijital dokümanlara dışarıdan müdahale edildiği, imha edilmesi gereken dokümanların bir yerlerde depolanıp daha sonra kullanıldığı veya başka kişi ve kuruluşlara servis edildiği, Bakanlık Başmüfettişlerinin

dokümanların imha edilip edilmediği ile ilgili görevlerini yerine getirmediği Komisyon çalışmaları sırasında tespit edilmesine rağmen bu konularla ilgili araştırma yapılmamıştır.

Komisyonunda özellikle talep edilmesine rağmen muhalefet parti temsilcilerinin komisyona bilgi vermesini istedikleri kişi ve kuruluşlar komisyona çağrılmamış, çağrılan kurum kuruluşlar ise komisyona yeterli cevaplar verilmemiştir.

Ülkemizde yaşanan yasa dışı dinlemelerle ilgili suç ve suçlulara karşı yetkili kuruluşların neden görevlerini yerine getirmedikleri raporda yer almamış, sınırlı bilgi ve yetkiye sahip kurum temsilcilerinin komisyonunda sunum yapması nedeniyle birçok konu açığa çıkarılamamıştır.

Komisyonunda sunum yapan eski Emniyet Genel Müdür Yardımcısı Emin ARSLAN'ın kaybolduğu iddia edilen 11 dinleme aracı ile ilgili olarak yaptığı bilgilendirmede, İsrail, Kanada, ABD firmalarından veya Almanya'da Rohde&Schwarz firmasından temin edildiği bilinen bu araçların hangi ülkelerden alındığı, hangi amaçla, nerelerde kullanıldığı, ithalatlarının yapılırken hangi prosedürün uygulandığının, paralarının nasıl ödendiğinin hatta amacı dışında bir Büyükşehir Belediye Başkanı'nın dahi bu araçlardan kullandığı iddialarının araştırılması sağlanamamıştır.

TT NET, PHORM ve TURKTRUST konuları raporda yer almış olmasına rağmen TURKTRUST şirketinin ürettiği, insanların tüm kişisel hesap hareketlerine, banka bilgilerine, elektronik postalarına, yazışmalarına kadar müdahale etme yetkisine sahip 2 adet hatalı sertifikanın bir tanesinin EGO Genel Müdürlüğü tarafından kullanıldığının tespit edilmesi, gözleri Ankara Büyükşehir Belediyesine çevrilmesine neden olmasına rağmen, bu sertifikanın nerelerde kullanıldığı, hangi işlemlerin yapıldığı, alt sertifikaların üretilip üretilmediği tespit edilmemiştir.

Komisyonunda sunum yapan Sabri UZUN'un **Türkiye'de yapılan yasa dışı işlemlerin tamamı devlet görevlileri tarafından yapıldığı**, kurumların başındaki insanların izni ya da iradesi olmadan böyle bir şey gerçekleştirilemeyeceği iddiası hükümetinde bu konuda sorumlu olduğunu ortaya çıkarmıştır.

BTK'nın üstünde dinleme ve izleme yapan kuruluşların faaliyetlerini denetlemek için bir üst kuruluş kurulması, ilgili yasaların ihlalleri yapan kişi ve kuruluşlara verilecek cezaların caydırıcı hale getirilmesi talebimiz raporda yer almamıştır.

Öncelikle Türkiye’de özellikle son 10 yılda yaşanan yasa dışı izleme ve dinlemelerin kimler tarafından yapıldığı, hangi amaçlarla yapıldığı, kimlere servis edildiği, harcamaların nereden ve nasıl karşılandığı, örtülü ödeneklerin kullanılıp kullanılmadığı, raporda yer almalıdır.

Türkiye’de hangi yabancı istihbarat örgütlerinin bulunduğu, eleman sayıları, bunların çalışma alanları, Türkiye’de hangi faaliyetlerde bulundukları, Türkiye’de ne kadar süre daha kalacakları, masraflarının nasıl karşılandığı, örtülü ödenek kullanıp kullanmadıkları, yaptıkları faaliyetlerden Türk Hükümetinin haberinin olup olmadığı konuları raporda yer almamıştır.

Komisyon üyelerinin dinlenecek kişiler ve kurumlarla ilgili talepleri karşılanmamış, gerek şahıs olarak komisyona başvuranlar, gerekse komisyon üyelerinin dinlenmesini istediği kişilerle ilgili başvurularının sonuçsuz kalmıştır.

Raporda Türkiye’de dinleme yapmaya yetkili kuruluşların hangi araç ve gereçleri kullandıkları, bu araç ve gereçlerin envanterlerinin olup olmadığı, nasıl ithal edildikleri, nerelerde hangi amaçlarla kullanıldığı yer almamıştır.

Log kayıtlarının tutulmasının önemi vurgulanırken Hrant Dink cinayetinde log kayıtlarının nasıl ve kimler tarafından, hangi amaçla değiştirildiğinden bahsedilmemiş, özellikle taklit baz istasyonları konusu yer bulmamış, A15, A25 araçlarının envanterleri ve nerelerde kimler tarafından hangi amaçlarla kullanıldıkları, hangi verilerin elde edilerek kimlere servis edildiği konusu raporda yer almamıştır.

Siyasi Parti yöneticilerine karşı yapılan itibarsızlaştırmalarla ilgili operasyonların nasıl, kimler tarafından hangi yetkilerle yapıldığı, elde edilen bulguların kimlerle paylaşıldığı konusu da raporda yer almamıştır.

İzleme ve dinleme cihazlarının ithali konusu yer almış, ancak bu zamana kadar ithal edilen amacı ya da amacı dışında kullanılan cihazların envanterinin çıkarılması yer almamıştır.

Komisyonun çalışmalarını bitirmesi tamamen siyasi bir karar olup komisyonun toplumdan kaçınılmasına ve komisyonun gerçek kuruluş amacı dışına çıkmasına sebep olmuştur.

ÖNERİLER

Mevcut komisyonun araştırma komisyonu olması, çalışmalarını amacına uygun olarak yürütmemesi nedeniyle, TBMM’de özel hayatın gizliliği ihlalleri, yasa dışı dinleme ve izlemelerin araştırıldığı bir soruşturma komisyonu kurulması son derece gereklidir.

TİB ve BTK tarafından son 10 yılda yapılan uygulamaların tekrar incelenmesi ve soruşturulması gereklidir.

Günümüzün teknolojisi karşısında dinleme faaliyetlerini belki bir ölçüde sınırlandırılması mümkün olsa da temelde bütünüyle engellenmesi mümkün olamaz. Bu nedenle Türkiye’de yasal olarak dinleme ve izleme yetkisi olan kuruluşları ve GSM operatörlerini denetleyen bağımsız bir kuruluş kurulmalıdır.

Bu kuruluşta İstihbarat Kuruluşlarının temsilcileri, HSYK, Cumhuriyet Başsavcılığı, Anayasa Mahkemesi, Sayıştay, Danıştay, Barolar Birliği ve Yasama organından temsilciler bulunmalı, 3 er ay arayla dinleme yapan kamu kuruluşlarını denetlemelidir.

Hem adli, hem de önleme amaçlı yapılan izleme ve dinlemelerde yetkilerini yasalara aykırı olarak kullanan yetkililere verilecek cezalar artırılmalı, dinleme ve izlemelerde CUMUK’ a göre yapılan düzenlemeler yeniden güncellenmeli ve uygulanacak cezaların caydırıcı olması için ilgili yaslarda değişiklik yapılarak cezalar caydırıcı hale getirilmelidir.

Suç unsuru bulunmadığı halde silinmeyen her türlü dataların, saklanmasına ve daha sonra başka kişi ve kurumlara servis edilmesinde ihmali bulunan kişi ve kurumlar hakkında ciddi ceza uygulamaları getirilmeli, bu dataların kanıt olarak kullanılmaması için düzenleme yapılmalıdır.

Mahkeme kararlarıyla yapılan dinleme ve takipler uygulanırken (devlet sırrı olsa dahi) bu dinleme ve takiplerin hangi kişi ve kurum tarafından, hangi işlemlerin yapıldığına dair kayıtlı envanterlerinin tutulması, dinleme yapmak için kullanılabilecek tüm araç ve gereçler içinde ayrı bir envanter tutulmalıdır.

Acil dinlemelerde hâkim kararı haricinde yapılan ve 24 saat içerisinde hâkime getirilmek zorunda olunan dinlemelerin kararını hangi kuruluş adına kimin talep ettiğini içeren kayıtlarının tutulması zorunlu hale getirilmelidir.

Türkiye’de dinleme ve izleme yapmaya yetkili kuruluşlara ait örtülü ödenekler ve bu ödeneklerden yapılan harcamaların denetiminin yapılacağı ayrı bir komisyon kurulmalıdır.

Bu kuruluşların örtülü ödeneklerden aldığı her türlü araç ve gereç kayıt altına alınmalı, envanterleri tutulmalıdır.

Kişiler bireysel olarak dinlendiğinden veya izlendiğinden şüphe duyduğu zaman, kendilerini korumak için dinleme engelleyici cihazları (kayıt altına alınmak şartıyla) alabilmelerine olanak tanınmalıdır.

Telekomünikasyon altyapısının ulusal anlamda imalat kodlarına hâkim olmadığımız sürece güvenlik anlamında bir sonuç alınabilmesi mümkün değildir. 1990’lı yıllarda Türkiye’de böyle birtakım çalışmalar yapılmış, ancak uluslararası bir firmanın çalışma yapan firmayı satın alarak tasfiye etmiştir. Ulusal ve bireysel güvenliğimiz için tüm GSM operatörlerinin santralleri ve kullanılan yazılımları yerli olmalı, GSM şebekelerinin nasıl kontrol edilebileceğine, nasıl denetim altına alınacağına ilişkin yasal düzenlemeler yapılmalıdır.

TİB’e veriler GSM operatörleri aracılığıyla gelmektedir. Bu nedenle öncelikli olarak denetim yapılması gereken yer asıl veri kaynakları olan GSM operatörleridir. Dinlemeler GSM operatörleri aracılığıyla yapılmaktadır. Türkiye’de yasa dışı dinlemelerin en önemli kaynağı olan GSM operatörlerinin kendi bünyesindeki hatlara izinsiz olarak yapılan girişleri engellemek için gerekli önlemleri almasını sağlamak gereklidir.

GSM operatörlerinin iletim hatlarının nerelerden geçtiği, güvenliğinin nasıl sağlandığı, hatların kriptolu olup olmadığı, hatlarda çoklama yapılmasının mümkün olup olmadığı, hangi yazılımların kullanıldığının tespit edilerek gerekli önlemlerin alınması gereklidir.

GSM operatörlerinin iletim hatlarına izinsiz girişleri önlemek için teknik yazılım ve donanımların sağlanması, ilgili logların tutularak sisteme kimlerin ya da hangi kurumların giriş yaptığı tespit edilerek kayıt altına alınmalı, ihlal edenlere ağır yaptırımlar getirilmelidir.

Dinleme ve izleme yapılan kuruluşların binalarının ve bu kuruluşlarda çalışan personellerin güvenliği sağlanmalıdır. Binalar Tempest veya Favadiay olmalı. Yani bina bir kafes gibi düşünülmeli dışarıya elektromanyetik dalga çıkışı engellenmelidir.

Giriş yerlerinde kullanılan bilgisayarların tümü biometrik olmalıdır. Bu işlerde görevlendirilecek personelin güvenilirliği test edilmeli, akreditasyon uygulanmalı, herkes kendi yetkisindeki işlemlere giriş yapabilmelidir. Bu işlemler tüm dinleme ve izleme yapan kuruluşlarla birlikte GSM operatörleri ve TİB’le birlikte bu kuruluşların bağlantıları olan tüm yerlerde (81 il) zorunlu hale getirilmelidir.

Dinleme ve İzleme yapma yetkisi bulunan kuruluşlar ve GSM operatörlerinde çalışanların özel kimlikleri olmalı, kimin nereye girip çıktığı bilinmelidir. Bilgisayar oturumlarına giriş şifreli olarak değil, biometrik (optik) el okuyucuyla yapılmalı, ayrıca güvenliği artırmak için pin ve elektronik imza kullanılmalı, sistemlerde güvenlik açısından kullanılan algoritmaların her görüşmede değişmesi gereklidir.

Cep telefonları ithal edilirken, Türkiye’de kullanım için mevcut yönetmeliğin değiştirilmesi ve kripto şartının getirilmesi gerekir.

Siyasi parti temsilcileri itibarsızlaştırmak için yapılan operasyonlarda kullanıldığı bilinen, çift sim kart takılarak kullanılan, görüntüleri 3G sistemiyle aktarılabilen, sim kartlarını arama veya SMS gönderme yöntemiyle çalışan kameraların hangi kurumlarda bulunduğu, bunların ülkeye hangi yollardan giriş yaptığı ve envanterlerinin bulunup bulunmadığı, sistemin bu güne kadar nerelerde kullanıldığı tespit edilmelidir.

Hrant DİNK cinayetinde logların değiştirilmesinde hem adli hem de idari olarak görev alan kişiler tespit edilmeli, bu kişilerin kimler adına bu işi gerçekleştirdiği tespit edilmelidir.

Türkiye’de yer tespiti ve sahte baz istasyonu olarak kullanılan A15, A25 olarak bilinen teknik cihazlar ve bu cihazların üst versiyonu hangi kurumlarımızda bulunduğu, bu cihazlar nerelerde ve ne amaçla kullanıldığı, ithalatların hangi kurum tarafından hangi ülkelerden yapıldığı tespit edilmeli, taklit baz istasyonlarının kullanımının engellenmesi gerekmektedir. Bunun içinde GSM operatörleri kullanıcılarına kriptolu kullanım sağlamak için gerekli alt yapıyı sağlamalıdır.

Bu cihazlar sahte baz istasyonu olarak kullanılıp kullanılmadığı, cihazlar kullanılırken herhangi bir mahkeme kararı alınıp alınmadığı, ithalatının hangi kurumlar

tarafından hangi ülkelerden yapıldığı, bu ithalat yapılırken örtülü ödenek kullanılıp kullanılmadığının araştırılması gereklidir.

MOBESE kameraları konusu raporda yer almıştır. Kamera görüntüleri insanların özel hayatına girecek şekilde İnternet ortamında yayınlanıyor. Kişilerin özel hayatının gizliliğini de ihlal ediliyor. Şahıslar bu konu kendileriyle ilgili eğer hukuki anlamda bir başvuruda bulunmazlarsa o konuda cezai anlamda veya kamusal anlamda bir yargısal tedbir veya idari bir tedbir geliştiremiyor. Ülkemizde de bütün kameraların MOBESE sistemlerine entegre edilerek bunların kayıtlarının bir merkezde toplanarak bu kayıtların giriş çıkışlarının kayıt altına alınması, elde edilen kayıtların farklı amaçlarla kullanılmasının engellenmesi, sisteme girenlerin kimler olduğu, hangi şifreleri kullandıkları kayıt altına alınması, devletin bu tür suçlarla mücadelede hassas ve takipçi olduğu kanısının kamuoyuna yaygın olarak yerleştirilmesi gerekiyor. Vatandaşlarımızın bu suçu işleyenlerin cezasız kalmayacaklarını bilinmesinin sağlanması gereklidir.

Son 10 yılda Emniyet, Jandarma, TİB, BTK ve MİT gibi kuruluşların sözleşmeli olarak çalıştırdığı personel sayıları, bu personellerin uzmanlık alanları, ayrıca bu kuruluşların kendi aralarında transfer ettiği personellerin kimler olduğu, bu personellerin uzmanlık alanları ve görevleri boyunca yaptıkları yurt dışı fuar ve gezileri, örtülü ödenekten harcama yapıp yapmadıkları, yurt dışı dönüşünde yanlarında getirdikleri cihazların neler olduğu, envanter kayıtlarının bulunup bulunmadığının araştırılması yasa dışı dinlemelerin ve izlemelerin nasıl yapıldığı konusunda yol gösterici olacaktır.

Komisyon çalışmalarının sonlandırılmasından sonra Türkiye’de yaşanan gelişmeler ayrıca incelenmelidir. Suç teşkil eden kullanımlar hariç olmak üzere, İstanbul Gezi Parkında başlayan ve tüm Türkiye’ye yayılan özgürlük mücadelesi gösterilerine katılan veya katılmasını teşvik ettiği gerekçesiyle sosyal medyayı kullanan kişiler hakkında işlem yapılması tamamen yasa dışıdır. Ana akım medyanın görevini yapmaması nedeniyle insanların sosyal medyayı kullanarak facebook ve twitter üzerinden haberleşmesi, AKP hükümetinin çare olarak bu hesapları kullanan kişilere yönelik uyguladığı baskı ve gözaltılar, haberleşme özgürlüğüne vurulan en büyük darbedir.

Türkiye’de milyonlarca facebook ve twitter kullanıcısı var. Twitter ana serverleri ABD’de olduğu için kullanıcılar hakkında yapılacak uygulamalar ABD yasalarına göre şekilleniyor. Ayrıca ABD yasalarına göre kişisel hak arama eylemleri suç kapsamında olmadığı için twitter hesaplarına ait bilgiler elde edilemez. Twitter kullanıcılarının IP

numaralarını ve kişisel bilgilerini vermemektedir. Ayrıca, başka kişilerin adına sahte hesap açabilmek mümkün olduğu için bu kullanıcılarında hesaplarının tespit edilmesi de kolay değildir.

Son günlerde basında ve kamuoyunda yer alan bilgilere göre MİT'in PTT, THY, Milli Eğitim Bakanlığı ile gizli protokoller yaparak bu kuruluşların sistemlerine dâhil olan kişilerin bilgilerinin elde etmesi üzerinde durulması gereken son derece önemli bir konudur. Bu yöntemle kaç kişinin hangi amaçla kişisel bilgilerinin alındığı ve depolandığı nerelerde kullanıldığı Hükümet tarafından açıklanmalıdır.

Siber Güvenlik, Elektronik Ticaret ve Kişisel Verilerin Korunması kanun taslağının bir an önce çıkarılması gerekliliği vurgulanması, yerli yazılım ve Ar-Ge çalışmalarına destek verilmesi, telekomünikasyon şirketlerinin altyapısının millileştirilmesi, Dedektiflik kanunu çıkarılması istenilmesi, MOBESE konusu ve alınması gereken önlemlerin raporda yer almış olması doğru bir uygulamadır.

Erdal AKSÜNGER
İzmir Milletvekili

Elazığ Milletvekili Enver Erdem ve İstanbul Milletvekili Atıla Kaya’nın Muhalefet Şerhi

Özel hayatın gizliliğine ve haberleşme hürriyetine yönelik ihlallerin araştırılması ve alınacak önlemlerin belirlenmesi amacıyla kurulan araştırma komisyonunca hazırlanmış olan raporda, mevzuat eksikliklerinin tamamlanması amacıyla birtakım tespit ve önerilere değinildiği ancak komisyonun gerek çalışma usulünün gerekse hazırladığı raporun, meselenin asıl sebeplerine inmekten uzakta olduğu ve ortadan kaldırılmasına yönelik tespit ve önerilere yer vermediği anlaşılmaktadır.

205 sayfadaki oluşan komisyon raporunun 180 sayfalık bölümünde özel hayatın gizliliği ve haberleşme hürriyetine ilişkin Uluslararası hukuk, Anayasa ve yasalarımızdaki mevcut düzenlemeler, yalnızca 25 sayfadaki sonuç ve öneriler bölümünde ise yasal düzenlemelerimizdeki eksiklikler yer almıştır. Ayrıca raporun hiçbir yerinde bu komisyonun kurulma amacı olan özel hayatın gizliliği ve haberleşme hürriyeti alanında yapılan ihlaller ve bu ihlalleri yapanların ortaya çıkarılması amacına matuf bir değerlendirme bulunmamaktadır.

Araştırma komisyonunca hazırlanan raporun, bu haliyle özel hayatın ve aile hayatının gizliliğinin korunması ve haberleşme hürriyetine yönelik ihlallerin ortadan kaldırılabilmesi amacına hizmet etmesi mümkün değildir. Çünkü, ihlalleri yapanların ortaya çıkarılması ve cezalandırılması sonucunu doğurmayan hiçbir uygulama bu amaca hizmet edemez ve etmeyecektir.

Meri mevzuatımız, bu ihlalleri yapanların cezalandırılması için gerekli uluslararası standartların üzerinde düzenlemelere haiz olmasına rağmen, uygulamada ihlalleri engelleyememiş, aksine AKP iktidarları zamanında gerek yasa dışı dinlemeler gerek özel hayatın gizliliğini ihlal suçları artan oranda bir hızla yükselmeye devam etmiştir.

Bu alanda ülkemizde yaşanan sorunun kaynağı bulunmak isteniyorsa yasalarımızdaki eksikliklerin yanında, uygulamaya yönelik kararlılığın gösterilmemiş olmasına bakmakta fayda olacağı aşikârdır. Ne var ki, komisyonca hazırlanan raporda, uygulamaya yönelik sorunlara hiç değinilmediği gibi işlenen suçları açığa çıkarmakla yükümlü olan Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve MİT Müsteşarlığı’nın neden görevini yapmadığı neden suç ve suçluları tespit etmediği sorularına cevap dahi bulunamamıştır.

Yine, özel hayatın ve haberleşme hürriyetinin ihlaline ilişkin suçlara, Cumhuriyet Savcılıkları ve Mahkemelerin neden sessiz kaldığı, bu suçların faillerini ortaya çıkarmak için neden harekete geçemedikleri sorularının cevapları da bulunamamıştır.

Haberleşme hürriyeti ve özel hayatın gizliliğine yönelik ihlalleri yapanların hiç birisinin tespit edilmemesi, yargılanmaması ve cezalandırılmamaları da; iktidarın bu yönde ciddi zan altında kalmasına hatta bizatihi bu usulsüzlükleri kendisinin yaptırdığına dair suçlamalarla karşılaşmasına neden olmaktadır.

Hukuk devletinde işlenen bu çeşit suçların faillerinin tespit edilememesi, haklarında yasal işlem yapılmaması başka nasıl izah edilebilir.

Özel hayatın gizliliğinin ihlalleri ve haberleşme özgürlüğüne yapılan yasa dışı müdahaleler üç şekilde karşımıza çıkmaktadır:

1. Yasal çerçevede yapılan adli amaçlı dinlemeler, önleme amaçlı dinlemeler ve iletişimin tespiti uygulamalarında; yasanın amacını aşan veya kamu görevlisinin yasal yetkisinin aşılması suç işlenmesi.

2. Bu yasal müesseseler yasanın amacı dışında tamamen suç işlenmesi amaçlanarak yasa dışı yöntemlerle kullanılması.

3. Suç örgütlerinin veya istihbarat örgütlerinin özel hayatın veya aile hayatının mahremiyetine yönelik işlemiş oldukları suçlar olarak karşımıza çıkmaktadır.

Bütün demokratik ülkelerde olduğu gibi ülkemizde de yasal çerçevede ve mahkeme kararı olmadan kişilerin izlenmesi, dinlenmesi, kayda alınması mümkün olmadığı halde, hatta ülkemizdeki yasal düzenlemelerin insan hakları sözleşmesine ve uluslararası normlara daha yakın düzenlemeler getirmesine rağmen, neden bizim ülkemizde daha fazla ihlallerin yaşandığı, neden faillerinin açığa çıkarılmadığı üzerinde durulması gereken bir husustur.

İletişimin denetlenmesi faaliyetleri kapsamında, telekomünikasyon sektörünün üçlü saç ayağını; karar mercileri, Bilgi Teknolojileri ve İletişim Kurumu ile işletmeler oluşturmaktadır.

Her üç aktörün de yasal çerçevede görevlerini yerine getirmesi için ihtiyaç duyulan bütün düzenlemeler yapılmaya çalışılsa da ortaya çıkan ihlaller her üç aktördeki

eksiklikler, ihmaller veya kötü niyetli uygulayıcılar nedeniyle ortaya çıktığı anlaşılmaktadır.

Komisyonla davet edilen uzmanların vermiş oldukları bilgiler çerçevesinde özel hayatın gizliliğine ve iletişime müdahalede kullanılabilecek çok çeşitli araç ve yöntemlerin olduğu ifade edilmiştir.

Uzman kişilerce yapılan bilgilendirmeler ve yasal olarak dinleme yapılan kurumların temsilcilerin verdikleri bilgiler çerçevesinde; kamuoyunda herkesin sürekli dinlendiğine dair kanaatlerin doğru olmadığı, Ancak TİB’in (Telekomünikasyon İletişim Başkanlığı) yüz bin civarında telefonu dinleme kapasitesinin olduğu değerlendirilmektedir.

TİB’in 2005 yılında kurulması ve 2006 yılından itibaren dinleme işlerinin bu kurumun bünyesinde tek çatı altında toplanmasıyla yasal dinlemelerin mevzuat çerçevesinde hukuka uygun olarak yürütülmesi ve gayri yasal uygulamaların ortadan kaldırılması gerekirken; 2006-2010 yılları arasında özel hayatın gizliliği ve haberleşme hürriyetinin ihlalleri hızla artarak bu yıllarda zirve yaptırmış, gayri hukuki dinlemeleri yasal bir kılıfa sokarak bu usulsüzlüklerin içinden çıkılmaz bir hal almasına neden olmuştur.

Milliyetçi Hareket Partisi olarak vermiş olduğumuz araştırma önergesinde, hükümetin ‘dinleme iddialarını’ gerektiği gibi araştırarak gereken tedbirleri yeterli ölçüde almadığı, bu konuda kamuoyunu aydınlatmak yerine olayları örtbas etme cihetine gittiği belirtilmiş, haberleşme hürriyetine ve özel hayatın gizliliğine yönelik ihlallerin tespit edilerek alınacak önlemlerin belirlenmesi, Ayrıca, 12 Haziran 2011 seçimleri öncesinde MHP tüzel kişiliğine ve yönetici kadrolarına ilişkin hazırlanan komploların açığa çıkarılması ve bu komploları yapanların belirlenerek gerekli soruşturmaların açılması amaçlanmıştı.

Ancak, kurulmuş olan komisyonun çalışma yöntemi ve ulaşmak istediği sonuçlar açısından, gerek MHP gerekse CHP’ye karşı yürütülen bu siyasi operasyonları yapanların ortaya çıkarılması gayretlerinin olmadığı, özellikle başbakanın ofisi ve makamında bulunan böcekler sonucunda, toplumdaki %80’lere varan ‘dinlenme endişesinin’ yersiz olduğu kanaatinin yaygınlaştırılmasını sağlamak amacını taşıdığı değerlendirilmektedir.

Özel hayatın gizliliği ve haberleşme hürriyetinin ihlal edilmesi suçunun tamamen siyasal iktidarın sorumluluğunda olduğu, bu suçları işleyenlerin yargı önüne çıkarılmasının da siyasal iktidarın görevleri arasında olduğu unutulmamalıdır.

Haberleşme hürriyetinin engellenmesinin bir ülkede milli güvenlik sorunu olduğu gibi aynı zamanda bir insan hakları sorunu olduğu, demokratik hukuk devletlerinde bu çeşit insan haklarının güvence altında olduğu ve ihlali yapanların önemli cezalarla cezalandırıldığı bilinmektedir.

Haberleşme hürriyeti ve özel hayatın gizliliğine yönelik ihlallerin araştırılmasına ilişkin kurulan araştırma komisyonunun çalışma usulünün ihlalleri ortaya çıkaracak nitelikte olmadığı; Ayrıca komisyonun ihlallerin araştırılması noktasında kendisine tanınan süreyi verimli kullanmayarak özellikle son 6 haftada kendisini tamamen işlevsizleştirdiği görülmüştür.

Komisyonunda somut sunumlar yapan uzmanlara komisyonun AKP’li üyeleri tepki göstermişler ve komisyon çalışmaları için faydalı olabilecek bilgilendirmelere müsaade etmemişlerdir.

Komisyon çalışmalarında Emin ARSLAN ve Sabri UZUN, komisyon çalışmaları dışında yapılan görüşmelerde de Hanefi AVCI gibi istihbarat dairesi başkanlığı görevlerini yürütmüş olan eski kamu görevlileri, yapmış oldukları açıklamalarda çok sayıda kişi ile ilgili organize ihlallerin devlet gücü kullanılmadan, iletişimin tespiti ve önleme amaçlı dinleme yetkisi olmadan yapılamayacağına vurgu yapmışlardır.

Komisyon çalışmaları sonucunda aşağıdaki tespitlerin yapılması uygun bulunmuştur.

1) Delilden sanığa gitme ilkesi doğrultusunda bilim ve teknolojinin imkânlarından yararlanarak, suçlunun yakalanması, delillerin elde edilmesi, suçun önlenmesi, suç ve suçlularla mücadele edilmesinin gerekli olduğu; Ancak anayasa ve yasalarla güvence altına alınan haberleşme hürriyeti ve özel hayatın gizliliğinin zedelenmemesi gerektiği, bu nedenle de; kamu otoritesinin bu hassas dengeyi sağlamak için, gerekli özeni gösterip hem bu yasaları yaptırmak, hem uygulamak hem de ihlal edenleri şiddetli bir şekilde cezalandırarak bu alanı güvence altına almalıdır.

2) Anayasa’nın 20 ve 22. maddelerindeki düzenlemeler ile CMUK’un 135 ve devamı maddelerindeki düzenlemelerin, AB ülkeleri ve diğer gelişmiş ülke

düzenlemelerine göre bazı eksiklikleri olsa da bu alandaki ihlallerin nedeni olarak gösterilmesini gerektirecek düzeyde eksiklikler olmadığı, ihlallerin sorumluluğunun AKP hükümetinde olduğu, iktidarın ihlalleri yapanların ortaya çıkarılması ile ilgili gerekli siyasi iradeyi ortaya koymadığı ve yapılan ihlalleri zımnen desteklediği anlaşılmaktadır. Zaten genel seçimler öncesinde hükümet mensuplarının yaptıkları açıklamalar söylediklerimizi kanıtlar niteliktedir.

3) Komisyon çalışmalarını belirleyen AKP milletvekilleri, komisyonun özellikle yasal dinlemelerin usul ve şekilleri üzerinde çalışmalar yapmasını sağlamıştır.

4) Komisyonun dinlediği kurum, kuruluş ve şahıslara sorulan sorulara, ya hiç cevap verilmemiş, ya yazılı olarak cevaplandırılacağı söylenmiş ya da yasal olarak yapmaları gereken şekilde yapıldığına ilişkin cevaplar verilmiştir.

5) Yapılan çalışmalarda TİB’in ‘‘dinleme kapasitesi’’ dâhil olmak üzere birçok teknik bilgi dahi alınamamıştır.

6) TİB’in yapmış olduğu denetimin ‘yetki aşımalarını’ engelleyecek nitelikte olmadığı anlaşılmıştır.

7) TİB’in iletişimin tespiti anlamında, ülkedeki bütün iletişimi kontrol ettiği bunun insan haklarına ve haberleşme hürriyetine uygun olmadığı anlaşılmıştır.

Ülkemizdeki toplam 75 milyon cep telefonunun görüşme ve mesajlaşmalarının tespit edilmesi ve bu yetkinin mahkeme kararları ile üçer aylık periyotlarla, hukuki müsaadeye dönüştürülmesi manidar bulunmuştur.

8) Teknik anlamda dinleme ve izlemelerin tamamen önlenemeyeceği ve teknolojiyi üreten ülkelerin dinleme ve izlemeler konusunda bir adım önde olduğu anlaşılmaktadır.

İnternet, cep telefonu, IP tabanlı telefonlar, ADSL’ler, bilgisayarlar, yazılım ve işletim sistemleri ile donanımın yabancı firmalardan temin edilmesinin ülke güvenliğini tehdit eder nitelikte olduğu anlaşılmaktadır.

9) Ülkemizde cumhurbaşkanı, başbakan ve genelkurmay başkanı da dâhil olmak üzere önemli kişi ve kurumların dinlendiği ulusal güvenliğin kevgire döndüğü görülmüştür.

10) Önemli kurum ve kuruluşların siber güvenlik anlamında riskler taşıdığı değerlendirilmektedir.

11) Hem adli hem de önleme amaçlı dinlemelerde; yasadaki amaçlar göz ardı edilerek ve iletişimin tespitine ilişkin yetkiler kötüye kullanılarak yasa dışı dinleme ve kayıtlar gerçekleştirildiği bilindiğine göre, yasal düzenlemelerin çok da fazla bir anlam ifade etmediği açıktır. Oysa hukukun üstünlüğünün esas alındığı bir ülkede yasaların koşulsuz uygulanması zorunluluktur. Bu kanunsuz uygulamaların önüne geçebilmek için öncelikle bu ihlalleri yapanların kamuoyunun karşısına çıkarılması, yargılanması ve cezalandırılması gerekmektedir. Aksi takdirde yasaları uygulayanlar aynı şahıslar olduktan sonra, yasaların sadece metinlerini değiştirmek çözüm olmayacaktır.

Önleme dinlemeleri terör, uyuşturucu, cebir ve tehdit içeren organize suçlar çerçevesinde suç işlenmesini önlemek ve ulusal güvenlik için ne kadar önemli olsa da bu alan kullanılarak yapılan gayrı yasal dinlemenin mutlaka önüne geçilmesi gerekmektedir.

Adli amaçlı dinlemelerde de yasada ayrıntılı bir düzenleme olmasına rağmen, hâkimlerin gözünden kaçan veya ihmal ettikleri durumlar olduğu görülmektedir. Bu hususta hata yapan hâkimlere de yaptırımlar getirilmelidir.

12) Dinleme ve izleme cihazlarının ithalatı ve kullanımı ile ilgili daha net düzenlemeler yapılmalı ve uygulamadaki belirsizliklerin önüne geçilmelidir.

13) Teknolojinin geldiği aşama, bugün hedefe konan kişi, yapı ya da devletlerin tamamen dinlenebileceğini göstermektedir. Bu durumu engellemek için “güvenlik tedbirleri” almanın gerekli olduğunu ancak yeterli olmadığını ifade etmek yerinde olacaktır. Bu nedenle evrensel yasal düzenlemelerin yapılması, siber güvenlik eylem planının hazırlanması ve siber savunma gücümüzün biran önce oluşturulması gerekmektedir.

14) Teknik olarak yasa dışı dinlemeler tamamen önlenemeyeceği için, yasal düzenlemelerdeki eksiklikler giderilmeli, görevini kötüye kullanan, yasanın amacını aşacak şekilde hareket eden kamu görevlilerinin tespiti için, denetim mekanizmalarının artırılması gerekmektedir.

Bu bağlamda, dünyadaki yasal dinlemelerde amacın aşılmaması ve görevin kötüye kullanılmaması için ne gibi denetim mekanizmaları kurulmuşsa, bu sistemler mutlaka incelenip benzer denetim mekanizmaları ülkemizde de kurulmalıdır.

Sonuç olarak, yasa dışı dinlemeleri araştırma komisyonunun çalışmaları neticesinde, özellikle yasal olarak dinleme yapan kurumların tepe noktalarında daha önce

görev yapmış eski kamu görevlilerinin komisyona yapmış oldukları açıklamalar göz önünde bulundurulduğunda, yasa dışı dinlemelerin tamamen yasal dinleme izni verilen kurumlar tarafından yapıldığı ortaya çıkmıştır.

Siyasal iktidar yasa dışı dinlemeleri yapan sanıkları ortaya çıkarma niyetinde olursa, derhal yasa dışı dinlemeleri soruşturma komisyonu kurarak çok kısa bir süre içerisinde tespitler yapılarak sorumluların mahkemelerin karşısına çıkarılması mümkün görülmektedir.

Yasa dışı dinlemeleri yapanların yargı karşısına çıkarılmadan, sadece bu alanda yapılacak düzenlemelerle özel hayatın gizliliğinin ve haberleşme hürriyetinin sağlanamayacağı çok net olarak ortaya çıkmıştır.

Atıla KAYA
İstanbul Milletvekili

Enver ERDEM
Elazığ Milletvekili

Şırnak Milletvekili Hasip Kaplan’ın Ayrışık Oyu

Yurttaştan, Başbakana, Cumhurbaşkanına, Genel Kurmay Başkanlığına, Anayasa Mahkemesi Başkanlığı dâhil, üst yargı kurumlarına, medyaya, siyasi partilere, sivil toplum örgütlerine kadar herkes dinlenmekte, haberleşme özgürlüğü ve özel hayatın gizliliği ortadan tamamen kalkmış bulunmaktadır.

Özellikle seçim dönemlerinde skandal kaset olayları şantajlar acı bir gerçeği ortaya çıkarmıştır, seçim yarışında hukuki ve etik olmayan yollara başvuranlar maalesef devlet görevlisi olup, açığa çıkarılamamıştır.

Meclis Araştırma Komisyonumuzun vardığı sonuç kaygı vericidir, yüzde seksenini devletin resmi görevlileri Emniyet, Jandarma, İstihbarat görevlileri yapmakta ve sadece “yürütmeye” hesap verebilen, denetlenemeyen bir kontrolsüz güç konumundadırlar.

90’lı yıllarda Jitem dâhil Genel Kurmay İstihbaratı, GES gibi farklı ve bağımsız dinleme istihbarat birimlerinin tamamı son beş yılda birleştirilmesine rağmen, TİB başkanlığında merkezileşen dinlemeler, MİT bünyesinde farklı bağımsız olarak yürütülmektedir.

Gizli dinlemelerin geri kalan yüzde yirmisini yabancı ülke ajan faaliyetleri, içerde çeteler, suç organize örgütleri yapmaktadır.

Analog sistemden dijital sisteme geçişin yaşandığı günümüzde teknoloji son derece hızla gelişmektedir. Sabit telefonlardan, GSM’lere uydu üzeri haberleşmeye sesin titreştiği her yerde, akıllı telefonlardan, bilgisayarlara casus yazılımlardan, böceklerle kadar dinleme araç ve aygıtları son derece yaygınlaşmıştır.

Kalem, anahtarlık, kravat iğnesi, gözlük, yüzük, priz, düğme, kül tablası, masa aksesuarları, tablolar, lambalar her obje bir cihaz olabilir.

Güç kaynağı ve uzun süreli dinlemelerde priz ve elektrik bağlantılı aletler kullanılırken, cam titreşimlerinden lazer dinlemelere, yabancı menşeli telefon santrallerine, yazılımın olduğu her araca kadar her türlü araçlar sesli, görüntülü kayıt, dinleme yapabilmektedir.

Teknik takip, ortam dinleme, telefon dinleme, bilgisayarlar üzeri tüm bilgilere erişim, bankacılık sektöründen, rekabete dayalı teknolojik AR-GE araştırmalarına kadar,

askeri ve güvenlik alanlarından uçaklara, uzay çalışmalarından günlük yaşama izleme ve kayıt altındadır.

Piyasada ekmek peynir gibi satılan internet üzeri her çeşit aracın satıldığı, denetlenmediği bir ülke konumunda olduğumuz acı gerçeği ile karşılaştık.

Asıl vahim olanı devletin görevlilerinin elindeki cihazların kayıt dışı olduğunu gördük, TİB, MİT, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığında sorularımızın çoğu “gizli” “devlet sırrı” gerekçeleriyle cevapsız bırakıldı.

Yasama yani Meclisin milletin iradesini temsil eden en üst irade olduğu, egemenliğin kayıtsız şartsız millette olduğu gerçeği, MİT, TİB ve kolluk birimlerinin kapısında sona ermekte ve meclisin üzerinde bir güçle karşı karşıya olduğumuzu gördük.

Meclis Araştırma Komisyonumuza, gezici dinleme araçlarının en eski modeli gösterilirken, kayıp 12 araçla ilgili sorularımız cevapsız kaldı. Dinleme kayıtlarının durumu netleşmedi, silinme ve denetim belirlenemedi, yargı karar ve uygulamaları vahim üzeri dehşet vericiydi. Araştırma ve inceleme esnasında komisyonumuzun üyelerinin vardığı ortak kanı, bize bilgi vermek yerine dalga geçiriyorlar oldu.

Araştırmalarımız sonucu vardığımız çarpıcı sonuçlar, önlemler konusunda ne kadar hassas davranmamız gerektiğini ortaya koyuyor. Bunları üç ayrı bölümde değerlendirmek gerekiyor.

1- Önleyici/İstihbari dinleme

Kolluk güçlerinin ve MİT’in yaptığı bu tür dinlemelerde yargı kararı yok, 81 ilde her emniyet müdürü veya komutan dinleme kararı alabiliyor, denetimi yok.

Kayıtlar silinmiyor, Özel Yetkili Mahkemeler delil olarak kullanabiliyor. Rahatlıkla medyaya sızdırılabilir.

2- Adli dinleme kararları

Anayasa, AİHS, 5397 sayılı kanunla önleme amaçlı dinleme tüm yasalar hukuk rafa kaldırılmış, uygulamada yargı kararları düşündürücüdür.

Bazı uygulama örnekleri vahameti ortaya koymaya yetmektedir, Ülke çapında iletişimin tespitine karar veren mahkemeler oldu, sınırsız süresiz ve kişi suç belirtilmeksizin dinleme kararları verildi. Kantarın topuzu öylesine kaçtı ki;

Medya tmden dinleme altına alınırken bazı yazarlar kod adları ile dinlendi, bazı yargıçlar kendi telefonlarının olduėu kararlara okumadan imza attılar.

Dinleme srelerine uyulmadı, CMK hkmleri yok sayıldı, yasa dıřı ahlak dıřı dinlemelerle elde edilen kayıtlar iddianamelerde yer aldı. Dokunulmazlıklara raėmen herkes dinlendi.

3- MİT’e son yasal deėiřikliklerle sadece Bařbakanın iznine tabi bir soruřtırma prosedr getirildi, devletin gvenliėi, devlet sırrı, meslek sırrı gibi kavramlar ardına sıėınılarak yapılacak hukuksuzluklar denetlenemez oldu.

Yasa dıřı dinlemelerin byk çoėunluėu uygulamadan kaynaklanmaktadır. Daha nce 3. yargı paketinde bizim nerdiėimiz biliřim dinleme suçlarında cezaların kısmen arttırılması etkili olduėu grlmřtr. Uygulama yařanan yasa dıřılıkların giderilmesi iin daha caydırıcı nemler alınması gerekmektedir.

Anayasal ve yasal dzenlemelerin, gizli ynetmelik ve genelgelere boėdurulduėu gereėi karřısında uygulamada yapılması gerekenlerin meclis kararı ile yasal olarak yeniden dzenlenmesi, ulusal st hukukun dikkate alınması gerekmektedir.

Kuvvetli řphe varlıėı, orantılılık, aıklık, denetlenebilirlik, geri bildirim, sreler, kayıtların korunması silinmesi, CMK 135-138 ve benzeri konularda daha somut dzenlemelere gidilmesi gerekmektedir.

Trkiye’de yařayan 76 milyon yurttařımızın ‘‘gizli dinleme sendromundan’’ kurtulması, hukukunun korunması en temel hak ve hrriyeti olup demokrasinin vazgeilmezidir.

1- Resmi devlet katında ki tm birimlerde dinleme cihaz ve aygıtlarının demirbař kayıt ve denetimi saėlanmalıdır.

Piyasada ekmek peynir gibi satılan tm cihazların giriř ıkıř ve satıřları denetim altına alınmalıdır.

2- zel Gvenlik, Detektiflik broları denetim altına alınmalı, yabancı ajan faaliyetleri, siber saldırılar konusunda daha etkili denetim yolları geliřtirilmelidir.

3- Adli dinlemeler sil bařtan yeniden dzenlenmeli, katalog sular, terrle mcadelede ve diėer tm alanlarda grevi ktye kullanan yargıdan kolluėa tm grevlilere caydırıcı cezalar getirilmelidir.

4- Dinlemelerin denetlenmesi için mecliste tüm partilerden ikişer milletvekilinden oluşturulacak bir denetleme birimi kurulmalıdır.

5- Medya meslek etik kuralları konusunda mecliste bir araştırma komisyonu kurulmalı ve öneriler doğrultusunda yasal düzenlemeler yapılmalıdır.

6- TİB'in yapısı ve görevleri yeniden düzenlenmeli 23 Temmuz 2006 tarihinden bu yana tek merkezi kurum olmasına rağmen istihbari/önleyici dinlemelerde uygulamada bunun dışına çıkıldığı görülmektedir.

7- Dinleme kayıtları tek başına delil olarak değerlendirilmemeli, iddianamelere alınmamalıdır.

8- Yeni anayasa çalışmalarında haberleşme özgürlüğü ve özel hayatın gizliliğinin korunması konusunda etkili düzenlemeler yer almalıdır.

9- Yeni anayasa çalışmaları ile Meclis İçtüzük Uzlaşma Komisyonu çalışmaları sürmekte olup, yeni içtüzükte meclis denetim komisyonu oluşturulması yer almalıdır.

10- Müdafilerin/milletvekillerinin, medyanın dinlemelerine mukayeseli hukuk sözleşmeler dikkate alınarak düzenlemeye gidilmelidir.

11- Bilgilerin sağlanması, korunması ve keyfiyetin önlenmesi konusunda iletişimin denetlenmesi için yeni bir yasal düzenlemeye gidilmelidir.

12- Beş yıl ve üzeri ağır hapis cezaları için dinleme kararları verilebilmelidir.

13- Dinleme istihbarat konularında kolluk ile MİT arasında ki kopukluk giderilmeli için yasal düzenleme yapılmalıdır.

14- Barış ve çözüm sürecinde, ülkemiz ve Ortadoğu'da yaşanacak gelişmeler dikkate alınarak, güvenlik ve özgürlük denkleminin mutlaka meclis denetiminde sağlanmalıdır.

15- Kişisel verilerin yabancı servis, telekomünikasyon iletişimde, GSM servislerinde, yabancı ortaklıklı bankalarda korunması ve müeyyide altına alınması sağlanmalıdır.

Raporun ortaklaştığımız önerileri dışında, farklı önerilerimiz ışığında ayrışık oyumuz bulunmaktadır.

Hasip KAPLAN
Şırnak Milletvekili

KAYNAKÇA

- A. KERCKHOFFS, “La cryptographie militaire”, Journal des Sciences Militaires, 9th Series (February 1883).
- ABBAS, R. MICHAEL, K. MICHAEL, M.G. ALOUDAT, A. Emerging Forms of Covert Surveillance Using GPS-Enabled Devices, Journal of Cases on Information Technology, vol. 13, no. 2, pp. 19-33 (2011), IGI Global.
- AKAD Mehmet/DİNÇKOL Abdullah, 1982 Anayasası, Madde Gerekçeleri ve Maddelerle İlgili Anayasa Mahkemesi Kararları, Alkım Yayınevi, İstanbul, 1998.
- AKYÜREK Güçlü, Özel Hayatın Gizliliğini İhlal Suçu (TCK m. 134), Birinci Baskı, Ankara 2011.
- AYCI Emrullah, İletişim Özgürlüğü ve Özel Hayatın Gizliliği, Polis Dergisi, Yıl 11, Sayı 45, Temmuz-Ağustos-Eylül, 2005.
- BALANIS Constantine A., Antenna Theory: Analysis and Design – Third Edition, John Wiley & Sons, Inc. (2005).
- BENSON Robert Louis, A History of U.S. Communications Intelligence during World War II: Policy and Administration, United States Cryptologic History, Series IV, Volum 8, Center For Cryptologic History, National Security Agency (1997).
- CAVE M., DOYLE C., WEBB W., Essentials of Modern Spectrum Management, Cambridge University Press (2007).
- CENTEL Nur, ZAFER Hamide, Ceza Muhakemesi Hukuku, 7. Baskı, İstanbul 2010,
- COE Lewis, The Telegraph: A History of Morse's Invention and Its Predecessors in the United States, McFarland (2003).
- ÇAKMAK Seyfullah, Hâkim ve Savcılar Hakkındaki Araştırma, İnceleme ve Soruşturma İşlemleri, Adalet Dergisi, 43. Sayı, Mayıs 2012.
- ÇINAR Soner, 2005, GPS İle Araç Takip ve Yönlendirme Sistemi, Yüksek Lisans Tezi, Ankara.

DANIŞMAN Ahmet, Ceza Hukuku Açısından Özel Hayatın Korunması, Selçuk Üniversitesi Yayınları, Konya 1991.

DEVELİOĞLU Ferit, Osmanlıca–Türkçe Ansiklopedik Lügat, 15. Baskı, Ankara 1998.

ERDEM Mustafa Ruhan, ÖZBEK Veli Özer, 4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu Çerçevesinde Uzakla Haberleşmenin Denetlenmesi, Prof. Dr. Seyfullah Edis’e Armağan, İzmir, 2000.

ERSOY Yüksel, Özel Telefon İşletmelerinin Dinleme ve Bilgi Verme Sorunları, Prof. Dr. Çetin Özek Armağanı, İstanbul, 2004.

GELERİ Aytekin, Türkiye’de İletişimin Denetlenmesi, SDE Analiz, Ankara, Temmuz 2010.

GÖKÇEN Ahmet, Ceza Muhakemesi Hukukunda Basit Elkoyma ve Postada Elkoyma, DEÜHF Döner Sermaye İşletme Yayınları No: 49, Ankara, 1994.

GÖZLER Kemal, Türk Anayasa Hukuku Dersleri, Ekin Kitabevi Yayınları, 9. Bası, Bursa, 2010.

GRUBER Robert, Physical and Technical Security: An Introduction, Thomson and Delmar Learning (2006).

GÜVEL Enver Alper, Organize Suç Ekonomisi ve Hukuk Uygulaması, Ankara 2004.

HALLIDAY David, RESNICK Robert, WALKER Jearl, Fundamentals of Physics – Fourth edition – Extended, John Wiley & Sons, Inc. (1993).

HECHT Eugene, Optics – Third Edition, Addison Wesley Longman, Inc.(1998).

HOLMA Harri, TOSKALA Antti, 2004, WCDMA for UMTS, Radio Access for Third Generation Mobile Communications Third Edition, John Wiley & Sons, West Sussex.

<http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper19.pdf>

http://en.wikipedia.org/wiki/Blackhole_exploit_kit

http://en.wikipedia.org/wiki/Brute-force_attack

http://en.wikipedia.org/wiki/HTTP_cookie

<http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/>, Haziran 2013

<http://tech.slashdot.org/story/11/12/02/2224256/was-conficker-stuxnets-trojan>

http://www.btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/TTNET-PHORM.pdf

<http://www.europarl.europa.eu>

<http://www.museumwaalsdorp.nl>

<http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf>

<http://www.stuxnet.net/>

http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

http://www.tubitak.gov.tr/sites/default/files/62_2013_104.pdf.

<https://www.turktrust.com.tr/kamuoyu-aciklamasi.1v2.html>

ITU-R, 2000, M.1455-1 No’lu “ Key Characteristics for the International Mobile Telecommunications-2000 (IMT-2000) Radio Interfaces” başlıklı tavsiye kararı.

JACKSON John David, Classical Electrodynamics - Third Edition, John Wiley & Sons, Inc. (1998).

JAWWAD Ahmad vd., 2003, 4G Wireless Systems, Next-Generation Wireless Working Group.

KALABALIK Halil, İnsan Hakları Hukuku, Seçkin Kitabevi, Ankara 2009.

KAYMAZ Seydi, Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Seçkin Yayıncılık, 1. Baskı, Ankara, 2009.

KEKLİK Ramazan, Ceza Yargılamasında İletişimin Denetlenmesi, Adalet Dergisi, Sayı 25,

KORHONEN Juha, 2003, Introduction to 3G Mobile Communications Second Edition, Artech House, Norwood.

- KUNTER Nurullah, YENİSEY Feridun, NUHOĞLU Ayşe, Muhakeme Dalı Olarak Ceza Muhakemesi Hukuku; Beta Yayınları; 18. Bası; İstanbul 2010.
- LINDELL Yehuda and PINKAS Benny, Secure Multiparty Computation for Privacy-Preserving Data Mining, The Journal of Privacy and Confidentiality, 2009.
- MARTINEZ Rut Sánchez, 2005, 3G Systems WCDMA (UMTS) & CDMA2000.
- MERAN Necati, Adli ve Öneme Amaçlı İletişimin Denetlenmesi Gizli Soruşturmacı Teknik Takip, Adalet Yayınevi, Ankara 2009.
- NUHOĞLU Ayşe, Adli Amaçlı Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi ile Teknik Araçlarla İzleme Tedbirine Konu Olan Suçlar, Yargı Dünyası, Sayı 128, Ağustos 2006.
- ÖZBEK Veli Özer, TCK İzmir Şerhi Yeni Türk Ceza Kanunun Anlamı, C. 2, Ankara 2008.
- ÖZTÜRK Bahri, 2006, Uygulamalı Ceza Muhakemesi Hukuku, Yeni Ceza Muhakemesi Kanununa Göre Yenilenmiş 9. Baskı, Seçkin, Ankara.
- ÖZTÜRK Bahri, ERDEM Mustafa Ruhan, Uygulamalı Ceza Muhakemesi Hukuku, Seçkin Yayınevi, 11. Bası Ankara 2007.
- PETER WRIGHT. Spycatcher: The Candid Autobiography of a Senior Intelligence Officer. New York: Viking Penguin Inc. (1987)
- POLAT Ahmet, Fransa’da Terörizme Karşı Mücadele, Polis Dergisi, Yıl 11, Sayı 46, Ekim-Kasım-Aralık 2005.
- ROEBUCK Kevin, 2011, 4G Standard, Emereo Pty Limited, Australia.
- SAYDAM Mehmet, Ceza Muhakemesi Kanununa Göre Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Oniki Levha Yayıncılık, İstanbul Ocak 2011.
- Secure Multi-Party Computation, http://en.wikipedia.org/wiki/Secure_multi-party_computation.
- SELEK Y. K., İLHAN E., YAYLA F., Esnek Spektrum Yönetimi: Spektrum İhaleleri ve Spektrum Ticareti, Bilgi Teknolojileri ve İletişim Kurumu (2010).

SEZER Yasin, İPEK Ali İhsan, PARLAK Engin, Adli ve Önleme Amaçlı İletişimin Denetlenmesi, Gizli Soruşturmacı, Teknik Araçlarla İzleme, Seçkin Yayınevi, Eylül 2012.

SIMONS R. W., GUGLIELMO Marconi and Early Systems of Wireless Communication, Gec Review, Vol. 11, No.1 (1996).

SIMPSON Rachel, Listening Devices And Other Forms Of Surveillance: Issues And Proposals For Reform, Briefing Paper No 20/97 (1997).

Side Channel Attacks, http://en.wikipedia.org/wiki/Side_channel_attack

Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing, NIST, 2005, <http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper19.pdf>

Sophos Security Threat Report 2013, <http://nakedsecurity.sophos.com/2012/12/04/sophos-security-threat-report>.

SÖZÜER Adem, Türkiye’de ve Karşılaştırmalı Hukukta Telefon Telefaks Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Yıl 1997, Sayı 3, Cilt LV.

Spectrum as a Technical Resource, InfoDev (Information for Development) & ITU Joint Project, ICT Regulation Toolkit, www.ictregulationtoolkit.org/en/Section.2658.html.

STERN Jonathan, The Audible Past: Cultural Origins of Sound Reproduction, Duke University Press (2003).

ŞAHİN Cumhur, Ceza Muhakemesi Şerhi, Seçkin Yayınevi, Ankara 2006.

ŞEN Ersan, Türk Hukuku’nda Telefon Dinleme-Gizli Soruşturmacı-X Muhbir, Seçkin Yayınevi, Ankara 2008.

TANENBAUM Andrew S., 2011, Computer Networks Fifth Edition, Prentice Hall PTR, New Jersey.

- TANÖR Bülent, YÜZBAŞIOĞLU Necmi, 1982 Anayasasına Göre Türk Anayasa Hukuku, İstanbul, 2004.
- TAŞKIN Mustafa, Adli ve Önleme Amaçlı İletişimin Denetlenmesi, Seçkin Yayınevi, Ankara 2011.
- TRAYNOR, Ian The Guardian 17 May 2007: Russia Accused Of Unleashing Cyberwar To Disable Estonia.
- TURGUTALP Mehmet Ali, 2011. Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi (5271 sayılı CMK'nın 135'inci maddesi). Yayınlanmamış Yüksek Lisans Tezi, Konya: Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Yüksek Lisans Programı.
- Türk Dil Kurumu, Güncel Türkçe Sözlük, <http://tdkterim.gov.tr/bts/22.04.2013>.
- ÜNVER Yener, HAKERİ Hakan, Sorularla Ceza Muhakemesi Hukuku, Türkiye Barolar Birliği, Ankara 2006.
- ÜZELTÜRK Sultan, 1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı, İstanbul 2004.
- WRIGHT Peter, Spycatcher: The Candid Autobiography of a Senior Intelligence Officer. New York: Viking Penguin Inc. (1987).
- XENAKIS Christos, MERAKOS Lazaros, “Security in 3G Mobile network ”, Computer communications, vol. 27, (2004).
- YARDIMCI Mehmet Murat, Amerika Birleşik Devletleri Hukuku, Avrupa İnsan Hakları Mahkemesi İçtihatları ve Türk Hukukunda İletişimin Denetlenmesi, Seçkin Yayıncılık, 1. Baskı, Ankara, 2009.
- YENİSEY Feridun, Çıkar Amaçlı Örgüt Suçlarındaki Araştırmalar, Hukuk Kurultayı 2000, Cilt 2, Ankara.
- YENİSEY Feridun, NUHOĞLU Ayşe, Global Hukuk Eğitim Programları (IGUL) Seminer Notları 2009-2010 Seminer Notları. İstanbul: Bahçeşehir Üniversitesi Hukuk Fakültesi IGUL Birimi.
- Yılmaz Ejder Hukuk Sözlüğü, Yetkin Yayınları, 2001 Ankara.

TUTANAK ÖZETLERİ

1- 12 Şubat 2013 Tarihli Toplantı

Komisyunun ilk toplantısında Komisyon Başkanlık Divanı seçimi yapılmış, Komisyonun çalışma usulüne ilişkin kararlar alınmıştır.

2- 14 Şubat 2013 Tarihli Toplantı

Komisyunun çalışma programı, Komisyon çalışmaları için davet edilecek kişi ve kurumlar ile sivil toplum kuruluşları, Komisyonca ziyaret edilmesi ve incelemelerde bulunulması gereken kişi ve kurumlar ile Türkiye Büyük Millet Meclisi dışından Komisyonunda görevlendirilecek uzmanlar belirlenmiştir.

3- 20 Şubat 2013 Tarihli Toplantı

Komisyon, 3'üncü toplantısında Adalet Bakanlığı ve Telekomünikasyon İletişim Başkanlığı yetkililerini dinlemiştir.

Adalet Bakanlığı adına sunum yapan Kanunlar Dairesi Başkanı Doç. Dr. Mustafa TAŞKIN sunumunda özetle;

- Mukayeseli hukuktaki iletişimin denetlenmesine ilişkin düzenlemeleri aktarmak amacıyla Almanya, Fransa, İtalya, Avusturya ve İngiltere'deki düzenlemelerin; iletişimin denetlenmesi kapsamında suçlar, süre, son çare prensibi, tanıklıktan çekilme, iletişiminin denetlenmesi özel usule bağlı olan kişiler, önleme amaçlı iletişimin denetlenmesi ve geri bildirim uygulaması açılarından ne şekilde olduğunu,

- Avrupa ülkelerinin hemen hepsinde iletişimin denetlenmesi tedbirinin hem adli hem de istihbari olarak uygulandığını,

- Ülkemizde iletişimin denetlenmesi tedbiri kapsamında beş tane alt tedbir olduğunu ve bu alt tedbirlerin; iletişimin dinlenmesi, kaydedilmesi, sinyal bilgilerinin değerlendirilmesi, iletişimin tespiti ve mobil telefonun yerinin tespiti şeklinde sıralandığını, ayrıca ilk üç tedbir bakımından farklı, dördüncü ve beşinci tedbirler bakımından daha farklı prosedürler öngörüldüğünü,

- İletişimin denetlenmesi tedbirine işlenmiş olan bir suçun aydınlatılması, şüpheli veya sanığın, kaçmakta olan şüpheli veya sanığın yakalanması ve istihbari amaçlı olarak, suç işlenmesinin önlenmesi amacıyla başvurulduğunu,

- İletişimin denetlenmesi tedbirlerinin uygulanmasının sakıncalarının; hem taraf olduğumuz uluslararası sözleşmelerde hem Anayasa’ımızda koruma altına alınan ve temel hak olarak nitelendirilen haberleşme hürriyeti ve özel hayatın gizliliğinin korunması gibi haklara ciddi bir müdahale oluşturuyor olması olduğunu,

- Son yirmi yıldır küreselleşmeyle, ülkeler arası sınırların kalkmasıyla beraber organize suçta, örgütlü suçta ciddi bir artış olduğunun görüldüğünü ve bireysel suçların yerini, örgütlü suçların almaya başladığını ve klasik ceza muhakemesi tedbirlerinin artık yetersiz kaldığını ve bunun sonucunda, sadece ülkemizde değil, bütün dünyada iletişimin denetlenmesi tedbirinin uygulanmasına ihtiyaç duyulduğunu,

- İletişimin denetlenmesi tedbirinin uygulamasında; sadece telekomünikasyon yoluyla gerçekleştirilen iletişimin kapsam içerisinde olduğunu, posta ve kargo yoluyla yapılan iletişimin kapsam dâhilinde olmadığını ancak telefonun yanında faks, e-posta, teleks, çağrı cihazları ve mesaj aletleri üzerinden gerçekleştirilen iletişimin de tedbir kapsamında olduğunu, ayrıca resmî veya özel, her türlü telefon (ankesörlü ve kartlı telefonlar dâhil) bakımından bu tedbire başvurulabileceğini,

- Başka yol ve yöntemlerle, klasik ceza muhakemesi tedbirleriyle amaca ulaşılabiliriyorsa, suç aydınlatılabiliriyorsa iletişimin denetlenmesi tedbirine başvurulmaması gerektiğini (son çare ilkesi),

- Talep ve karar bakımından kural olarak kararı hâkimin verdiğini ancak gecikmesinde sakınca bulunan hâllerde savcının da karar verebildiğini ancak savcının vermiş olduğu bu kararın ivedi bir şekilde, yirmi dört saatlik bir süre içerisinde hâkim onayına sunulması gerektiğini,

- İletişimin denetlenmesi tedbirinin uygulama süresinin üç ay olduğunu, ancak bir sefere mahsus olmak üzere gerekmesi hâlinde üç aylık uzatma ile sürenin toplamda altı ay olarak belirlendiğini, bununla birlikte örgüt faaliyeti çerçevesinde işlenen suçlarda birer aylık sürelerle müteaddit defalar bu tedbire başvurmaının mümkün olduğunu yani örgütlü suçlar bakımından bir üst süre sınırı bulunmadığını,

- Koşullara uyulmaksızın iletişimin denetlenmesi tedbirine başvurulması durumunda elde edilen verilerin delil olarak kullanılamayacağını, Anayasa Mahkemesi ve

Yargıtay kararlarında da koşullara uyulmaksızın gerçekleştirilen iletişimin denetlenmesi sonucu elde edilen verilerin delil olamayacağının kesin olarak hükme bağlandığını,

• Ülkemizin yasal düzenlemeler bakımından Avrupa insan hakları standartlarını karşıladığını, ancak uygulamadan kaynaklanan bazı eksikliklerin olduğunu,

ifade etmiştir.

Toplantının ikinci kısmında Telekomünikasyon İletişim Başkanlığı adına sunum yapan Telekomünikasyon İletişim Başkanlığı Başkan Vekili Osman Nihat ŞEN sunumunda özetle;

• Telekomünikasyon İletişim Başkanlığının; bağımsız, idari, özerk, telekomünikasyon sektörünü denetleyen ve düzenleyen bir üst kurul olan Bilgi Teknolojileri ve İletişim Kurumuna bağlı bir birim olduğunu,

• İletişimin denetlenmesiyle getirilen dört koruma tedbiri bulunduğunu; “iletişimin tespiti” tedbirinin kimin, kimi, hangi saatte, ne zaman ve nereden aradığı bilgisi, “iletişimin dinlenmesi ve kayda alınması” tedbirinin iletişimin gerçekleştirildiği araca göre değişmekte olan içerik, ses, SMS ve data bilgilerinin içeriği, “sinyal bilgilerinin değerlendirilmesi” tedbirinin iletişimin tespit edilmesi bilgilerinin topluca analizi ve değerlendirilmesi ve “mobil cihazın yerinin tespit edilmesi” tedbirinin bir cihazın, bir cep telefonunun nerede olduğu bilgisinin tespit edilmesi olduğunu,

• Telekomünikasyon İletişim Başkanlığı bünyesinde Emniyet Genel Müdürlüğü, Millî İstihbarat Teşkilatı ve Jandarma Genel Komutanlığı temsilcilerinin bulunduğunu ve bu temsilcilerin şeffaflık adına, TİB içerisinde yürütülen bütün süreci a’dan z’ye takip ettiklerini,

• İletişimin denetlenmesine ilişkin kurumlar, işletmeciler ve TİB arasındaki bütün işlemlerin, tüm kararların (sadece kararlardaki bilgiler), TİB’e ve TİB’den diğer kurumlara veya işletmecilere elektronik ortamda iletildiğini ve bütün işlemlerin kapalı, güvenli bir ağ üzerinden yapıldığını ve hem TİB, hem ilgili kurumlar hem de işletmeciler tarafında çok ciddi güvenlik önlemleri alındığını,

• TİB’in kurulmasından önce dinleme yapılırken ilgili görevlilerin hepsinin dinleme yapma yetkisi bulunduğu ancak TİB’in kurulması ile dinleme işlemini yapacak görevlinin, adli kolluk görevlisinin aidiyet numarasının bildirilmesi sisteminin getirildiğini ve böylelikle bir sesi, bir içeriği dinleyebilmek için mahkeme kararını alanın belirli olduğu

gibi o mahkeme kararının gereğini yerine getiren kişinin, dinleme yapan görevlinin de belirli olması şeklinde bir önlem getirildiğini,

- TİB içerisinde gerçekleştirilen bütün işlemlerde kompartımantasyon sistemi uygulandığını, sürecin bütün aşamalarının farklı kişilerce yerine getirildiğini ve böylelikle hiç kimsenin sürecin birden fazla aşamasına vakıf olmadığını,

- TİB tarafından iletişimin denetlenmesi tedbirine ilişkin kararların şekli incelemesinin yapıldığını ve bu incelemelerde; katalog suç sınırlamasına, soruşturma ve kovuşturma bilgilerine, süre sınırlamasına ve şüpheli kimlik bilgilerine bakıldığını, eksiklik bulunan kararlara itiraz edildiğini ve yedi buçuk yılda dinleme kapsamında 1.614 adet karara, dinleme dışı yani HTS, sinyal bilgileri veya iletişim tespitine benzer evraklarda da 23.401 adet karara itiraz ettiklerini,

- Bütün ses dosyalarının teknik olarak imzalandığını, bu imzalarda zaman, log, personel ve IP bilgisinin bulunduğunu ve imza sonrasında ses dosyalarının çok küçük çaplı bir değişiklik bile olsa kesinlikle değiştirilemeyeceğini,

- TİB’de her türlü fizikî güvenlik önleminin mevcut olduğunu ve bilişim, uygulama, veri tabanı, sistem ve personel güvenliğinin en üst düzeyde sağlandığını,

- İletişimin denetlenmesi tedbirinin uygulanmasına ilişkin olarak TİB öncesi dönemde son derece karmaşık ve dağınık bir yapı olduğunu ancak TİB’in kurulması ile oluşturulan yapının çok sade, denetlenebilir bir yapı olduğu ve bütün işlemlerin şeffaf ve denetlenebilir durumda olduğunu,

ifade etmiştir.

4- 21 Şubat 2013 Tarihli Toplantı

Komisyon, 4’üncü toplantısında Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı yetkililerini dinlemiştir.

Emniyet Genel Müdürlüğü adına sunum yapan Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkan Yardımcısı Gürsel AKTEPE sunumunda özetle;

- Emniyet İstihbarat Daire Başkanlığının önleme amaçlı dinleme yapabilmesi için kesinlikle mevzuatta izin verilen üç temel katalog suç olan terör, uyuşturucu imalatı ve ticareti ile cebir ve tehdit uygulayan çıkar amaçlı örgüt suçlarından birine bağlı olarak karar alınması gerektiğini,

- İletişimin denetlenmesi karar taleplerinde; kişinin kimliği, iletişim aracının türü, kullanıcı telefon numaraları, iletişim bağlantısının tespitine imkân veren, korunan, belirlenebilenler, tedbirin türü, kapsamı, süresi, tedbire başvurulmasını gerektiren nedenlerin neler olduğunun mutlaka bulunması gereken unsurlar olduğunu,

- İletişimin denetlenmesi tedbirine ilişkin olarak işlemin başladığı ve bitirildiği tarih ve saat, işlemi başlatan ve işlemi yapan personele ait bilgilerin tutulduğunu,

- Gecikmesinde sakınca bulunan hâllerde Emniyet Genel Müdürü veya İstihbarat Daire Başkanı'nın yazılı emriyle telekomünikasyon yoluyla yapılan iletişimin tespit edilebileceğini, dinlenebileceğini, sinyal bilgilerinin değerlendirilebileceğini ve kayda alınabileceğini ancak verilen yazılı emrin yirmi dört saat içerisinde mutlaka yetkili ve görevli hâkimin onayına sunulduğunu, yetkili hâkimin kırk sekiz saat içerisinde kararı ya onayladığını ya da reddettiğini, uygulamada iki yönde verilmiş kararların da olduğunu ve hâkim tarafından reddedilen kararlara ait ilk yirmi dört saat içerisinde elde edilen içeriklerin imha edildiğini,

- İletişimin denetlenmesi tedbirine yönelik kararların süresinin üç ay olduğunu ve mahkemeden uzatma kararı alınmaması durumunda tedbire ilişkin işlemlerin devam ettirilmesinin teknik olarak mümkün olmadığını,

- İletişimin denetlenmesi tedbirinin uygulanması sırasında soruşturmaya mesnet teşkil edecek bir sonuca ulaşıldıysa bunun adli birimlerle paylaşıldığını, ancak suça yönelik herhangi bir tespit söz konusu değilse, elde edilen bütün içeriklerin kanun gereği imha edildiğini,

- Terör örgütleri ile uyuşturucu imalatı ve ticareti yapan örgütlere yönelik önleme amaçlı iletişim denetlenmesi sonucu yapılan operasyonlar sonucunda elde edilen başarılar çok önemli olduğunu,

ifade etmiştir.

Toplantının ikinci kısmında Jandarma Genel Komutanlığı adına sunum yapan Jandarma Genel Komutanlığı Teknik İstihbarat Daire Başkanı Jandarma Kurmay Albay Fuat GÜNEY sunumunda özetle;

- Jandarma Genel Komutanlığının telekomünikasyon yoluyla iletişimin tespiti, dinlenmesi ve kayda alınması imkân ve kabiliyetinin mevcut olmadığını, iletişimin denetlenmesine yönelik bu faaliyetlerin yasal mevzuat esasları çerçevesinde

Telekomünikasyon İletişim Başkanlığı imkân ve kabiliyetleri kullanılmak suretiyle yürütüldüğünü,

- İletişimin denetlenmesine yönelik faaliyetlerin, adli ve önleyici maksatlı teknik takip faaliyetleri olmak üzere ikiye ayrıldığını,

- Adli teknik takip faaliyetlerine ilişkin olarak; adli teknik takip kararının alınabilmesi için bir suça ilişkin olarak bir soruşturma ve kovuşturma aşamasında suç işlendiğine dair kuvvetli şüphe ve başka suretle delil elde edilmemesi durumunun söz konusu olması gerektiğini, bu durumda kolluk olarak jandarmanın öncelikle hakkında tedbir uygulanacak şahsın abone kimlik bilgisini sistem üzerinde tespit ettiğini, şahsın daha önceki suç bilgilerini, jandarma sorumluluk sahasıyla ilişkisini ve bütün bilgileri içerecek şekilde teferruatlı bir araştırma tutanağı tanzim edildiğini, bu araştırma tutanağından maksadın hakkında tedbir uygulanacak şüpheli şahsın suçla irtibatının ortaya konulması ve başka suretle delil elde edilemeyecek durumun belirtilmesi için olduğunu, araştırma tutanaklarının karar talep formlarıyla birlikte ilgili cumhuriyet savcısına gönderildiğini, bütün bu faaliyetlerin her aşamasından ilgili Cumhuriyet savcısının bilgisi olduğunu ve Cumhuriyet savcısıyla müştereken yürütüldüğünü ve Cumhuriyet savcısının kolluğun bu çalışmalarını kendi iradesiyle yetkili mahkemenin onayına sunduğunu,

- Mahkeme kararını müteakip savcılık tarafından il jandarma komutanlığına iletilen kararların, güvenli hatlar üzerinden elektronik ortamda Teknik İstihbarat Daire Başkanlığına gönderildiğini, alınan bu kararların şekli bir incelemeye tabi tutulduğunu, şekli incelemeyi müteakip yine elektronik ortamda Telekomünikasyon İletişim Başkanlığına iletilildiğini, bu kararlar ilgili olarak TİB'in operatörlerden aldığı verileri, kararda belirtilen cihazlarla ve numaralarla ilgili olarak doğrudan aidiyeti belirlenmiş, kararlar birlikte TİB'e ulaştırılmış olan aidiyet numarasına doğrudan il jandarma komutanlığındaki dinleme odalarına gönderdiğini, yani iletişimin denetlenmesi faaliyetlerinin, Cumhuriyet savcılığınca yetkilendirilmiş aidiyet numaralı personel tarafından il jandarma komutanlıklarında tesis edilmiş teknik istihbarat odalarında Telekomünikasyon İletişim Başkanlığı tarafından gönderilen veriler üzerinden icra edildiğini ve yapılan bütün bu faaliyetlerin Cumhuriyet savcılarının gözetim ve denetiminde icra edildiğini,

- Teknik takibin sonlandırılmasının Cumhuriyet savcısının talimatı veya mahkemenin kararıyla olduğunu, bir suç tespiti söz konusuysa iletişimin dinlenmesi esnasında dinlemeye ilişkin tüm kayıtlar ve veriler cumhuriyet savcısına teslim edildiğini

ve yasa gereği on gün içerisinde Cumhuriyet savcısının denetiminde iletişimin içeriğine ilişkin kayıtlar imha edildiğini, bu işlemin bizzat Cumhuriyet savcılarının il jandarma komutanlıklarındaki dinleme odalarına gelmeleri suretiyle yapıldığını, suç tespiti olmadığı durumlarda yani kovuşturmayla yer olmadığına dair karar verilmesi durumunda da on gün içerisinde adli süreçle ilgili olan kayıtların dinleme odalarındaki bilgisayarlardan bizzat cumhuriyet savcılarının gözetiminde silindiğini,

- Önleyici teknik takip faaliyetlerine ilişkin olarak; Jandarma Genel Komutanlığının Jandarma Teşkilat Görev ve Yetkileri Kanunu’nun 7’nci maddesi kapsamında sadece kendi sorumluluk alanında önleyici dinlemeler yapmakta olduğunu, sürecin kolluk aşamasının, adli dinlemelerdeki süreçle paralel olduğunu,

- Karar taleplerinin yetkili ağır ceza mahkemelerine doğrudan il jandarma komutanlıkları tarafından gönderildiğini,

- Adli süreçte Cumhuriyet savcılarının kontrolünde yapılan işlemlerin, önleyici teknik takip faaliyetlerinde yetkili komutanlıkların denetiminde icra edildiğini, tüm işlem kayıtlarının sistem üzerinde muhafaza edildiğini,

- İletişimin denetlenmesi kapsamında TİB’den elektronik ortamda gönderilen verilerin incelenmesinin güvenli odalarda yapıldığı, bu odaların fiziki güvenliğinin sağlandığını, giriş çıkışların yetkili personelle sınırlı olduğunu,

- Jandarma Genel Komutanlığının sorumluluk alanındaki tüm faaliyetlerini mevzuat çerçevesinde insan odaklı, açık, şeffaf ve hesap verebilir bir anlayışla ve insan haklarına saygılı bir şekilde yürütme gayretini sürdürdüğünü,

ifade etmiştir.

5- 27 Şubat 2013 Tarihli Toplantı

Komisyon, 5’inci toplantısında Milli İstihbarat Teşkilatı yetkililerini dinlemiştir. Yetkililer tarafından yapılan sunumda özetle;

- Türkiye Cumhuriyeti’nin güvenlik ve dış politikası doğrultusunda iç ve dış unsurlara ait haberleşmelerin elde edilmesi, haberleşme amaçlı olmayan elektronik sinyallerin izlenmesi, istihbarata karşı konulması ve stratejik istihbaratın oluşturulmasının MİT’in temel ve yegâne görevleri olduğu ve bu görevlerini yerine getirirken insan unsuru yanında elektronik ve teknik her türlü cihaz ve teknik imkânlardan faydalandıkları,

• MİT'in sadece istihbari amaçlı dinleme yaptığı, ancak Ceza Muhakemesi Kanunu'nda ve Ceza Kanunu'ndaki düzenlemeler kapsamında devlet sırrının ifşası ve casusluk suçlarında genel zabıtaya yani polis teşkilatına ve jandarma teşkilatına tanınan hak ve yetkilere sahip olunması nedeniyle, Cumhuriyet savcılarının hazırlık soruşturması usul ve esaslarına tabi şekilde bu iki suç kapsamında adli dinleme yapma yetkisine sahip olduğu,

• Hedeflere yönelik olarak sabit telefon, cep telefonu, uydu telefonu görüşmeleri ve çeşitli ortamlarda yapılan internet haberleşmelerinin TİB üzerinden geldiği ve bu veriler üzerinden izleme ve dinleme faaliyetlerinin gerçekleştirildiği,

• Genelkurmay Elektronik Sistemler Başkanlığının 1 Ocak 2012 tarihi itibarıyla Millî İstihbarat Teşkilatına devredildiği ve Başkanlık faaliyetlerinin muhabere istihbaratı ve elektronik istihbarat olmak üzere iki ana konuda yoğunlaştığı,

• Yapılan çalışmaların espionaj, kontrespionaj ve terörle mücadele kapsamında yoğunlaştığı,

• Bilgilerin gelişen teknoloji ile birlikte herkes tarafından erişilir olmaya başlamasının güvenlik gereksinimi artırması sonucunda hemen hemen her verinin kriptolanmaya başlandığı ve bu yüzden kripto analiz konusunun çok önemli olduğu ve ülkemizin devlet güvenliği açısından bu alanda yatırımlarını hızlandırması gerektiği,

• Yasa dışı dinlemelerde iki tane temel konu bulunduğu; birincisinin, uzaktan erişilebilen sistemler ve cihazlar olduğu yani bir cihazın içerisindeki bilgiye erişmek için cihazla fiziksel olarak aynı ortamda bulunma zorunluluğunun bulunmadığı, bir cihaz eğer bir şekilde bir ağla, genel bir ağla herhangi bir yere bağlıysa o cihaza erişmenin birçok yöntemi olduğu, ikincisinin ise fiziksel erişim olduğu yani bir cihaz üzerinde işlem yaparak yasa dışı dinleme ve izleme yapıldığı,

• Dinleme ve izleme faaliyetleri hangi kanun dışı yöntemlerle yapılabilir diye sorulması durumunda günümüzün teknolojisinin geldiği noktada bu işlemlerin aslında çok rahat yapılabildiği, kullanmış olduğumuz çok ileri teknoloji cihazların hayatımızın her alanına girmesi ve bu tür cihazların ne tür zafiyetleri olabileceğinin, ne tür sorunlar yaratabileceğinin bilinmemesinin yasa dışı dinleme ve izleme faaliyetlerinin yapılabilmesini kolaylaştırdığı,

• Haberleşmenin gizliliği, özel hayatın mahremiyeti ve haberleşme özgürlüğünü tehdit eden unsurların neler olabileceğinin MİT tarafından yakından takip edildiği ve ülkemize yönelebilecek bu tür tehditler karşısında, bu tür tehditlerin kimler tarafından

geliştirildiğine ve yönlendirildiğine bakılmasında fayda olduğu, eskiden istihbarat çalışmaları ve teknolojilerinin devletler tarafından üretildiği ve yönlendirildiği ancak dünyada artık devletlerin yanı sıra çok uluslu şirketlerin, çeşitli sivil toplum örgütlerinin ve çeşitli uluslararası organizasyonların da sermayenin küreselleşmesiyle beraber istihbarat ve bilgi toplama faaliyetleri geliştirdiği ve yürüttüğü,

- Başta ulaştırma konusunda faaliyet gösteren kamu kurumlarımız ve özel şirketlerimiz olmak üzere, çeşitli kamu kurum, kuruluşlarımızda ve önemli devlet projeleri yürüten özel sektör firmalarında uluslararası devlet dışı aktörlerden kaynaklanabilecek birtakım risklerin tespiti ve önlenmesi amacıyla 101 istihbarata karşı koyma ve koruyucu güvenlik brifingi, gerçekleştirildiği ve bu brifinglere, 7.400 civarında “kritik personel” olarak adlandırılan yönetici ve proje sorumlusu düzeyinde uzman personelin katıldığı,

- Yasa dışı dinleme ve izlemeyi engelleyebilmenin gelişen teknoloji karşısında ancak insanların farkındalığının artırılmasına bağlı olduğu,

ifade edilmiştir.

6- 28 Şubat 2013 Tarihli Toplantı

Komisyon 6’ncı toplantısında Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsünü (TÜBİTAK-UEKAE) dinlemiştir.

TÜBİTAK-UEKAE Müdür Yardımcısı Dr. Uğur SARAÇ “*teknik takip ve karşı tedbirler konulu*” sunumunda özetle;

- Dinleme ve izleme cihazlarının (böcekler) teknolojiyle oldukça ileri noktalara geldiğini, hiç fark edilemeyecek, ancak mercekle, elektroskoplarla tespit edilebilecek boyutlara ulaşmış cihazlar yapılabildiğini,

- Böceklerin kapalı devre çalışan ve açık devre çalışan olmak üzere ikiye ayrıldığını; kapalı devre böceklerin üzerine yerleştirilen mikrofon ve kameralar marifetiyle depoladıkları bilgileri kablosuz bir şebeke üzerinden uzaklara iletme gibi bir fonksiyonları olmadığını, bu tip sistemlerin herhangi bir verici içermedikleri için RF tarama cihazlarıyla tespit edilmesinin biraz daha zor olduğunu; daha sık rastlanan açık devre böceklerin ise üzerlerinde kablosuz bir verici bulunduğunu ve bunların ortamda tespit ettikleri sesleri ve

görüntüleri optik üzerinden, ultrasonik ses dalgaları üzerinden, RF dalgaları üzerinden veya hibrit şekilde ileten sistemler olduğunu,

- Açık devre böcek türlerinden olan optik böceklerin ortamdaki sesi veya görüntüyü alarak ışığa çevirdiklerini ve bunu ışık üzerinden modülasyonlu bir şekilde uzağa ilettiklerini,

- Ultrasonik böceklerin aldıkları sesi veya görüntüyü ses dalgasına çevirerek uzağa ilettiklerini,

- En çok kullanılan açık devre böcek türlerinden olan RF böceklerin topladıkları bilgiyi RF sinyale çevirerek ve belli bir haberleşme protokolüne göre verici kısımlarını kullanarak uzak yerlere gönderebildiklerini,

- Çok rastlanan bir böcek türü olan GSM böceklerin, cep telefonu kullanımının yaygınlaştığı günümüzde tespitinin oldukça zor olduğunu,

- Benzer şekilde ortamdaki enerji yoğunluğuna bakılarak tespiti güç olan diğer bir böcek türünün de Wi-Fi böcekler olduğunu, bunları tespit edebilmek için protokolün içine girip oradan aktarılan işaretlerin tespit edilmesi gerektiğini,

- Sinyal hatları üzerinden yapılan izlemelerin yetkili kurumlar tarafından yapılan yasal izlemeleri içerebileceğini, bunun telefon ve internet hatları üzerine yapılan tablarla da gerçekleştirileceğini,

- Fiber optik sistemin hem dinlemeye karşı hem de RF yayınlara karşı ciddi bir avantajı olduğunu,

- Ulusal imkânlarla yurt içinde kontrollü şartlarda üretilmiş sistemlerin daha güvenli olduğunu ve özellikle telefon santrallerinin milli sistemlere sahip olması gerektiğini, TÜBİTAK ve başka bazı kurumların bu konuda çalışmalarının bulunduğunu,

- Böceklerle karşı alınacak önlemler arasında inşaat aşamasındaki önlemlerin, jammer ve özel cam filmi kullanımının, binalara güvenli giriş-çıkış sağlanmasının, kriptolu telefon kullanımının yaygınlaştırılmasının bulunduğunu,

ifade etmiştir.

7- 6 Mart 2013 Tarihli Toplantı

Komisyon 7'nci toplantısında Gazi Üniversitesi Mühendislik Fakültesini dinlemiştir.

Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü öğretim üyesi ve Fen Bilimleri Enstitüsü Müdürü Prof. Dr. Şeref SAĞIROĞLU “*haberleşme ve özel hayatı ihlal edebilecek teknolojiler*” konulu sunumunda özetle;

- İşlenmiş veriye bilgi; katma değeri olan, farklı değer ifade eden, deneyimi gösteren, deneyimi sunan, birikimi ifade eden varlıklara öz bilgi denildiğini,
- Elektronik ortamda bilgi güvenliğinin sağlanmasının gizlilik, kimlik doğrulama, inkâr edilememe ve şifreleme gibi unsurları ihtiva etmesi gerektiğini,
- Teknoloji çağında salt bilginin değil, güvenliği sağlanmış bilginin bir güç olduğunu, matematiksel bir anlatımla binde 1 korunmasızlığın yüzde 100 güvensizlik demek olduğunu,
- Saldırganların ihtiyaç duydukları araçları internetten çok kısa sürede elde edilebildiğini, saldırılacak sistemin açıklarını kolaylıkla tespit edebildiklerini ve kişilere, kurumlara yönelik dolaylı saldırıların yaygınlaştığını,
- Yapılan saldırıların yüzde 70’inin insanların geliştirdiği yazılımlardan kaynaklandığını, ticari içerikli web sayfalarının yüzde 75’inin korunmasız olduğunu, web uygulama yazılımcılarının yüzde 60’ının güvenli yazılım geliştirme tekniklerini bilmediğini,
- Saldırgan tarafların kendilerini her geçen gün geliştirerek aralarındaki işbirliğini arttırdığını, savunan tarafların ise eğitim ve yatırım eksikliği, yüksek korunma maliyetleri gibi nedenlerle yeterince önlem alamadığını,
- Akıllı cep telefonlarına yönelik sadece 2011’de 100 bin yeni virüs ve casus yazılım çıktığını, bunların da pek çoğunun çözümünün olmadığını. 2012’de bu sayıların düşmesi beklenirken yaygınlaşan teknoloji kullanımı nedeniyle giderek arttığını,
- Casus yazılımların kendilerini saklayabildiklerini, silinseler de kendilerini tekrar kopyalayabildiklerini, çeşitli yerlere e-mail ve sms gönderebildiklerini, bu yazılımları taşınabilir bellekler vasıtasıyla yaygınlaştırmanın sık rastlanan ve maliyeti düşük bir yöntem olduğunu,
- Arama motorları üzerinden çok geniş bir açık veri tabanına ulaşılabilirdiği gibi kişi ve kurumların bazı özel bilgilerine de ulaşılabilirdiğini,
- Teknoloji konusunda dışa bağımlılığın azaltılmasının bilgi güvenliğinin sağlanması hususunda atılması gereken en önemli adımlardan biri olduğunu,
- İhtiyaç duyulan işe göre işletim sistemi kullanımının, başka bir ifadeyle kısıtlı kullanım sunan işletim sistemlerinin tercih edilmesinin bilgi güvenliğini arttıracığını,

- Türkiye’de, casus yazılımlar ve bankacılık sistemiyle ilgili olarak çalışmalar yaptıklarını ve bankacılık sisteminin eskiye nazaran çok daha güvenli hale getirildiğini,
 - Bilgi güvenliğinin artırılması doğrultusunda sivil toplum kuruluşları, kamu kuruluşları, üniversite ve özel sektörün birlikte çalışması ve çözümler üretmesi gerektiğini,
- ifade etmiştir.

8- 7 Mart 2013 Tarihli Toplantı

Komisyon 8’inci toplantısında Türkiye Barolar Birliği ve İstanbul Üniversitesi Siyasal Bilgiler Fakültesi öğretim üyesi Prof. Dr. Ersan ŞEN’i dinlemiştir.

Türkiye Barolar Birliği Başkan Yardımcısı Av. Talay ŞENOL haberleşme özgürlüğüne ve özel hayatın gizliliğine yönelik ihlaller ve bu ihlallerin önlenmesiyle ilgili tedbirler hakkındaki sunumunda özetle;

- Türk hukukunda iletişimin denetlenmesine ilişkin en önemli yasal düzenlemenin CMK’da "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi" başlığı altında 135 ve devamı maddelerinde yer aldığını,
- Türk hukuk sisteminde, suç öncesi önleyici tedbir ve adli tedbir olmak üzere iletişimin denetlenmesin ikiye ayrıldığını; adli amaçlı iletişimin denetlenmesinin CMK’da, önleme amaçlı iletişimin denetlenmesinin ise 5397 sayılı Kanun hükümlerine göre yapılabilirdiğini,
- Türkiye’de iletişimin denetlenmesine adli ve idari anlamda olanak sağlayan sayılan kanunların Avrupa İnsan Hakları Mahkemesinin kararlarıyla örtüştüğü yönleri yaygın olsa da, bazı konularda mahkeme kararları ile uyumsuzlukların bulunduğunu, bu uyumsuzlukların bir kısmının yasal düzenlemelerin içeriğinden bir kısmının ise uygulamadan kaynaklandığını;
- 5397 sayılı Kanunda, iletişimin denetim altına alınması tedbirine başvurulabilmesi için CMK’dakinin aksine basit bir suç işleme şüphesinin bulunmasını yeterli olduğunu, kanunun bu denetim tedbirine başvurulması için şart koştuğu şüphede hiçbir yoğunluk, kesinlik veya derece belirtmemiş olmasının CMK’ya aykırı uygulamalara sebebiyet verebileceği ve bu nedenle, bu kanundaki düzenlemenin CMK düzenlemesine paralel hâle getirilmesi gerektiğini,

• CMK'nın 135'inci maddesindeki iletişimin denetlenmesi tedbirini son çare olarak görme anlayışının 5397 sayılı Kanunda öngörülmemiş olduğunu ve uygulamada bu tedbirlerin ultima ratio, yani son çare olarak uygulanması gereğinin dikkate alınmadığını,

• 5397 sayılı Kanunda önleyici amaçlı iletişimin denetlenmesi tedbirinin uygulanacağı kişi ya da kişilerden, sanık veya şüphelilerden bahsedilmediğini, ancak kanunun lafzından kanunda belirtilen suçları işleme ihtimali olan tüm bireylerin iletişimlerinin denetlenmesine izin verildiğinin çıkarılabileceğini, bu açıdan bakıldığında tedbirin uygulanabileceği kişilerin kapsamının oldukça geniş tutulduğunu,

• Adli amaçlı iletişimin denetlenmesinde sanık veya şüphelinin müdafii veya tanıklıktan çekilme hakkına sahip kişilerle iletişimi denetlenemezken, önleme amaçlı denetlemede bu yönde herhangi bir istisna öngörülmediğini,

• İletişimin adli amaçlı denetim altına alınmasını sağlayan yasal mevzuatta, iletişimin denetlenmesi sonucu elde edilen kayıt ve bulguların haberleşme özgürlüğü sınırlandırılan kişi veya kişilere bildirilmesi hususu düzenlemişken, önleme amaçlı iletişimin denetlenmesinde elde edilen verilerin ilgisine bildirilmesi hususunun bu denetime olanak sağlayan yasal mevzuatta öngörülmediğini,

• Haberleşme özgürlüğü hukuka aykırı olarak sınırlandırılan ve bundan bilgilendirilen kişilerin tazminat talep etme haklarının adli amaçlı iletişimin denetlenmesine olanak tanıyan yasal düzenlemelerde öngörüldüğünü, ancak aynı durumun, önleme amaçlı denetim için mümkün olduğunun söylenemeyeceğini,

• Türk Ceza Kanununun 132'nci maddesinin üçüncü fıkrasına, 6352 sayılı "Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun'un 79'uncu maddesi ile "hukuka aykırı olarak" ibaresi eklendiğini ancak bu ibare ile özel hayatın korunması ve haberleşme özgürlüğünün özüne bazı subjektif gerekçelerle müdahale etme olanağı doğabileceğini,

• Avrupa Birliği Komisyonu tarafından hazırlanan "Genişleme Stratejisi ve Başlıca Zorluklar 2012-2013" bildiriminde yer alan; Türkiye'nin özel hayata ve aile hayatına saygı ve kişisel verilerin korunmasına ilişkin ulusal mevzuatını, verilerin korunmasına ilişkin Avrupa Birliği müktesebatı ile uyumlu hâle getirmesi ve bu bağlamda tam bağımsız bir veri koruma ve denetleme birimi kurulması, Kişisel Verilerin Otomatik İşlemden Geçirilme Sürecinde Bireylerin Korunması Hakkında Avrupa Konseyi Sözleşmesinin ve

bu sözleşmenin Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Ek Protokolünün onaylaması gerektiği yönündeki tespitlerine aynen katıldıklarını,

- Adli amaçlı iletişimin denetlenmesinde avukatlar için getirilen istisnanın araç ve cep telefonlarını kapsamamasının bir eksiklik olduğunu,
- Avukatlık bürolarının savcı değil, hâkim nezaretinde aranması düzenine geçilmesi gerektiğini,

ifade etmiştir.

Toplantının ikinci kısmında sunum yapan İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Öğretim Üyesi Prof. Dr. Ersan ŞEN sunumunda özetle;

- Türkiye’de -bütün dünyada olduğu gibi- hukuka aykırı delillerin kullanılıp kullanılmamasından ziyade, istihbaratın gayrihukuki kullanımının daha tehlikeli sonuçlar ortaya çıkarabileceğini,
- Mevcut Anayasa’nın özel hayatla ilgili hükümlerinin, adli amaçla iletişimin denetlenmesine ilişkin kanuni düzenlemelerin tatminkâr olduğunu, sorunların hükümlerin uygulanmasından doğduğunu,
- İletişimin dinlenmesi kararlarının alınıp uygulanmasında hâkim-savcı açısından ve adli kolluk teşkilatının bulunmayışından kaynaklanan sorunların bulunduğunu,
- Yargıtayın içtihadı doğrultusunda yalnızca telefon dinlemeleri delil olarak kullanılarak mahkûmiyet kararı verilmemesi, somut delillerin elde edilmeye çalışılması gerektiğini,
- Gelişen iletişim teknolojilerinin nimetleri kadar külfetlerinin de olduğunu, ülkemizde birçok insanın dinlenme ve takip edilme endişesi taşıdığını,
- Ülkedeki tüm bireyleri ilgilendiren ceza ve ceza muhakemesi kanunlarında tek seferde kapsamlı değişiklikler yapılmasının kanun tekniği bakımından hatalı olduğunu,
- Önleme amaçlı dinlemeyi düzenleyen hükümlerde yetki unsurunun yeterince açık olmadığını,
- Yargıtayın bir kararında hangi suçtan dinleme yapılıyorsa, elde edilen kayıtların sadece o suç için delil teşkil edebileceğinin ifade edildiğini,
- Örgütlü suçlarla ilgili düzenlemelerin eksik olduğunu, sadece Türk Ceza Kanununun 220. maddesinde bazı tanımlamalara yer verildiğini,

ifade etmiştir.

9- 20 Mart 2013 Tarihli Toplantı

Komisyon 9’uncu toplantısında Bilgi Teknolojileri ve İletişim Kurumunu (BTK) dinlemiştir. Toplantıya Teknik Düzenlemeler Daire Başkanı Atilla ARSLAN, Tüketici Hakları Daire Başkanı Özgür Fatih AKPINAR, Spektrum İzleme Daire Başkanı Necati UĞURLU ve Hukuk Müşaviri Atilla ÖZTÜRK katılmıştır.

Bilgi Teknolojileri ve İletişim Kurumu adına ilk sunumu yapan Hukuk Müşaviri Atilla ÖZTÜRK sunumunda özetle;

- Bilgi Teknolojileri ve İletişim Kurumunun, Telekomünikasyon Kurumu adıyla 2000 yılında 4502 sayılı Kanun ile kurulduğunu, kurumun görevinin telekomünikasyon alanında piyasada yetkilendirme yapmak, spektrumu düzenlemek, tüketici haklarını korumak ve denetim yapmak olduğunu,

- Hâlihazırda dört tanesi imtiyaz olmak üzere 688 adet yetkilendirme yapıldığını, 433 şirketin elektronik haberleşme alanında muhtelif konularda yetkilendirildiğini, imtiyaz verilen dört şirketten üç tanesinin mobil haberleşme konusunda 2G ve 3G denilen imtiyaz sözleşmeleriyle yetkilendirildiğini, Türk Telekom’a ise sabit telefon konusunda imtiyaz yetkisi verildiğini, diğer şirketlerin bildirim ve kullanım hakkı kapsamında İnternet servis sağlayıcılığı, alt yapı işletmeciliği gibi değişik alanlarda yetkilendirilerek faaliyetlerini yürüttüklerini,

- Kurumun belli bir büyüklüğe ulaşan şirketlerin tarifelerini belirleme yetkisi bulunduğunu,

- Piyasaya yeni giren şirketler ile diğer şirketler ara bağlantı sözleşmeleri konusunda anlaşamazlarsa, taraflardan birinin kuruma müracaatı sonucu uzlaştırma prosedürünün işletildiğini ve böylece telekomünikasyon hizmetinin kesintisiz ve mevzuata uygun verilmesinin sağlandığını,

- Kurumun spektrum yönetimi ve denetimi ile teknik düzenleme konusunda da görevleri bulunduğunu,

- Türkiye’ye yasal yollardan girmesi mümkün olan telekomünikasyon cihazlarının piyasadaki standartlara uygun bir şekilde işletilip işletilmediğinin, piyasadaki cihazların mevcut standartlara uygun olup olmadığının denetlenmesinin de kurumun görevleri arasında yer aldığını,

- Telekomünikasyon yoluyla yapılan iletişimin tespiti ve dinlenmesi konusunda da TİB Başkanlığı marifetiyle görevleri bulunduğunu,

- Kurum faaliyetlerinin Devlet Denetleme Kurumu ve Sayıştay tarafından denetlendiğini,

ifade etmiştir.

Bilgi Teknolojileri ve İletişim Kurumu adına ikinci olarak sunum yapan Spektrum İzleme Dairesi Başkanı Necati UĞURLU sunumunda özetle;

- Elektromanyetik dalgaların enerjilerine ve dalga boylarına göre sıralı bir dizin ya da frekans aralığı oluşturulmasına spektrum denildiğini,

- Spektrum İzleme Dairesinin görevleri arasında frekans aralığı içerisinde tahsis edilen frekansların usulüne uygun olarak yapılıp yapılmadığının denetlenmesi ve ilerleyen süreçte oluşabilecek enterferansın tespitine yönelik işlemlerin gerçekleştirilmesinin bulunduğunu,

- 20 MHz ile 2.5 GHz frekans aralığındaki frekansların enterferansa neden olup olmadığı yolundaki denetimin ASELSAN tarafından üretilmiş olan Millî Monitör Sisteminin ekipmanlarıyla gerçekleştirildiğini,

- AM/FM ve tek analog yayınlar dışında sayısal yayınlara ilişkin hiçbir teknik dinleme yapma imkân ve kabiliyetlerinin bulunmadığını,

ifade etmiştir.

Bilgi Teknolojileri ve İletişim Kurumu adına son olarak sunum yapan Tüketici Hakları Dairesi Başkanı Özgür Fatih AKPINAR sunumunda özetle;

- BTK tarafından 2009 yılında alınan karar uyarınca, bir kişinin GSM bayisinden bir ay içerisinde en fazla dört (yabancılar için üç), toplamda ise en fazla on beş ön ödemeli hat alabileceğini,

- Faturalı hatlarda MERNİS kapsamında kişilerin adres bilgilerinin temin edildiğini,

- 5809 sayılı Kanunun yürürlüğe girmesiyle birlikte BTK tarafından tüm GSM operatörlerinin abone merkezlerinde yapılan çalışma sonucunda her bir abonenin isminin karşısına TC kimlik numarası girilmesi yükümlülüğünün getirildiğini,

- 2013 yılı itibarıyla, kişilerin elektronik ortamda TC kimlik numaralarını girerek ve güvenlik önlemlerinden geçerek üzerlerine kayıtlı olan hatları BTK web sitesinden öğrenebildiğini,

ifade etmiştir.

10- 21 Mart 2013 Tarihli Toplantı

Komisyon 10'uncu toplantısında Türk Telekomünikasyon Anonim Şirketi ile Türksat Uydu Haberleşme Kablo TV ve İşletme Anonim Şirketini dinlemiştir. Toplantıda TÜRK TELEKOM adına Operasyon Başkanı Mehmet ATALAY ve TÜRKSAT adına ise Genel Müdür Yardımcısı Cemil SAĞIROĞLU sunum yapmışlardır.

TÜRK TELEKOM Operasyon Başkanı Mehmet ATALAY sunumunda özetle;

- Telekomünikasyon İletişim Başkanlığı (TİB) ve TÜRK TELEKOM sistemleri arasında teknik olarak bağlantı bulunduğunu, dinleme taleplerinin TİB sistemleri üzerinden kendilerinin göremeyeceği şekilde santrallerine ulaştığını, yapılan teknik sorgulama neticesinde elde edilen datanın aynı şekilde TİB'e aktarıldığını,

- TÜRK TELEKOM'un sermayesinin yüzde 30'unun Hazineye, yüzde 55'inin Ojer Telekom'a ait olduğunu, yüzde 15'inin ise İstanbul Menkul Kıymetler Borsasında işlem görmekte olduğunu,

- Bilgi Teknolojileri ve İletişim Kurumunun elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğin korunması hakkında yayımladığı yönetmelik ile işletmecilere bazı yükümlülükler getirildiğini ve bu doğrultuda veri tabanlarının tutulması, bunlara ilişkin işlemlerin kişilerin rızaları alınarak yapılması, verilerin saklanması ve altyapıya uyarlanması ile ilgili teknik çalışmaların tamamlandığını,

- TÜRK TELEKOM'un; ALCATEL, NSN, Ericsson ve Huawei gibi şirketlerden çok sıkı şartnameler çerçevesinde santral temin ettiğini, bu santrallerin üretimine, sistemin altyapısına ve yazılımına ilişkin haklarının mevcut olduğunu, santrallere uzaktan veya merkezinden yapılabilecek her türlü müdahalenin kontrolleri altında olduğunu, santrallere internet üzerinden erişimin mümkün olmadığını, yetkili personelin belli prosedürler çerçevesinde faaliyette bulunduğunu, yabancı uzman çalıştırılması gereken hallerde BTK dâhil ilgili tüm mercilerden izin alındığını ve yapılacak çalışmaların TÜRK TELEKOM personeli nezaretinde gerçekleştirildiğini, bunun dışındaki bütün işlemlerin TÜRK TELEKOM personeli marifetiyle yapıldığını,

- Fiber teknoloji sayesinde 2017 yılına kadar Türkiye'nin bütün şehirlerinde, 100 megabite yakın erişim altyapısı kurmayı hedeflediklerini, böylece kullanıcı mahallinde dış müdahaleden kaynaklanabilecek olası sorunların büyük ölçüde önüne geçilebileceğini,

- Binden fazla AR-GE mühendisi ile Türkiye’de AR-GE ve eğitim konusunda en fazla yatırım yapan şirketlerden biri olduklarını,
- BTK’nın koordinasyonunda siber saldırılara yönelik tatbikatlar yaptıklarını, TÜRK TELEKOM ve TÜRK TELEKOM’dan hizmet alan kamu kuruluşlarının bu tatbikatların hiçbirinde zafiyet yaşamadığını,

ifade etmiştir.

TÜRKSAT Uydu Haberleşme Kablo TV ve İşletme Anonim Şirketi adına sunum yapan Genel Müdür Yardımcısı Cemil SAĞIROĞLU sunumunda özetle;

- 16 Haziran 2004 tarih ve 5189 sayılı Kanun ile kurulan TÜRKSAT’ın, sermayesinin tamamı Hazineye ait olup Ulaştırma, Denizcilik ve Haberleşme Bakanlığının ilişkili kuruluşu olarak faaliyette bulunduğunu,
- Verilen temel hizmetler arasında uyduların kontrolü ve işletilmesinin, televizyon ve radyo yayınları ile uydu haberleşme sistemlerinin bulunduğunu,
- Uydu haberleşmesinin veri istasyonundan gönderilen sinyalin uyduda alınıp güçlendirilerek kapsama alanının tamamına yayınlanması ve buradaki alışı sistemleri tarafından alınması şeklinde gerçekleştiğini, uydunun temel görevinin, gelen sinyali ve içerdği veriyi değiştirmeden aynen yansıtmak ve iletmek olduğunu,
- 1994 ve 1996’da fırlatılan 1B ve 1C uydularının 2006 ve 2010’da ömürlerini tamamladıklarını, 2A ve 3A uydularının şu an yörüngelerinde hizmet vermeye devam ettiklerini, TÜRKSAT 4A uydusunun 2013 yılının 4’üncü çeyreğinde ve 4B uydusunun 2014’ün ilk çeyreğinde fırlatılmasının planlandığını,
- Uydularla ilgili tüm kontrol ve gözlem faaliyetlerinin gölbaşı merkez kampüsünde yürütüldüğünü, Ankara’nın iki farklı noktasında ana ve yedek yer kontrol istasyonları, yedeklenebilir antenler, elektronik düzenler, veri işletim sistemleri ve diğer altyapı donanımları bulunduğunu ve bu sayede ile uyduların kesintisiz ve güvenli bir şekilde yörüngelerinde kalmalarının sağlandığını,
- Millî Eğitim Bakanlığı İnternet Okul Projesi bünyesinde 2006 yılından itibaren 4.198 köy okuluna geniş bant uydu erişim teknolojiyle İnternet alt yapısı sağlandığını, Acil Durum Haberleşmesi Projesi kapsamında toplam 31 adet sabit ve mobil terminal üzerinden Kızılay’ın acil durum haberleşme ihtiyaçlarının karşılandığını, Pakistan ve Somali’de uydu üzerinden haberleşme hizmeti verildiğini, 100 adet deprem istasyonundan alınan deprem

sinyallerinin uydu üzerinden Afet ve Acil Durum Yönetimi Başkanlığının Ankara merkezine iletiildiğini,

- Ticari gizlilik arz eden veri iletimi uygulamalarında, kullanıcıların yer terminallerinde şifreleme sistemi kullandıklarını, millî askerî uydu haberleşmesinde askerî haberleşmeye özgü frekans bantlarının kullanıldığını, TÜRK SAT AŞ' nin buradaki rolünün uydu kapasitesi sağlamak ve gelen sinyallerin içeriğini değıştirmeden, güçlendirerek iletmekten ibaret olduğunu,

ifade etmiştir.

11- 27 Mart 2013 Tarihli Toplantı

Komisyonun 11'inci toplantısında araştırma konusunun hukuki ve teknik yönlerinin ayrıntılarıyla incelenebilmesi amacıyla, biri Hukuk Alt Komisyonu diğeri Teknik Alt Komisyon olmak üzere iki alt komisyon kurulmasına karar verilmiş ve kurulması kararlaştırılan bu alt komisyonlara üye seçimi yapılmıştır.

12- 2 Mayıs 2013 Tarihli Toplantı

Komisyonun 12'nci toplantısında Alt Komisyonlarca gerçekleştirilen çalışmalar değerlendirilmiş ve İttüzüğün 105'inci maddesine göre çalışma süresinin ek süre alınarak uzatılması yönünde karar alınmıştır.

13- 29 Mayıs 2013 Tarihli Toplantı

Komisyon 13'üncü toplantısında Başkanlık Divanı seçimi gündemiyle toplanmıştır. Yapılan seçimde Tokat Milletvekili Zeyid ASLAN'ın istifası nedeniyle boşalan Komisyon Başkanlığına Yozgat Milletvekili Yusuf BAŞER, Komisyon Başkanvekilliğine İzmir Milletvekili Hamza DAĞ seçilmişlerdir.

HUKUK ALT KOMİSYONU TOPLANTI TUTANAK ÖZETLERİ

1- 27 Mart 2013 Tarihli Hukuk Alt Komisyonu Toplantısı

Hukuk Alt Komisyonu ilk toplantısında Alt Komisyon Başkan seçimi yapılmış ve Elazığ Milletvekili Şuay ALPAY Hukuk Alt Komisyonu Başkanı seçilmiştir.

2- 28 Mart 2013 Tarihli Hukuk Alt Komisyonu Toplantısı

Alt Komisyon çalışma takvimi, çalışma usul ve esasları ile Alt Komisyona davet edilecek kişi, kurum ve kuruluşlar belirlenmiştir.

3- 2 Nisan 2013 Tarihli Hukuk Alt Komisyonu Toplantısı

Alt Komisyon üçüncü toplantısında Milliyet, Sabah ve Zaman gazeteleri yetkililerini dinlemiştir.

Milliyet Gazetesi adına sunum yapan Ankara Temsilcisi Fikret BİLA sunumunda özetle;

- Haberleşme özgürlüğünün engellenmesi konusunun Türkiye’de bir süredir gündemde olan bir konu olduğunu ve toplumda telefonların dinlenmesi konusunda, özellikle, yaygın bir endişe olduğunu ve toplumda oluşan bu duyarlılığın, bu endişenin Türkiye Büyük Millet Meclisi tarafından bir araştırma komisyonu marifetiyle incelenmesinin yararlı olacağını,

- Teknolojideki değişim hızının çok yüksek olması nedeniyle hukukun zaman zaman teknolojinin gerisinde kalmasından kaynaklı sorunlar yaşandığını, ancak son dönemlerde özellikle Avrupa Birliği Hukuku’na uyum anlamında çıkarılan yasalarla bu sorunların büyük ölçüde giderildiği kanaatinde olduğunu,

- Ülkemizde yaşanan problemin, hukuki çerçeve belirli olmasına rağmen büyük ölçüde uygulamadan kaynaklandığını,

- Ülke gündeminde önemli yer teşkil eden çok büyük davalarda özellikle, birtakım telefon dinleme kayıtlarının basına yansıdığının bilindiğini, dinlenen kişinin özel hayatının kamuoyuna yansımalarının Anayasa güvencesi altında olan kişi hak ve özgürlüklerine, özel hayatın gizliliğine aykırı bir durum olmasının yanı sıra bu kayıtların toplum nezdinde bir itibarsızlaştırma aracı olarak kullanıldığını,

- Dinleme ve izleme kayıtlarının basına yansımalarının kolluk güçleri ve yargı mekanizmasının yasayla yükümlü olmasına rağmen bu çalışmaları gerekli gizlilikte yapmadığını ortaya koyduğunu,

- Sorunun uygulamadan kaynaklandığını düşündüğünü ve bunun önlenmesinin de ancak idari denetimle ve yargı denetimiyle olması gerektiğini,

- Yasa dışı yollarla elde edilmiş izleme veya dinleme kayıtlarını internet ortamına koyan kişilerin bulunamaması ve yargı önüne çıkarılmamasının önemli bir sorun olduğunu,
- Son olarak iletişimin denetlenmesi tedbirine ilişkin olarak ülkemizde mevzuat açısından bir eksiklik bulunmadığını ve dolayısıyla uygulamaya dönük bazı önlemlerin geliştirilmesinin konuya ilişkin sorunların çözülmesine ve şikâyetlerin ortadan kalkmasına katkıda bulunabileceğini,

ifade etmiştir.

Toplantıda ikinci olarak Turkuaz Medya Grubu adına sunum yapan Sabah Gazetesi Ankara Temsilcisi Okan MÜDERRİSOĞLU sunumunda özetle;

- Gerek yasa dışı gerekse yasal izleme ve dinlemelerin, özel hayatın gizliliği ve haberleşme özgürlüğünün ihlali noktasında özellikle üç husus açısından önemli olduğunu ve basın yayın kuruluşlarının ilgi alanına girdiğini, bu üç husustan birincisinin; yasal ve yasa dışı yolla elde edilmiş ses ve görüntü kayıtlarının özel hayata ilişkin yönleri ve buradaki gizlilik sınırları, mahremiyet boyutu, varsa sürmekte olan soruşturma ve kovuşturmalarla doğrudan bağlantısı ve tabii ki kamunun haber alma hakkıyla ilişkisi olduğunu, ikinci hususun; bizzat basın mensuplarının özel hayatına ilişkin veya görevlerini yaparken belli amaçlarla izlendiği ya da dinlendiği konusundaki kanaatleri veya somut tespitleri olduğunu, üçüncü hususun ise, birey hak ve özgürlüklerinin geliştirilmesi, demokratikleşmenin pekiştirilmesi, şeffaflık ve hesap verebilirlik noktasında kamuoyunun bize yüklediği görev olduğunu,

- İnternet ortamında genellikle kaynağı belirsiz şekilde yer alan kayıtların, basın yayın kuruluşları tarafından bir süre sonra haber değeri taşıdığının düşünüldüğü veya buna kayıtsız kalınması durumunda mesleki rekabette geri planda kalma korkusunun yer aldığını,

- Her hâlükârda yasa dışı yollarla elde edilen kayıtların, nasıl mahkemelerce delil kabul edilmiyorsa kurumları açısından da haber değeri taşımadığını varsaydıklarını ve bunu ön ilke olarak dikkate aldıklarını,

- İletişimin denetlenmesi tedbirinin uygulanması sırasında suçla ilgisi olmayan birtakım bilgi ve belgelerin de iddianamelere girdiğini, dava dosyalarının ekinde yer aldığını ve bu durumun gazeteciler tarafından nasıl olsa aleniyet kazandı, nasıl olsa dava dosyasının içinde var, bunlar yazılabilir şeklinde algılandığını,

- Geri bildirim ve kayıtların imha edilmesi konusunda uygulamada sorun olduğunu ve kanundaki hükmün uygulanmasını teşvik ettiklerini,
- Gerek medya kuruluşlarında gerekse medya mensuplarında “Ya, nasıl olsa dinleniyoruz.” algısının hâkim kanaat olduğunu,
- İlk elden gelen bu tür herhangi bir bilgi ve belgeyi, sorumlu olduğu bölümde hiçbir şekilde habere konu yapmadığını ve haber yapılmasına da kategorik olarak karşı durduğunu,

ifade etmiştir.

Toplantıda son olarak, Zaman Gazetesi adına sunum yapan Genel Yayın Yönetmen Yardımcısı Bülent KORUCU sunumunda özetle;

- Özel hayat, haberleşmenin gizliliği ve mahremiyeti, haber alma özgürlüğü ve basın özgürlüğü konularının dengeli bir biçimde, ne kadar verimli, bir arada yaşatılabilirse o kadar demokratik hukuk devleti olunabileceğini,
- Ne özel hayatın gizliliği için basın hürriyetinden ya da haber alma hürriyetinden vazgeçme lüksünün olduğunu, ne de basın hürriyeti diyerek özel hayata tecavüz etme, özel hayatı yerle bir etme gibi bir hakka sahip olunmadığını,
- Yasa dışı dinleme ve izleme yapanlar ile bu kayıtları yayınlayanların birbirinden ayırt edilmesi gerektiğini, yasa dışı dinleme ve izleme yapmak üzere teşkilat kuran ve bu işlemleri yapanların yakalanması ve çok ağır cezalandırılması gerektiğini,
- Gazetecilerin, kamu yararını gözeterek ve kayıtların elde edilmesinde kesinlikle bir dahillerinin bulunmadığı ve gelmiş materyali de tahrif etmeden, bozmadan, üzerinde bir kısım şeyler yapmadan, amaca matuf düzenlemeler yapmadan elde ettikleri kayıtları, kamu yararı süzgecinden geçirdikten sonra yayınlayabileceğini,
- Yayımlanan bir haberin muhtemel bir kamu zararını engellemeye matuf olup olmadığının önemli bir kriter olduğunu ve bu kriterden hareketle, gazetecinin samimi, iyi niyetli bir yaklaşımla bir kamu görevi mi gördüğü yoksa bir tetikçilik mi yaptığı, özel hayata tecavüz niyetiyle ya da maksadıyla mı bu işe giriştiğinin rahatlıkla ayırt edilebileceğini,

ifade etmiştir.

4- 3 Nisan 2013 Tarihli Hukuk Alt Komisyonu Toplantısı

Hukuk Alt Komisyonu dördüncü toplantısında Habertürk, Yeni Şafak ve Akşam gazeteleri yetkilileri ile Hürriyet Gazetesi Yazarı Ertuğrul ÖZKÖK’ü dinlemiştir.

Habertürk Gazetesi adına sunum yapan Ankara Temsilcisi Erdal ŞEN sunumunda özetle;

- Yasa dışı dinlemeler konusunun, Türkiye’de son zamanlarda daha çok gündeme gelen bir konu olmakla beraber aslında çok uzun yıllardır, teknik imkânların oluşmasıyla birlikte, Cumhuriyet tarihinin belki ilk yıllarında bile yaşanan bir sorun olduğunu,

- 1950’li yıllara ait bir araştırma çalışması olan “Belgelerin Dilinden Yassıada’nın Karakutusu” adlı kitabında bazı belgelere yer verdiğini ve bu belgelerde Demokrat Partinin ilk yıllarında, özellikle Menderes’in iktidar olduğu dönemlerde, Başbakan’ın evinin de, parti genel merkezinin de bir şekilde dinlendiğini, kimlerle konuştuğunun kayıt altına alındığının ve bunun dönemin PTT’si tarafından veya PTT’deki bazı unsurlar tarafından yapıldığının yer aldığını,

- Yasa dışı dinlemeler konusunun ülkemizin önemli sorunlarından biri olduğunu, ancak Türkiye’nin demokratikleşme süreciyle beraber bunların da minimize edilmesi gerektiğini,

- Yasa dışı izleme ve dinleme faaliyetlerinin toplum geleneğimizde yeri olmadığını, hem inanç noktasında hem de toplumsal kültür noktasında bu faaliyetlerin aslında kınanan ve karşılığı olumsuz olan davranışlar olduğunu,

- Gazetecilerin yasa dışı dinlemelerle ilgili yayınlar yaparken bütün bu yayınların yapılmasının aslında uygunsuz olduğu bilinciyle hareket etmeleri gerektiğini,

- Gelişen modern bir ülkede yasa dışı dinleme ve izlemelerin bir sorun alanı olmaktan çıkartılması gerektiği ve Komisyon tarafından gerçekleştirilen çalışmaların bu sorunun çözülmesine ön ayak olacağını,

ifade etmiştir.

Toplantıda ikinci olarak Yeni Şafak Gazetesi adına sunum yapan Ankara Temsilcisi Abdülkadir SELVİ sunumunda özetle;

- Dinlemeler konusunu meslek hayatı boyunca her zaman takip etmeye çalıştığını, kimi zaman bu konuda yazılar yazdığını,
 - Telefon dinlemelerinin daha çok cuntalar ya da çeteler tarafından sivillere, sivil hükûmetlere, aydınlara, yazarlara yönelik olarak uygulanmış bir sistem olduğunu ve geçmiş dönemlerde istihbarat örgütlerinin bağlı oldukları başbakanları bile dinlediklerini,
 - “Gladio” isimli kitabında Vatansever Kuvvetler Güç Birliği çetesi tarafından Başbakan Recep Tayyip ERDOĞAN’ın evinin dinlendiğini belgeleriyle yazdığını ve bu konu yargılama konusu olduğunu ve beraat ettiğini,
 - Devletin kendince tehdit olarak gördüğü sivil hükûmetleri, bir dönem solcuları, aydınları, bir dönem de sağcılar, dindarları dinlerken bu ayırdıkları zamanı terör örgütlerini dinleme, olayları önleme yönünde gösteremediğini,
 - Gizli kamera kullanımı ve telefon dinlemelerinde tapelerin yayınlanması konusunda maalesef basın olarak yeterince etik kurallara saygı göstermediklerini ve basın yayın kuruluşlarının bu konuda bir zaafı olduğunu,
 - Yeni Şafak Gazetesi’nin bu sürecin mağdurlarından olduğunu,
 - 1999 yılında 28 Şubatın rüzgârlarının devam ettiği bir dönemde, Ankara Emniyetinin 8’inci katında bir dinleme birimi ortaya çıkarıldığını ve Cumhurbaşkanının, Başbakanın, Genelkurmay Başkanının, Milli Güvenlik Kurulu Genel Sekreterliğinin, bazı bakan ve milletvekillerinin de burada dinlendiğinin tespit edildiğini,
 - Yasa dışı dinleme ve izlemelerin ülkemizde bir rejim meselesi olduğunu ve sadece etik bir sorun olarak izah edilmesinin yeterli olamayacağını,
- ifade etmiştir.
- Toplantıda üçüncü olarak Akşam Gazetesi adına sunum yapan Ankara Temsilcisi Çiğdem TOKER sunumunda özetle;
- Araştırma Komisyonu çalışmalarının ülkemizde dinlenme konusundaki yüksek ve yaygın toplumsal kaygıyı azaltmasına katkıda bulunacağını düşündüğünü,
 - Yasa dışı dinlemeler ve özel hayatın gizliliğini ihlal konusunun bugünün sorunu olmadığını, bu sorunun telefonların analog olduğu dönemlerden beri var olan kadim bir sorun olduğunu,

- Yasa dışı dinlemelerin; sonuçları, hukuki çerçevesi ve yol açtığı mağduriyetler itibarıyla “telefon dinlemesi” ve “ortam dinlemesi” şeklinde mutlaka ikiye ayrılması gerektiğini,

- Konunun bugün itibarıyla daha güncel ve daha vahim hâle getiren hususun bilişim teknolojisindeki gelişme olduğunu ve bu faaliyetlerin artık biraz daha steril, biraz daha hijyenik yani iz bırakmadan yapılabildiğini,

- Bilişim teknolojisindeki gelişmelerin hayatlarımızı olağanüstü kolaylaştırırken bu dinlemeler ve özel hayat ihlallerinin bu konunun gri bir alanı olarak tezahür ettiğini,

- İnsanlara sanal bir agorafobi yani açık alanda bulunma korkusu yaşatıldığını ve toplumun her kesiminin dinlendiği kuşkusunu taşıdığını,

- Abdülkadir SELVİ tarafından da ifade edilen yasa dışı dinlemelerin ve özel hayat ihlallerinin bir rejim sorunu olduğuna dair tespiti katıldığını,

- Yasa dışı dinleme ve özel hayat gizliliğine konu olan eylem ve işlemlere bağlanan yaptırımların yeterince caydırıcı olmadığını, bu caydırıcılığın cezaların ağırlığı kadar yargının işleyiş hızıyla da ilgili olduğunu ve bu faaliyetlerde bulunmanın toplumsal açıdan bakıldığında korkulan ve ürkülen bir suça dönüşmüş görünmediğini,

- Yasa dışı dinleme ve izlemeler ile özel hayat ihlallerinin teknoloji bu kadar gelişmişken herkesin elinde akıllı telefonlar varken bitmesini ve sıfırlanmasını beklemenin çok gerçekçi olmayacağını,

ifade etmiştir.

Toplantıda son olarak sunum yapan Hürriyet Gazetesi Yazarı Ertuğrul ÖZKÖK sunumunda özetle;

- Araştırma Komisyonunun toplumun büyük bir kısmında paranoya denilebilecek bir duygunun yayılmasına neden olan bir sorun üzerinde çalıştığını ve bu Komisyonun Türkiye’de illegal telefon dinlemeleri konusunda insanlarda yaratılan o kötü duygunun izlerini silecek bir sonuca ulaşmasını beklediğini,

- Kendisinin de telefon dinleme mağduru olduğunu, telefon dinleme mağduru olmanın ötesinde, yirmi beş yıldan bu yana, hayatının her anının devletin beş ayrı kuruluşu tarafından dinlendiği şüphesiyle değil, dinlendiğinden emin olarak yaşadığını ve dinleme kayıtlarının radyolarda yayımlandığını,

- Yasa dışı dinleme ve izleme mağduru olmanın yarattığı psikolojik etkinin çok ağır olduğunu ve o psikolojik etkiyi atmanın kolay kolay mümkün olmadığını,
- Ülkemizde yasa dışı izleme ve dinleme sorununun henüz üzerinde uzlaşmış bir sorun olmadığını ve bu sorunun çözülebilmesi için, Türkiye’de bütün kurumların ve bütün insanların ortak bir anlayış zeminine gelmesi gerektiğini,
- İzleme ve dinleme teknolojilerinin her gün daha da geliştiğini ve kolaylaştığını, teknolojideki bu gelişme ve kolaylık karşısında bu kayıtların yayınlanmasını önlemenin tek çaresinin bu faaliyetlerin büyük bir toplumsal ayıp ve suç olduğunun toplumun bütün fertlerine anlatılması gerektiğini,

ifade etmiştir.

5- 4 Nisan 2013 Tarihli Hukuk Alt Komisyonu Toplantısı

Hukuk Alt Komisyonu beşinci toplantısında Hürriyet, Star, Taraf ve Cumhuriyet gazeteleri ile Dicle Haber Ajansı yetkililerini dinlemiştir.

Hürriyet Gazetesi adına sunum yapan Ankara Temsilcisi Metehan DEMİR sunumunda özetle;

- Başbakan, Genelkurmay Başkanlığına, MİT müsteşarlarına kadar, çok kritik konumda bulunan isimlerin; basından farklı sektörlere kadar herkesin olmasa bile çok kritik isimlerin, maalesef yasa dışı dinlendiğini ve bu faaliyetlerin kimi zaman dinlenme, kimi zaman da gözetleme şeklinde gerçekleştiğini,
- Yasa dışı görüntü ve kayıtların Türkiye’de büyük travmalar yarattığı ve bu kayıt ve görüntülerin hem toplum tarafından hem de basın yayın kuruluşları tarafından çok büyük ilgi gördüğünü,
- Teknolojinin beraberinde getirdiği imkânlarla dinleme ve izleme yapabilmenin kolaylaştığını,
- Yasa dışı dinleme ve izleme faaliyetlerinin engellenememesinde önemli bir faktörün de bu suçu işleyenlerin yakalanamamaları olduğunu,
- Sorunun çözümünün yasal düzenlemelerle olamayacağı çok açık olduğunu, karşı teknolojilerin, istihbarata karşı koyma sistemlerinin güçlendirilmesi ve devletin teknik olarak bu faaliyetleri yapanlardan daha donanımlı hale getirilmesi gerektiğini,

ifade etmiştir.

Toplantıda ikinci olarak Star Gazetesi adına sunum yapan Ankara Temsilcisi Mustafa KARTOĞLU sunumunda özetle;

- Haberleşme hürriyeti ve özel hayatın gizliliğine yönelik ihlallerin iki yönü olduğunu; bunların yasa dışı dinleme ve izleme faaliyetleri ile yasa dışı dinleme ve izleme kayıtlarının gazetelerde, medyada haber olması, medyada değerlendirilmesi olduğunu,
- Son dönemlerde yasa dışı dinlemelerin teknik olarak çok kolaylaştığını ve bunun önlenmesi konusunda toplumun çok umutlu olmadığını,
- Türkiye'de uzun zamandır, biraz da medyanın desteğiyle, herkesin dinlendiği, herkesin izlendiği yolunda bir algı var olduğunu,
- Basın yayın kuruluşlarının elde ettikleri kayıt ve görüntülerin haber niteliği taşıyıp taşımadığı, haber niteliği taşısa bile yayınlamanın ahlaki olup olmadığı konusunda çalışması gerektiğini,

ifade etmiştir.

Toplantıda üçüncü olarak Taraf Gazetesi adına sunum yapan Ankara Temsilcisi Melih ALTINOK sunumunda özetle;

- Ülkemizde herkesin dinlendiği, herkesin izlendiği yolunda yaygın bir algı olduğunu, kendisinin de bu algıyı paylaştığını ve özellikle Ergenekon ve Balyoz davalarının kamuoyuna mal olmasıyla bazı tapelerin, dinlemelerin yayınlanmasıyla birlikte bu algının daha da yükseldiğini düşündüğünü,
- Gazetecilik etiği açısından Taraf gazetesi olarak kesinlikle ellerine ulaşan yasa dışı dinleme kayıtlarını yayınlamadıklarını ve hiçbir şekilde yasal olmayan delillere haberlerinde ve yorumlarında yer vermemeye çalıştıklarını,
- Medyanın bu konuda etik bir tavır ortaya koyması gerektiğini ve böylelikle bu tarz faaliyetlerin işlevselliğini yitireceğini,
- Yasa dışı dinleme ve izleme sorununun bugünden yarına aşılabilecek bir sorun olmadığını ve sorunun toplumun bilinçlendirilmesi ve medyanın, kanaat önderlerinin, siyaset kurumunun açıkça süreci mahkûm etmesiyle aşılabileceğini,

• Türkiye Cumhuriyeti şeffaflaştıkça, demokratikleştikçe, Avrupa Birliğiyle ilişkilerini geliştirdikçe bu tarz faaliyetlerin siyasi kültürden, pratikten kalkacağını düşündüğünü,

ifade etmiştir.

Toplantıda dördüncü olarak Dicle Haber Ajansı adına sunum yapan Haber Müdürü Abdurrahman GÖK sunumunda özetle;

• Yasal dinlemelerin mevzuatla belirlenmiş süre sınırlarına riayet edilmeden yapıldığını, iki yıl süreli dinleme ve izlemelerin yapıldığını,

• İddianamelerde özel hayatın gizliliğini ihlal eden telefon görüşmeleri, MSN yazışmalarının bütünüyle yer aldığını,

• Ajans muhabir ve çalışanlarının teknik ve fiziki takip altında olduğunu ve yasal çerçevede telefonların dinlendiğine ya da MSN yazışmalarının kayıt altına alınmasına ilişkin herhangi bir karar olmadığını ayrıca dinleme sonrasında hiçbir kurum tarafından ilgililere geri bildirimde bulunulmadığını,

• Yasa dışı dinlemelere ilişkin herhangi bir suç duyurusunda bulunmadıklarını ancak fiziki takiplere ilişkin suç duyurusunda bulunduklarını,

• Özel hayatın ihlaline ilişkin herhangi bir bilgi, bir görüntü ellerine ulaştığında hiç tereddüt etmeden reddetdiklerini ve kesinlikle bu tarz kayıtları yayınlamadıklarını,

ifade etmiştir.

Toplantıda son olarak Cumhuriyet Gazetesi adına sunum yapan Cumhuriyet Gazetesi Genel Koordinatörü Akın ATALAY sunumunda özetle;

• Dinlemelerin, yasal dinlemeler ve yasa dışı dinlemeler olmak üzere iki türü olduğu, yasal dinlemelerin de ikiye ayrıldığı, ilkinin kamuoyunda istihbarat dinlemesi olarak da ifade edilen önleme dinlemesi diğerinin de Ceza Muhakemesi Kanunu'na göre bir suç soruşturması nedeniyle Cumhuriyet savcılarının ve hâkim kararına dayalı adli dinlemeler olduğunu;

• Adli dinlemelerin CMK 135'inci maddeye göre ancak belirli suçların soruşturmasında mümkün olabildiğini,

• Yasa dışı dinlenme ve izlenme algısının topluma yayılmış olduğunu,

- TİB üzerinden yapılan dinleme verileri doğrultusunda, bir yılda yapılan dinleme sayısını Adli Sicil ve İstatistik Genel Müdürlüğünün internet sitesinden alınabilecek dinlemeye müsait olan suçlardan bir yıl içinde, aynı yılda, aynı bazda yapılan soruşturma sayısı ile kıyasladığında aradaki farkın çok yüksek olduğunu, bu karşılaştırmanın ortaya vahim bir tablo çıkardığını,

- Haberleşme hürriyeti ve özel hayatın gizliliğine yönelik ihlallerin, ancak saygın kabul edilen ünlü kişilerin başına geldiğinde gündeme geldiğini, bu durumdan medyanın da sorumlu olduğunu ancak bu sorunun Türkiye’nin yıllardan beri yaşadığı bir problem olduğunu,

- Cumhuriyet gazetesinin Ankara Temsilcisi Mustafa Ali Balbay’la ilgili bir soruşturma kapsamında alınan dinleme kararına bakıldığında kendisinin ev telefonu ve şahsi telefonlarının ve mobil telefonlarının yanı sıra ayrıca bir karar daha alındığını ve bu kararın da gazetenin Ankara bürosunun santral telefonunun dinlenmesi kararı olduğunu,

- Cumhuriyet gazetesinin Ankara bürosunda gerçekleştirilen bütün görüşmelerin haber kaynaklarıyla, bürokratlarla, siyasetçilerle, kamu görevlileriyle, bütün haber kaynaklarıyla yapılan görüşmelere ilişkin kayıtların tutulduğunu ve bunların ifşa edilmesinde de hiçbir sakınca görülmediğini,

- Anılan dava dosyasına bu suçla hiçbir ilişkisi olmayan, şüpheli olmayan bir gazetecinin dönemin RTÜK üyelerinden birisi arasındaki, konuyla hiçbir ilgisi olmayan görüşmenin dinlendiğini, kayda alındığını ve “tapelerin” suç delilleri arasında dosyada yer aldığını ve anılan örnekte olduğu gibi özel hayat ihlalleri sonucunda Cumhuriyet gazetesi Ankara bürosunda çalışan gazetecilerin telefon görüşmesi yapmaktan çekindiklerini, bürokratları, haber kaynaklarını, siyasetçileri, hiç kimseyi aramadıklarını ve bu olay sonucunda Ankara temsilciliğinin haber alma, haber verme hakkının sonlandırıldığını,

- Önleme amaçlı yapılan dinlemelerin, suçun önlenmesi için yapılan ortada bir soruşturma falan yokken, cezai soruşturma yokken yapılan bir dinleme olduğu ve bu dinlemelerin istihbarat, önleme amaçlı olması nedeniyle adli dinlemeler için CMK 135’inci maddede aranan sıkı şartların aranmadığını, başkaca delil elde etme imkânı olmaması, kuvvetli şüphe olması gibi şartların aranmadığını,

- Gazetenin eski imtiyaz sahibi rahmetli İlhan Selçuk hakkında Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanlığınca istihbarat dinlemesi yapıldığını ve o dinleme kayıtlarının delil olarak dosyaya konulduğunu ve Polis Vazife ve Salahiyet Kanunu’nun ek 7’nci maddesinde yer alan *“Bu şekilde dinlenen ve kayda alınan görüşmeler başka hiçbir*

amaçla kullanılmaz.” hükmünün uygulamada bu kayıtların delil olarak kullanılmaması açısından yeterli olmadığını,

ifade etmiştir.

6- 10 Nisan 2013 Tarihli Hukuk Alt Komisyonu Toplantısı

Hukuk Alt Komisyonu altıncı toplantısında Emniyet Genel Müdürlüğü emekli İstihbarat Daire Başkanı Bülent ORAKOĞLU’nu, Merkez Emniyet Müdürü Osman AK’ı ve emekli İstihbarat Daire Başkanı Sabri UZUN’u dinlemiştir.

Toplantıda ilk olarak sunum yapan Bülent ORAKOĞLU sunumunda özetle;

- Yasa dışı telefon dinlemelerinin Türkiye’nin çok önemli sorunlarından biri olduğunu, dünyanın birçok gelişmiş ülkesinde de illegal veya yasa dışı diyebileceğimiz birtakım olayların ortaya çıktığını ve bunların büyük bir skandal seviyesinde yansıtılarak kamuoyuyla paylaşıldığını ve bu faaliyetlerin Türkiye’de ve dünyanın birçok yerinde kamuoyunu çok ciddi rahatsız ettiğini,

- Yasal olarak yapılan telefon izleme ve dinlemelerinin suç ve suç örgütlerinin ortaya çıkarılmasında çok faydalı bir görev gördüğünü,

- Türkiye’de yaklaşık yirmi altı yıl, bilfiil emniyet teşkilatında bulunduğunu, görevde bulunduğu süre içerisinde gerek sivil gerekse askerî yargı tarafından hiçbir suretle “illegal telefon dinlediği” iddiasıyla muhatap olmadığını,

- İstihbarat Daire Başkanı olarak görev yaptığı dönemde Emniyet İstihbarat Daire Başkanı olarak yargıdan yasal dinleme kararı almanın zor olduğunu,

- Yasal dinleme yapan kurumlar içerisinde geçmiş dönemlerde hakikaten yasa dışı izleme ve dinleme yapanlar olduğunu ve ancak son yıllarda dinlemelerin yapıldığı birimlerde herkese bilmesi gerektiği kadar veya girmesi gerektiği kadar sisteme girme izni verildiğini, bunun dışında girenlerin sistemde kolayca tespit edilebildiğini ve buna benzer önlemler ile yasal dinlemelerin çok ciddi bir zapturapt altına alındığını,

- Dinlemeler yasal bir tedbirlerle zapturapt altına alınsa da muhakkak ki uygulamadan kaynaklanan veya uygulayıcılardan kaynaklanan sorunlar da olduğunu,

- Mevzuat ne kadar yerinde olursa olsun, cezalar ne kadar artırılırsa artırılсын dinleme yapmak isteyenlerin her halükarda dinleme yapabileceğini ancak cezaların caydırıcılık etkisinin de olduğunu,

- Son yıllarda dinlemeyle ilgili birimlerde suiistimallerin azalmış olduğunu ve bununla sistemlerin rahatlıkla kontrol edilebilmesi yani dinleme yapabilecek unsurların kendi iç mekanizma denetimleriyle ortaya çıkarılabilmesi imkanının artmasından kaynaklandığını,

- Teknolojinin ve teknolojinin gelişmesiyle yabancı gizli servislerin de ülkemizde rahatlıkla dinleme ve izleme yapabileceklerinin de unutulmaması gerektiğini,

- Özel dedektiflik bürolarıyla ilgili sistemin bir an önce kurulması ve konuya ilişkin düzenlemelerin yapılarak dedektiflik bürolarının zapturapt altına alınması gerektiğini,

- Yasa dışı dinleme ve izlemelere ilişkin olarak esas yapılması gerekenin Türkiye'nin ulusal güvenliğini tehdit edebilecek, yabancı ülke gizli servisleri tarafından yapılabilecek dinlemelerin önlenmesi konusu olduğunu ve bu görevin de tamamen Millî İstihbarat Teşkilatımıza düştüğünü,

- Dinleme ve izlemelerin teknolojinin gelişmiş olduğu seviye itibarıyla yüzde 100 engellenmenin mümkün olmadığını,

ifade etmiştir.

Toplantıda ikinci olarak sunum yapan Osman AK sunumunda özetle;

- Günümüz teknolojisi karşısında dinleme faaliyetlerinin belirli bir ölçüde sınırlandırılması mümkün olsa da temelde bütünüyle engellenmesi mümkün olamayacağını,

- Bu faaliyetlerin üç boyutta ele alınması gerektiğini; ilk boyutun, ulusal ve uluslararası mevcut iletişim üzerindeki teknik faaliyetlerin dinleme veya izleme faaliyetlerinin kontrol edilmesi veya denetlenmesi, ikinci boyutun kamuoyu gündeminde yaygın olan, ortam dinlemeleri, üçüncü boyutun ise görsel, görüntü anlamındaki dinleme ve izleme faaliyetleri olduğunu,

- İnternet üzerinden son sistem telefonların üzerinde dinleme, ortam dinleme programları da yüklenmiş şekliyle satılabildiğini, değişik dinleme aletlerinin, dijital vericilerin satılabildiğini, satımın ötesinde bu alanda 24 saat hizmet verildiğini ve ülkemizde bu alanda, maalesef, ciddi anlamda bir denetim mekanizması eksikliğinin bulunduğu,

- MOBESE kameraları ile herkesin kendi evinin, iş yerinin önüne yerleştirebildiği özel güvenlik kameralarına ait özel hayatın gizliliğini ihlal eden görüntülerin internet

ortamında yayınlandığını ve ilgililerin bu konuda hukuki anlamda bir başvuruda bulunmamaları durumunda maalesef o konuda cezai anlamda veya kamusal anlamda bir yargısal veya idari bir tedbirin geliştirilemediğini,

- İletişim alanında kullanılan santrallerin milli olmaması, yazılımı ve donanımının bilinmemesi ve bu santrallerin kontrolünün ülkemizce gerçekleştirilmemesi durumunda dileyen insanın, dünyanın dilediği yerinden, dilediği şekilde, bu santraller üzerinden görüşme yapan numaraları dinleyebileceğini,

- Telekomünikasyon altyapısının ulusal anlamda imalat kodlarına hâkim olunması gerektiğini,

- Fiber optik teknolojinin kullanılmaya başlaması ile birlikte fiber ortamında bir bilginin kablunun geçtiği yerde üzerine bir bilgisayarla bağlantılı bir kod çözücü ve ses depolamanın konulması durumunda çok rahat dinleme yapılabileceğini,

- Dinleme ve izlemelerde geçmiş dönemlerde ses ve görüntüyü depolamanın çok zor olduğunu ancak gelişen teknoloji sayesinde çok küçük boyutlu cihazlarla çok yüksek depolama imkanı olduğunu,

- Dinleme ve izleme cihazlarının bu kadar ucuz, bu kadar rahat temin edilebilir olduğu bir ortamda eğer şahıs çalıştığı kurumda veya bulunduğu ortamı kullanabilecek veya burada birtakım motivasyonlarla yasa dışı anlamda bir faaliyete girerse bunu engellemenin oldukça zor olduğunu,

- Dinleme ve izleme faaliyetlerinin son derece önemli olduğunu ve ciddi anlamda denetlenmesi ve kontrol altına alınması gerektiğini,

ifade etmiştir.

Toplantıda üçüncü olarak sunum yapan Sabri UZUN sunumunda özetle;

- Türkiye’de yapılan yasa dışı dinlemelerin büyük bir kısmının devlet görevlileri tarafından yapıldığını, devlet görevlisi olmayanlar tarafından da yapılan dinlemeler olduğunu ancak bunların faillerinin hemen yakalandığını,

- 1999 yılında “Ankara Emniyetinde 983 kişinin telefonu dinlendi.” şeklinde ulusal yayın yapan bir gazetede bir haber çıktığını, kendisinin 2011 yılında o kamu kurumlarının telefonunun dinlenmediğini, uzaktan müdahaleyle Ankara Emniyet Müdürlüğü’nün LMS (lean monitoring system) bilgisayarına sırf, Ankara Emniyetindeki insanlar bu işte mağdur olsun diye, uzaktan müdahaleyle yükleme yapıldığını,

- 2001 yılında İstanbul’da gözetim altına alınan bir şahıs bir örgüt hakkında bilgi verdiği ifadelerinin kravat kamera yöntemi ile kaydedilerek kullanıldığını,
- 2001 yılında İstihbarat Daire Başkanı olduğu dönemde Ergenekon şemasını gördüğünü,
- 2005 yılında konuya ilişkin olarak 5237 sayılı Kanun’un çıkarıldığını, 5237 sayılı Kanun’un o zamanki teknolojiler içerisinde yasa dışı dinlemeleri önleyecek bir kanun olduğunu ancak daha sonraki yıllarda gelişen teknolojilerin var olduğunu,
- A15 ve A25 denilen mobil dinleme aletlerin geliştirildiğini ve bu araçların istenilen yere konularak, istenilen numaranın da cihaza yazılarak, o cihazın kendisini baz istasyonuna telefon gibi tanıtmaya yoluyla dinlenebildiğini,

ifade etmiştir.

7- 11 Nisan 2013 Tarihli Hukuk Alt Komisyonu Toplantısı

Hukuk Alt Komisyonu 7’nci toplantısında Hürriyet Gazetesi Yazarı Sedat ERGİN ve Ekonomi Bakanlığı yetkililerini dinlemiştir.

Hürriyet Gazetesi Yazarı Sedat ERGİN sunumunda özetle;

- Ülkemizde yasa dışı telefon dinlemelerinin vatandaşların temel hak ve özgürlükleri açısından ana ihlal alanlarından biri olduğunu,
- Özel hayatın gizliliğinin korunması bakımından Türk Ceza Kanunundaki düzenlemelerin yeterli olmadığını,
- Doksanlı yılların sonlarında meydana gelen bazı olayların, telefon dinlemeleri konusunun disipline edilmesi ve hukuki düzenlemelerin yapılması ihtiyacını ortaya çıkardığını,
- 1985’te Polis Vazife ve Salahiyet Kanunu’na yapılan bir ekleme ile polise de istihbarat yetkisi verildiğini; fakat dinlemenin nasıl yapılacağına dair esaslara yer verilmediğini ve bu konuda bir boşluk oluştuğunu,
- 1999’da 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu çerçevesinde telefon dinlemelerinin esaslarının ilk kez düzenlendiğini ve bu düzenlemenin ihtiyaçlara cevap verdiğini,
- Bugün karşılaşılan en büyük sorunlardan birinin dinleme kayıtlarının herhangi bir ayıklama yapılmadan, olduğu gibi iddianame eklerinde yer alması olduğunu,

- 2011 yılında 1086 sayılı Kanunun yerine yürürlüğe giren 6100 sayılı Hukuk Muhakemeleri Kanunundaki düzenlemede, eski Kanunun aksine “münasebetsiz evrakın imha edileceğine” dair ibarenin bulunmadığını,

- 2005 yılında, 5237 sayılı CMK ile yeni bir düzenleme getirildiğini, Polis Vazife ve Salahiyet Kanunundaki anılan boşluğa ilişkin tamamlayıcı hükümler ihdas edildiğini, 4422 sayılı Kanunda yer alan, kayıtların soruşturmaya ilişkin olmayan bölümlerin ayrılmasına ilişkin düzenlemenin 5237 sayılı Kanun ve onun uygulama yönetmeliğinde yer almadığını,

- Avrupa İnsan Hakları Mahkemesi’nin dinleme kayıtlarının herhangi bir ayırım gözetilmeden, olduğu gibi yayımlanmasının kendi içtihatlarına ters düştüğüne yönelik bir kararı ve Avrupa Konseyi İnsan Hakları Eski Komiseri Thomas HAMMARBERG’in bu konuda bir raporu bulunduğunu,

- Adli ve istihbari amaçlı dinlemelere ilişkin alınan izinlerin süresinin en fazla ne kadar uzatılabileceği konusunun belirsiz olduğunu,

- Yargıtay içtihatlarının aksine istihbari amaçlı dinleme kayıtlarının uygulamada delil olarak değerlendirildiğini ve bu durumun temel hak ve özgürlükler açısından önemli bir sorun teşkil ettiğini,

- Dinleme izni başvurularında kolluk makamları tarafından yanıltıcı beyanlar verilmesi suretiyle hâkimlerin ilgisiz kişiler hakkında dinleme kararı verebildiklerini, bu konuda hâkimlerin daha özenli davranmaları gerektiğini ve hukuki sorumlulukla ilgili düzenleme yapılması gerektiğini,

ifade etmiştir.

Toplantıda Ekonomi Bakanlığı adına sunum yapan İthalat Genel Müdür Vekili Mehmet AZGIN, dinleme ve izleme cihazlarının ithalatına ilişkin sunumunda özetle;

- İthalat Genel Müdürlüğünün görevlerinin 637 sayılı Ekonomi Bakanlığının Teşkilat ve Görevleri Hakkındaki Kanun Hükmündeki Kararnamede düzenlendiğini; buna göre Genel Müdürlüğün ithalatın uluslararası anlaşmalar ve kalkınma planları ile uyumlu hâlde yürütülmesini sağlamak, kamu kurum ve kuruluşlarına verilmiş ithalatla ilgili çeşitli yetkilerinin kullanımında koordinasyonu sağlamak, ithalat rejimine ilişkin kararlar dâhil olmak üzere ithalata dair mevzuatı hazırlamak, ithalatı iç piyasa ve sanayinin ihtiyaçlarına

göre düzenlemek, ithal malların dünya piyasasına uygun olarak ithalini sağlayıcı tedbirleri almak ve bunları uygulayıp denetlemek gibi görevlerinin bulunduğunu,

- Mevzuata göre kamu ahlakı, kamu düzeni veya kamu güvenliği; insan, hayvan ve bitki sağlığının korunması veya sınai ve ticari mülkiyetin korunması amaçlarıyla alınan önlemlerin kapsamı dışında kalan malların ithalatının serbest olduğunu,

- İthalatı yasak ürünlerle ilgili olarak, tespit konusunda hangi kurumların yetkili olduğu ve hangi ürünlerin bu kapsama girdiği konusunda yasal düzenlemeye ihtiyaç duyulduğunu,

- İzleme ve dinleme cihazlarının ithalatının sınırlandırılması konusunda alınacak önlemlerin gümrük tarife istatistik pozisyonları çerçevesinde, farklı kurumlardan uzmanların görüşleri nazara alınarak ve piyasa dinamiklerini olumsuz etkilemeyecek biçimde belirlenmesi gerektiğini,

- İzleme ve dinleme cihazları birçok alanda yasal olarak da kullanıldığı için, bu cihazların ithalatının sınırlandırılması konusunda bugüne kadar herhangi bir düzenlemeye gidilmediğini,

ifade etmiştir.

8- 17 Nisan 2013 Tarihli Hukuk Alt Komisyonu Toplantısı

Hukuk Alt Komisyonu son toplantısında Gümrük ve Ticaret Bakanlığı yetkilileri ile Emniyet Genel Müdürlüğü emekli Genel Müdür Yardımcısı Emin ARSLAN'ı dinlemiştir.

Gümrük ve Ticaret Bakanlığı adına ilk olarak sunum yapan Gümrük ve Ticaret Bakanlığı Müsteşarı Ziya ALTUNYALDIZ sunumunda özetle;

- Gümrük ve Ticaret Bakanlığının, vizyonu ve misyonunda da yer alan temel ilkeler çerçevesinde ülkemizin dünyanın en kolay ve en güvenli ticaret yapılan ülkesi hâline getirilmesi doğrultusunda çalışmalarını sürdürdüğünü,

- Eşyaların gümrüğe gelip beklemesi hâlinde, hem eşyanın uzun dönem gümrükte beklemesi hem de eşyaya ilişkin nitelik, emniyet ve güvenlik açısından ülkemizin hem insan güvenliği hem iç pazar güvenliği açısından birtakım sıkıntılara yol açabildiğinden, eşyaların gümrüğe gelmeden önce elektronik özet beyan sistemine geçildiğini,

- Gümrük çalışmalarında risk analizi metodolojisini uyguladıklarını,

• Hızlı kargo ve posta yoluyla gönderiler, elektronik olarak gelen eşyaların tamamen kayıt altına alındığını ve izlenebildiğini ve raporlanabildiğini,

ifade etmiştir.

Gümrük ve Ticaret Bakanlığı adına ikinci olarak sunum yapan Gümrükler Genel Müdürü Rıza AKÇİN sunumunda özetle;

• Yasal olarak ülkeye eşya girişinin (gayri yasal olandan bahsedilmediğini, örneğin gümrük işlemine tabi tutmadan veya sınırlardan geçebilecek ya da gümrüğe beyan edilmeden kaçırılan eşyalar hariç) yasal olarak ülkeye eşya ithalatının iki şekilde söz konusu olduğunu; birincisinin ticari olarak ithalat yapma, ikinci olarak ticari nitelik arz etmeyen, yolcunun beraberinde gelen ya da yolcuya gönderilebilecek küçük miktarlardaki ithalat suretiyle eşya ülkeye getirme olduğunu,

• Dinleme veya izleme cihazlarının gümrük tarife cetvelinde ismen yer almadığını, dinleme ve izleme cihazlarının yer alabileceği dört gümrük tarife pozisyonu bulunduğunu, bu tarifelerdeki eşyaların, illa illegal dinlemelerde veya kişileri dinlemelerde kullanılabilecek cihazlar olduğu anlamına gelmediğini ve maalesef o ayrımı yapabilme imkânına sahip olmadıklarını,

• Yapılan incelemelerde normal şartlarda yasa dışı dinlemeler baz alındığında bu bir suç oluşturduğu için, kişilerin normalde bunu beyan edip normal ithalat yöntemine tabi tutmasının çok mantıklı olmadığını düşündüklerini ve bu nedenle, bu tür eşyaların daha çok yasa dışı veya kaçak yollardan geldiğini tahmin ettiklerini ve nitekim bu konuda daha çok valizlerde olmak üzere bazı yakalamalarının olduğunu,

• Bu dört gümrük istatistik tarife pozisyonlarında yer alan eşyaların denetimin farklı kamu kurumları tarafından yapıldığını,

ifade etmiştir.

Gümrük ve Ticaret Bakanlığı adına üçüncü olarak sunum yapan Gümrükler Muhafaza Genel Müdürü Yusuf GÜNEY sunumunda özetle;

• Gümrüklerdeki kontrollerin artırılması ve etkin denetim yapılabilmesi amacıyla personel sayılarını artırdıklarını bunun yanı sıra teknolojik cihazlarını da gelişen teknolojiyle beraber yenilediklerini ve artırdıklarını,

- Dinleme cihazlarıyla ilgili olarak bu cihazların ağırlıklı olarak yolcu beraberinde, bagajında getirildiğini ve bunlara ilişkin yakalamaların ihbar veya istihbarat üzerine ya da gözlem yoluyla yapıldığını çünkü hem hukuken hem de teknik olarak bütün yolcuları kontrol edemediklerini,
- Son dönemlerde internet yoluyla da yakalamalar gerçekleştirdiklerini ve buna özellikle önem verdiklerini,

ifade etmiş ve Gümrükler Muhafaza Genel Müdürlüğü tarafından gerçekleştirilen dinleme ve izleme cihazları yakalamalarından örnekler vermiştir.

Gümrük ve Ticaret Bakanlığı yetkililerinin ardından toplantıda son olarak sunum yapan emekli Emniyet Genel Müdür Yardımcısı Emin ARSLAN sunumunda özetle;

- Teknik dinleme ve izlemelerin teknik ve yasal anlamda geliştirilmesine İstihbarat ve KOM Daire Başkanlığı yaptığı dönemlerde katkı sağladığını,
- Teknik dinlemelerin çok elzem ancak bir silah kadar da tehlikeli olduğunu ve sorumsuzca kullanıldığında insanların hayatını nasıl kararttığının, onurlarını nasıl yok ettiğinin yaşanan olaylarla açıkça görüldüğünü,
- Polisiye çalışmalar için çok önemli olan bu imkânların yerleşmesine katkı sağladığını ancak kendi görev yaptığı yıllarda ve ünitelerde bu imkânların amacı dışında asla kullanılmadığını rahatlıkla söyleyebileceğini,
- Odalara böcek yerleştirilmesi, bazı telekom veya GSM operatörlerine yaptırılacak kişisel, kısmi dinleme çalışmalarının her zaman mümkün olduğunu ve bu cihazların internetten dahi satın alınabildiğini,
- Görüşmelere ilişkin detay kayıtlarının, sabit veya cep telefonlarıyla kimin kimi aradığı, telefonunun açılıp açılmadığını, açılmışsa ne kadar süre ile görüşüldüğüne dair kayıtların; herhangi bir somut olay gösterilmesine gerek duyulmadan Türkiye genelinde MİT, Emniyet ve Jandarmaya verilmekte olduğunu, bu yetkinin 2008 yılında Ankara’da mahkeme kararıyla sadece Emniyet Genel Müdürlüğü İstihbarat Daire Başkanlığına ve Jandarma Genel Komutanlığına verildiğini ve bilahare de mahkeme kararıyla Jandarmadan kaldırıldığını, sadece Emniyet Genel Müdürlüğü İstihbarat Daire Başkanlığı ve MİT’e verildiğini bildiğini,
- Dinleme işlemi sonrasında hangi bilgilerin imha edildiği, hangilerinin saklandığını öğrenmenin mümkün olmadığını,

- Yasa dışı dinlemelerin ağırlıklı olarak devlet gücünü art niyetli kullanan kişiler tarafından yapıldığını,
- Yasa ve yönetmeliğe göre önleme dinlemelerinin altı ayda bir mülkiye müfettişleri tarafından kontrol edilmesi gerekirken bu kontrollerin yapılmadığını,
- A15, A25 olarak adlandırılan teknik cihazların var olduğunu, bu cihazların sahte baz istasyonu görevi üstlenmekte, çevresindeki telefonları kapasitesine göre kendine bağlamakta, bu baz istasyonu üzerinden yapılan görüşmeleri istisnasız, hiçbir savcı, mahkeme kararına gerek duyulmaksızın kontrol etmekte olduğunu, buradan gönderilecek sinyallerle de evinizdeki telefonlarınızın mikrofonu verici hâline getirilip sanki odanıza böcek yerleştirilmiş gibi çok rahat bir şekilde insanların izlenebileceğini ve bu cihazların emniyet, jandarma ve MİT’te var olduğunu,
- Konuya ilişkin yasal düzenlemelerin yeniden ele alınması ve şimdiye kadar yaşananların tekrarlanmaması için caydırıcı olacak etkin bir denetim mekanizması gerektiğini,

ifade etmiştir.

TEKNİK ALT KOMİSYON TOPLANTI TUTANAK ÖZETLERİ

1- 27 Mart 2013 Tarihli Teknik Alt Komisyon Toplantısı

Teknik Alt Komisyonun ilk toplantısında Alt Komisyon Başkan seçimi yapılmış ve İstanbul Milletvekili Mihrimah Belma SATIR Teknik Alt Komisyon Başkanı seçilmiştir.

2- 28 Mart 2013 Tarihli Teknik Alt Komisyon Toplantısı

Alt Komisyon çalışma takvimi, çalışma usul ve esasları ile Alt Komisyona davet edilecek kişi, kurum, kuruluşlar ve Komisyonca ziyaret edilmesi ve incelemelerde bulunulması gereken kurumlar belirlenmiştir.

3- 3 Nisan 2013 Tarihli Teknik Alt Komisyon Toplantısı

Teknik Alt Komisyon, üçüncü toplantısında TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri Anonim Şirketi ve Bilkent Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Bölümü öğretim üyelerini dinlemiştir.

TÜRKTRUST adına sunum yapan Yazılım Geliştirme ve Ar-Ge Müdürü Musa Öner DEMİRKOL sunumunda özetle;

- TÜRKTRUST A.Ş.’nin Türk Silahlı Kuvvetleri Elele Vakfının bir iştiraki olarak 2004 yılında kurulmuş olup, 5070 sayılı Elektronik İmza Kanunu kapsamında elektronik sertifika hizmet sağlayıcılığı (ESHS) görevi yaptığını ve bu kapsamda SSL ve EV SSL sertifika hizmeti verdiğini,

- ESHS’lerin nitelikli bir elektronik sertifikayı gerçek kişilere gerçekten onlar olduğunu bilerek vermekle yükümlü olduğunu ve aksi takdirde güvenlik zincirinin sekteye uğrayacağını,

- 5070 sayılı Elektronik İmza Kanununa göre güvenli elektronik imzanın, elle atılan imza ile aynı hukuki sonucu doğurduğunu, diğer bir deyişle nitelikli elektronik sertifikayla yapılan elektronik imzalama işleminin elle atılan imzayla eş değer olduğunu,

- Elektronik imzanın sahibine ait olup olmadığını tespit etmeyi sağlayan matematiksel ve algoritmik yöntemler bulunduğunu,

- Yalnızca gerçek kişilerin elektronik imzaya sahip olabileceğini, elektronik imza sertifikalarının içerisinde isim, kimlik numarası ve geçerlilik süresi bilgilerinin yer alması gerektiğini,

- Basına yansıyan, bazı kurumlara hatalı SSL sertifikası verilmesi olayının hatalı şablonlar nedeniyle sehven gerçekleştiğini ve bu konuda güvenlik sistemi ve süreç yönetimine ilişkin gerekli önlemlerin alındığını,

ifade etmiştir.

Bilkent Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Bölümü öğretim üyesi Prof. Dr. Ahmet Enis ÇETİN “Dijital Ses, Konuşma, Görüntü ve Video İşleme” konulu sunumunda özetle;

- Ses sinyallerinin rakamlarla ifade edilebildiğini, telefon konuşması sırasında bir insanın saniyede sekiz bin rakam ürettiğini, konuşan kişinin 20-30 milisaniyede gırtlak modelinin çıkarılabileceğini,

- Bilgisayar ortamında metinden ses sentezleme yapılabildiğini, başka bir deyişle, elde yeteri kadar veri olması halinde herkese her şeyin söylenilebileceğini,

- Benzer şekilde, fotoğraf ve görüntülerin de rakamlarla ifade edilebildiğini ve uygun rakam dizileri üretilmek suretiyle montajlanan fotoğraf ve görüntüleri orijinalinden ayırt etmenin çok zor olduğunu,

- İnternet arama motorlarının internet üzerindeki birtakım hareketlerimizi izleyebildiğini, bu çerçevede milli anti-virüs yazılımı geliştirilmesinin gerektiğini,

- Telefon şebekelerinin devletler tarafından çeşitli güvenlik önlemleri alındığı için nispeten daha güvenli olduğunu,

ifade etmiştir.

Prof. Dr. Ahmet Enis ÇETİN'in ardından ikinci olarak sunum yapan Bilkent Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Bölümü öğretim üyesi Prof. Dr. Ayhan ALTINTAŞ sunumunda özetle;

- Bilkent Üniversitesi bünyesinde kurulmuş olan İletişim ve Spektrum İzleme Yönetimi Araştırma Merkezi'nin (İSYAM) esas faaliyetinin frekans planlaması olduğunu,

- Böcek adı verilen dinleme cihazlarının aktif ya da pasif çalışan modellerinin olduğunu ve aktif olanlarının ASM, GSM ya da çok geniş bantlarda yayın yapabileceğini,

- Milli Monitör Sisteminin ülkedeki frekansların verimli bir şekilde kullanımının sağlanmasını amaçladığını ve bu kapsamda izinsiz yayınların tespiti, spektrum doluluğu ve yayınların teknik parametrelere uygunluğu gibi konularda ilgili olduğunu,

ifade etmiştir.

4- 4 Nisan 2013 Tarihli Teknik Alt Komisyon Toplantısı

Teknik Alt Komisyon, dördüncü toplantısında Bilgi Güvenliği Derneği ve TOBB Türkiye Özel Güvenlik Hizmetleri Sektör Meclisi Başkanlığını dinlemiştir.

Toplantıda ilk olarak sunum yapan Bilgi Güvenliği Derneği Başkanı ve Gazi Üniversitesi Teknoloji Fakültesi Elektrik-Elektronik Mühendisliği Bölüm Başkanı Prof. Dr. Mustafa ALKAN sunumunda özetle;

- Bugünkü teknolojik altyapıyla, imkânlarla, eğer hedefte bir kişi, kurum ya da bir devlet varsa, o kişinin ya da kurumun dinlenmemesinin, izlenmemesinin ya da gerekli birtakım bilgilere erişilmemesinin neredeyse imkânsız hale gelmiş durumda olduğunu,

- Türkiye’nin siber güvenlik konusunda dünya ile rekabet edecek düzeyde insan kaynağına sahip olmakla beraber, bu kaynakları iyi organize edemediğini,
- Kendi milli çözümlerini üretemeyen ülkelerin siber güvenliklerini sağlamalarının çok zor olduğunu ve bu anlamda ülkemizin bilgi güvenliği ve teknolojileri konusunda milli çözümlerini üretmesi gerektiğini,
- 2010 yılı itibarıyla Türkiye’de dışarıdaki merkezlerden yönetilen iki bin civarında köle bilgisayar bulunduğunu,
- Ülkemizdeki kamu kurum ve kuruluşlarının bilgisayarlarına sızma testleri yapacak, siber güvenlik durumlarını sürekli izleyecek, mevcut ve potansiyel riskleri ortaya çıkaracak kuruluşlar oluşturulması gerektiğini,
- Türkiye’nin internet üzerinden yapılan her türlü kişisel ve kurumsal bilgi ve belge paylaşımı konularında siber tehdit altında olan on ülke içerisinde olması nedeniyle bilgi güvenliği konusunda ciddi tedbirler alması gerektiğini,
- Bilgi Güvenliği Derneği çatısı altında hazırlanan Türkiye Siber Güvenlik Strateji Belgesinin, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından gözden geçirilerek yayımlandığını ve bu belgenin yayımından sonra Bakanlar Kurulu kararıyla Ulaştırma, Denizcilik ve Haberleşme Bakanlığı koordinasyonunda Siber Güvenlik Kurulunun oluşturulduğunu,
- Yapılan düzenlemelere rağmen, ülkemizin henüz bir siber savunma gücüne sahip olmadığını ve gelişen teknoloji ile birlikte çeşitlenen siber saldırılara karşı böyle bir güç meydana getirmenin zorunlu olduğunu,
- Siber Güvenlik Strateji belgesi doğrultusunda bir eylem planı hazırlanması ve bu konuda geç kalınmaması gerektiğini,
- Kişisel verilerin güvenliği konusundaki yasal düzenleme eksikliği bulunduğunu ve bu konudaki yasanın mutlaka çıkarılması gerektiğini,

ifade etmiştir.

Toplantıda ikinci olarak sunum yapan TOBB Türkiye Özel Güvenlik Hizmetleri Sektör Meclisi Başkanı Hasan Gazi ÖZER ve Sektör Temsilcisi Hakan ÇEVİKOĞLU “Özel Güvenlik ve Elektronik Güvenlik Sistemleri Sektör Görüşleri” başlıklı sunumlarında özetle;

- Türkiye’de özel güvenlik sektörünün; yaklaşık 1.500 civarında firma ve 300 bin çalışanı içerisine alan, 2004 yılında kabul edilen 5188 sayılı Kanunla ve İçişleri Bakanlığının izniyle faaliyetlerini yürütmekte olan özel güvenlik şirketleri, buna paralel olarak yine kanunda içeriğini bulan elektronik güvenlik sistemleri ve alarm izleme merkezleri olmak üzere üç ayrı parçaya ayrılmış şekilde faaliyetini sürdürdüğünü,

- Alarm sistemlerinin haricinde kalan kamera sistemleri, MOBESE sistemleri, kayıt sistemleri vs. ile ilgili faaliyetlerin ticari olarak sürdürüldüğünü ve bunun için İçişleri Bakanlığından özel bir faaliyet izin belgesi almaya gerek olmadığını,

- Ülkemizde alarm ve kamera sistemlerinin satışı ve montajı konusunda serbest piyasa kurallarının uygulandığını ve bu nedenle bir standardizasyon ve kalite-kontrol sisteminin bulunmadığını,

- Fiyatı daha düşük olduğu için genellikle yedi günlük kayıt sistemlerinin kullanıldığını, bu süre sonunda eski verilerin üzerine kayıt yapılmasının belge ve görüntü temini konusunda sorunlara yol açtığını,

- Kayıtlara ulaşma ve yedekleme konusundaki yetkilerin belirli kişilere özgülenmek suretiyle sınırlandırılması gerektiğini,

- Dinleme ve izleme cihazlarının ithalatı, internet üzerinden satışı ve reklamlarının yapılması konularında ilgili kuruluşlarca tanımlama ve düzenleme işlemlerinin yapılması ve özellikle bu cihazların ithalatıyla ilgili ihtisas gümrüklerinin hayata geçirilmesi gerektiğini,

- İngiltere’dekine benzer şekilde, özellikle kamusal alanlarda kullanılan kamera sistemlerinin MOBESE sistemine entegre edilmesi gerektiğini,

- Akıllı cep telefonlarına yönelik uygulamaların içine gizlenmiş bazı yazılımlar marifetiyle sıradan bir cep telefonunun bir izleme-dinleme cihazına dönüştürülebildiğini ve bu konuda birtakım önlemler alınması gerektiğini,

- Kamera kayıtlarının güvenli biçimde saklanması için network güvenliğinin sağlanmasının gerektiğini,

- Ülkemizde çeşitli ad ve unvanlar altında özel dedektiflik faaliyeti gerçekleştiren hatırı sayılır miktarda firma bulunmasına karşın, bu alanın hukuken düzenlenmemiş olmasının özel hayatın gizliliğinin ihlali niteliğinde birçok uygulamaya yol açtığını,

- Birçok Avrupa ülkesinde, yapı iskân ruhsatı alabilmek için erken uyarı sistemi projesi hazırlanmasının zorunlu hale getirildiğini,

- Bugün Avrupa’da nüfus ve ülke büyüklüğü itibarıyla en çok özel güvenlik görevlisi çalıştıran ülkelerden biri olmamıza karşın, ülkemizde güvenliğe yapılan yatırımın boş bir yatırım gibi görüldüğünü,

ifade etmişlerdir.