



1954

TMMOB ELEKTRİK MÜHENDİSLERİ ODASI

BİLGİ BELGE MERKEZİ(BBM)

Döküman Bilgileri

EMO BBM Yayın Kodu	: 2
Raporun Adı	: İletişim Özgürlüğüne Müdahale Raporu 2009
Raporun Yayın Tarihi	: 01/05/2009
Yayın Dili	: Türkçe
Raporun Konusu	: İletişim Özgürlüğüne Müdahale; Elektronik Gözaltı Dünyası
Raporun Kaynağı	: TMMOB Elektrik Mühendisleri Odası, e@gözaltı, ISBN 978-9944-89-733-4, Mayıs 2009
Anahtar Kelimeler	: iletişim özgürlüğü, elektronik
Yazar 1	: TMMOB Elektrik Mühendisleri Odası

Açıklama

Bu doküman Elektrik Mühendisleri Odası tarafından açık arşiv niteliğinde olarak bilginin paylaşımı ve aktarımı amacı ile eklenmiştir.

Odamız üyeleri kendilerine ait her türlü çalışmayı EMOP/Üye alanında bulunan veri giriş formu aracılığı ile bilgi belge merkezinde yer almasını sağlayabileceklerdir. Ayrıca diğer kişiler çalışmalarını e-posta (bbm@emo.org.tr) yolu ile göndererek de bu işlemin gerçekleşmesini sağlayabileceklerdir. Herhangi bir dergide yayınlanmış akademik çalışmaların dergideki formatı ile aynen yer almaması koşulu ile telif hakları ihlali söz konusu değildir.

Elektrik Mühendisleri Odası Bilgi Belge Merkezi'nde yer alan tüm bilgilerden kaynağı gösterilerek yararlanılabilir.

Bilgi Belge Merkezi'nde bulunan çalışmalardan yararlandığında, kullanan kişinin kaynak göstermesi etik açısından gerekli ve zorunludur. Kaynak gösterilmesinde kullanılan çalışmanın adı ve yazarıyla birlikte belgenin URL adresi (http://bbm.emo.org.tr/genel/katalog_detay.php?katalog=4&kayit=2) verilmelidir.

**TMMOB
ELEKTRİK MÜHENDİSLERİ ODASI**

**İLETİŞİM ÖZGÜRLÜĐÜNE
MÜDAHALE RAPORU (2009)**

**ELEKTRONİK
GÖZALTI DÜNYASI**

e-Göz@ltı

Elektrik Mühendisleri Odası Yayın No: GY/2009/3



TMMOB Elektrik Mühendisleri Odası

1954

İLETİŞİM ÖZGÜRLÜĞÜNE MÜDAHALE RAPORU (2009)

ELEKTRONİK GÖZALTI DÜNYASI

“e-Göz@ltı”

Yayıma Hazırlayan

TMMOB-Elektrik Mühendisleri Odası

(Tarkan ÖDEN, Birkan SARIKAFIOĞLU, Hayati KÜÇÜK, Banu SALMAN, Kahraman YAPICI)

Mayıs, 2009

EMO Yayın No: GY/2009/3

ISBN:978-9944-89-733-4

Adres

TMMOB-Elektrik Mühendisleri Odası

İhlamur Sokak No:10 Kat:2 06420 Kızılay/Ankara

Tel:(312) 425 32 72 Faks: (312) 417 38 18

e-posta: emo@emo.org.tr <http://www.emo.org.tr>

621.38928 ELE 2009

Elektrik Mühendisleri Odası

İletişim Özgürlüğüne Müdahale Raporu (2009):

Elektronik Gözaltı Dünyası/Elektrik Mühendisleri

Odası – Ankara:EMO,2009.

56 s.:şkl.:24 cm. (Elektrik Mühendisleri Odası Yayın No:

GY/2009/3

Elektronik Güvenlik--İnsan Hakları

Dizgi,Tasarım

TMMOB-Elektrik Mühendisleri Odası

Baskı

Hermes Ofset

Kazım Karabekir Caddesi Murat Çarşısı 39/16 06060 İskitler- Ankara

Tel: (312) 384 34 32

İÇİNDEKİLER

SUNUŞ

5

GİRİŞ

7

İKTİDARIN ELEKTRONİK GÖZLERİ

11

DİNLEME VE İZLEME YÖNTEMLERİ

14

TRAFİK İZLEME

14

KONUM BELİRLEME

17

İÇERİK TAKİBİ

19

İLETİŞİM ÖZGÜRLÜĞÜNÜN KORUNMASI VE İSTİSNASININ SINIRLARI

28

TCY'DE HABERLEŞME ÖZGÜRLÜĞÜNÜN İHLALİ SUÇLARI

34

İLETİŞİMİN DENETLENMESİNE YÖNELİK YASAL DÜZENLEMELER

37

İLETİŞİMİN DENETLENMESİNDE GÖREVLİ BİRİMLER

42

NASIL VE NELER YAPILMALI?

49

SOSYOLOJİK AÇIDAN TEKNOLOJİ ODAĞINDA GÜNCEL SORUNLARIN YORUMLANMASI

Prof. Dr. Aytül KASAPOĞLU- Araş. Gör. Yonca ODABAŞ

51



SUNUŞ

İnternet'in dünya genelinde yaygınlık kazanması ile mekan kavramı bir anlamda ortadan kalkmış, kıtalararası iletişim ve bilgi transferi bir tuşa basmaktan ibaret hale gelmiştir. Teknolojideki bu gelişmelerden toplumlar pozitif anlamda yararlandıkları gibi, baskı, korku ve sindirme yöntemlerini olağan bir politikaya dönüştüren, özgür ve demokratik yaşam biçimini içselleştirememiş ülkelerde ise; teknolojik sistem ve cihazlarla temel hak ve hürriyetlere müdahale yaşam kültürü haline dönüştürülmeye çalışılmaktadır. Bununla birlikte; suç örgütleri de, gelişen bu teknolojiyi yakından takip ederek, hem kazançlarını arttırmakta, hem de geleneksel suç tiplerinin dışında yeni suç tiplerini de geliştirmektedirler. Küreselleşmenin kirliliği ve karanlık yüzü olarak tanımlayabileceğimiz bu gelişmeler toplumsal huzuru, barışı ve güvenliğimizi ciddi bir şekilde tehdit etmektedir.

Telefon ve diğer iletişim cihazları ile hayatın her alanında dinlenen, takip edilen, ortam dinlemelerine maruz kalan ve kayıt altına alınarak fişlenen yurttaşlarımız, özgür ve demokratik bir biçimde yaşam hakkını kullanamamaktadırlar. Ne yazık ki özel yaşamın gizliliğine yapılan bu müdahaleye sistem seyirci kalmaktadır. Ülkeyi yöneten siyasi karar vericilerin direktifleri; yasaları hiçe saymakta ve çağdaş hukuk anlayışına gölge düşürmektedir. Yakın tarihimizde 22 Temmuz 2007 genel seçimleri öncesinde özel bir talimatla tüm yurttaşların, sivil toplum kurumlarının, özel ve tüzel kişilerin haberleşmesinin tespit ve kayıt altına alınmasına ilişkin karar ile Türkiye'de temel hak ve özgürlükler yerle bir edilmişti.

Suçlu ile suçsuzu birbirinden ayırmaya özen gösteremeyen ve ülkede yaşayan yurttaşlarımızın büyük bir bölümünü şüpheli konumunda gören 12 Eylül uzantılı anlayışın artık kendisiyle yüzleşmesi, anti demokratik uygulamalara ve fişlemelere son vermesi gerekmektedir.

Milyonlarca yurttaşın haberleşme ve özel yaşamının ihlalinden hiçbir sıkıntı duymayan ve adeta korku imparatorluğu

yaratan siyasi iktidar, özel yaşama ve haberleşmeye saygıyı düzenleyen Anayasa'nın 13. ve 22. maddelerine, Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesi'nin 17. Maddesi'ne, İnsan Hakları Avrupa Sözleşmesi'nin 8. Maddesi'ne ve Ceza Muhakemeleri Usulü Kanunu'nun 135. Maddesi'ne, genel gerekçesine aykırı hareket ederek elektronik haberleşme alanında keyfi uygulamalar ortaya koymaktadır. Dinleme ve izleme kayıtları öyle bir düzeye ulaşmıştır ki, pek çok konuşma ve içerik çarşaf çarşaf İnternet ve basın ortamında yayınlanabilmektedir.

Sözde yasal izinlerle gerçekleştirilen ancak insan hakları temel hak ve hürriyetlerini ihlal eden bu tip uygulamaların engellenmesine ilişkin herhangi bir düzenlemenin bulunmaması; demokratik hukuk devleti olduğumuz iddiası ile çelişmektedir. Çağdaş hukuk düzenlemelerinde temel yaklaşım, sosyal düzenin korunması ile bireyin temel hak ve özgürlüklerine saygı arasında bir denge kurulması suretiyle gerçeği ortaya çıkarmak ve adil yargılama ilkesine uyarak adil yaptırımlar uygulamaktır.

Kamunun özgürce kullanabileceği güvenli haberleşme hakkı; yasal güvence altına alınmalıdır. Bu konudaki hak ihlallerinin önüne geçilmesi ve güvenlik açıklarını giderecek düzenlemelerin ivedi olarak hayata geçirilmesine ihtiyaç bulunmaktadır.

Kamu kurumu niteliğinde bir meslek örgütü olarak, uzmanlık alanımıza giren elektronik alanındaki teknolojik gelişmelerin yaşam içerisinde kullanımı ve yarattığı sorunlara ışık tutabilmek amacıyla; teknik, hukuki ve sosyal boyutunu gözeterek, kamuoyunu bilgilendirmek üzere bu rapor çalışması yapılmıştır. Raporumuza sosyolojik değerlendirmeleriyle katkıda bulunan Prof. Dr. Aytül Kasapoğlu ve Araştırma Görevlisi Yonca Odabaş'a teşekkürlerimizi sunarız.

ELEKTRİK MÜHENDİSLERİ ODASI
41. DÖNEM YÖNETİM KURULU
Mayıs 2009

GİRİŞ

Son dönemde çokça tartışılır olan telefon ve ortam dinlemenin teknik, hukuki, sosyal ve ekonomik olmak üzere birkaç boyutu bulunmaktadır. Teknolojinin gelişimine paralel olarak iletişim ve bilgiye erişim hem hızlanmakta, hem kolaylaşmakta ve giderek maliyetleri de azalmaktadır. Ne yazık ki bu gelişmeler, toplumun her kesimi için eşit bir şekilde iletişim ve bilgiye erişim olanağı sağlayamadığı gibi bilgi kirliliğinden iletişim özgürlüğünün yok edilmesine uzanan bir yığın tartışma içerisinde yeni teknolojilerin sorgulanmasını beraberinde getirmiştir.

Tarihsel olarak bakıldığında, jurnalcilik, muhbirlik, sansür gibi pek çok kavramla ele alınan konuların bugün telekulak, kocakulak, otosansür gibi ifadelerle kamuoyunda yaygın şekilde yer tuttuğu, neredeyse toplumsal paranoyanın yaşandığı bir dönemdeyiz.

Kapitalist sistemin temelini oluşturan karın dönüş sürecini kısaltma arayışları teknolojinin de hızla metalaşarak yaygınlaşmasını sağlamaktadır. Ancak bu yaygınlaşma pek çok yararlarla birlikte sorunu da beraberinde getirmektedir. Teknolojinin hangi amaçla kullanıldığı ise can alıcı noktayı oluşturmaktadır. Örneğin İnternet insanların bilgiye erişimlerini oldukça kolaylaştırıcı bir araç olmuşken, kelime bazlı arama motorları günümüzde bilgiye erişimin temel kaynaklarından biri konumuna gelmişken; diğer yandan bu bilgilerin güvenilirliği, doğruluğu giderek daha fazla sorgulanmaktadır.

Bugün cep telefonları, İnternet üzerinden elektronik posta haberleşmesi, anlık ileti gönderimini sağlayan servisler, sanal iletişim grupları gibi çeşitli sosyalleşme ağları, insanların kişisel ve toplumsal iletişiminde temel araçlar haline gelmişlerdir. Bu iletişim araçlarının gün geçtikçe artan kullanımı; insanların teknolojinin gelişimine paralel olarak iş ve ev yaşamlarında görülen değişikliklerin toplumsal iletişim ortamına bir yansıması olarak değerlendirilebilir. Elbette bu gelişmelerin insanların iletişim

olanaklarını kolaylaştırdığı söylenebilir. İnsanların toplumsallaşma süreci açısından ayrıca sorgulanabilir olan bu araçların yarattığı olanakların yanında önemli ölçüde kısıtlayıcı etkileri bulunmaktadır. Kişilerin telefon konuşmalarında, anlık ileti ve e-posta yazışmalarında kendilerine otosansür uyguladıkları, bazı konularda konuşmaktan ve yazmaktan çekindikleri, dolayısıyla iletişim ortamı içerisinde iletişimsizlik denilebilecek bir sürecin yaşandığı görülmektedir.

Yargı kararıyla ülkedeki tüm insanların telefon görüşmelerinin izlenmesine izin verildiğinin ortaya çıkması kamuoyunda geniş tepki uyandırırken, kaygıları da artırmıştır. Son olarak dönemin Adalet Bakanı Mehmet Ali Şahin, 21 Nisan 2009 tarihinde bir milletvekilinin soru önergesi üzerine, resmi olarak suç unsuruna rastlanmadığı için dinleme kayıtları imha edilen kişi sayısının son 3 yılda 12 bin 858 olduğunu açıklamıştır. Ceza Muhakemeleri Yasası'na dayanılarak iletişim tespiti, sinyal bilgileri değerlendirme, görüşmeleri dinleyip kaydetme uygulaması yapılmış olup, kovuşturmaya gerek olmadığı için kayıtları imha edilen kişi sayısında 2007 yılında bir önceki yıla göre yüzde 83, 2008 yılında ise yine 2006 yılına göre yaklaşık yüzde 93'lük bir artış olduğu görülmektedir. Açıklanan verilere göre 2006 yılında 2 bin 699, 2007 yılında 4 bin 947, 2008 yılında ise 5 bin 212 kişi gereksiz yere dinlenmiş bulunmaktadır. Ceza Muhakemeleri Yasası'na göre kayıtların yok edilmesi durumunda en geç 15 gün içinde yapılan işlemin nedeni, kapsamı, süresi ve sonucu hakkında yazılı olarak bilgi verilmesi gerekmektedir. İller bazında 3 yıllık kayıtları imha edilen dinlemeler incelendiğinde en fazla sayıda kişi dinlemesinin nüfusun da yoğunluklu olduğu İstanbul'da gerçekleştiği görülmektedir. İstanbul'da dinleme kayıtları imha edilen kişi sayısı 1912 iken, Diyarbakır'da bu sayının 1718 ile oldukça yüksek olduğu saptanmıştır. Adana 1205 imha edilmiş dinleme sayısı ile üçüncü sırada yer alırken, Van 1096 ile dördüncü sırada, Mersin ise 978 ile beşinci sırada bulunmaktadır.

Gaziantep 449 ve Kilis 398, Bursa 312, İzmir 284 ile dinleme kayıtları imha edilmiş kişi sayısının yüksekliği açısından sıralamada ilk 15'a giren yerler olmuştur. Nüfusa göre imha edilmiş dinlemelerin yüksek olduğu yerler olarak da Sinop 362, Söke 337 ve Malatya 330 ile dikkat çekmektedir. Ankara'da kayıtları imha edilen 35 kişi dinlenmişken, küçük bir il olmakla birlikte Hakkari'de bu sayının 221 olduğu görülmektedir.

Yalnızca kayıtları imha edilen dinlemeler bildirilirken, bütün dinlemelerin sayısı açıklanmamıştır. Sözlü olarak yapılan açıklamalar, nüfusun binde 1'i düzeyinde yıllık dinleme ve kayıt yapıldığı yönündedir.

Dünya'da ve ülkemizde teröre karşı önlem ve güvenlik gerekçesiyle iletişim özgürlüğü başta olmak üzere çeşitli haklar ve özgürlükler kapsamında ciddi sınırlamalara başvurulduğu bir dönem yaşanmaktadır. Bu sınırlandırmalar kapitalist sistem içerisinde kar artırma yöntemleriyle birleştiğinde daha da genişlemektedir. Örneğin sokakları gözetleyen kamera sistemleri kurulmaktadır. Son olarak 1 Mayıs öncesinde DİSK Genel Merkez binasını gözetlemek üzere İstanbul Emniyet Müdürlüğü'nce mobil elektronik sistem entegrasyonu (mobese) kamerası yerleştirilmesi kamuoyunda tepki çeken uygulamalardan biri olmuştur. Okullar, toplu taşıma alanları, büyük alışveriş merkezleri başta olmak üzere pek çok kamusal mekan devasa gözetim sistemi içerisinde yer almaktadır. Alışveriş ve bankacılık işlemleri gibi günlük yaşama ilişkin faaliyetler sırasında elde edilen kişiye özel bilgiler, bu kişilerin isteği ya da bilgisi olup olmadığına bakılmaksızın yine ticari amaçlı olarak kullanıma açılmaktadır. Büyük alışveriş marketlerinin dağıttıkları kartlar, kredi kartlarıyla yapılan harcamalar üzerinden şirketler pazar araştırması ve yönlendirmesi yapabilmektedirler. İnternet'te hizmet veren arama motorları başta olmak üzere bazı siteler kişinin elektronik ortamdaki gezintilerini kaydedip analiz ederek, o kişilerin ilgi alanlarına uygun yönlendirmelerde bulunabilmektedirler. Böylece modern dünyanın insanları tüketim alışkanlıklarından, hobilerine, okudukları kitaplara, gittikleri yerlere,

katıldıkları etkinlik ya da grupların takibine kadar uzanan geniş bir izleme ağı içerisinde bulunmaktadır. İzleme dünyası küçük yaş gruplarına kadar yayılmakta, kreşlerdeki kamera sistemlerinden çocukların okuduğu kitapların kayıtlara geçirilmesine varıncaya dek uzanmaktadır. Artık kapitalist sistem içerisinde "fişlemenin" adı "performans ölçümü" olmuştur.

Türkiye'de 2008 yılsonu itibarıyla 17 milyon 502 bin 205 sabit telefon abonesi, 65 milyon 824 bin 110 cep telefonu abonesi, 6 milyonu aşkın geniş bant İnternet abonesi bulunmakta olup, 113 milyon kayıtlı cep telefonu vardır.

İnsanların teknolojik yeniliklerden yararlanabilmeleri için maddi anlamda eşit erişim olanaklarına sahip olmaları yanında teknolojinin getirdiği yenilikler, olanakları ve sınırları konusunda bilgi sahibi olmaları gerekmektedir. Bunun için teknoloji okuryazarlığı büyük önem taşımaktadır. Teknoloji gelişiminde geri kalmış bir ülke olarak teknolojik ürün pazarının ülkemizdeki gelişmişliği dikkate alındığında teknoloji okuryazarlığı konusunda ciddi adımlar atılması gerektiği ortaya çıkmaktadır. Bunun için başta okullar olmak üzere eğitim müfredatında yenilenmeye ihtiyaç bulunmaktadır. Okullar dışında halka yönelik olarak da teknoloji okuryazarlığını sağlayacak çözümler üretilmesi gerekmektedir. Bilgi ve iletişim teknolojilerinin tamamen pazar inisiyatifine bırakılmış olması tüm dünyada olduğu gibi Türkiye'de de kamunun bu alanda politika izlemesini engellemiştir.

Teknoloji okuryazarlığıyla birlikte teknoloji kullanımı etiğinin geliştirilmesi ise ayrıca üzerinde durulması gereken bir konudur. Nükleer teknolojinin insanların yaşamlarını tehdit eden değil, tıp vb. alanlarda insanlığın yararına hizmet edecek şekilde kullanılmasını savunmak gibi teknolojinin gelişimine yönelik olarak da etik değerlerin oluşturulması önemli görünmektedir. Aldous Huxley'in Cesur Yeni Dünyası'na mı, George Orwell'in 1984'üne mi gidiyoruz tartışması içerisinde insanlığın değerlerinin korunabildiği özgür bir dünya yaratabilmek için teknoloji etiği önemli bir kavram olarak karşımızda durmaktadır.

İKTİDARIN ELEKTRONİK GÖZLERİ

Günümüzde, teknolojinin ve buna bağlı olarak da kitle iletişim araçlarının baş döndürücü gelişimi, günlük yaşam üzerinde birçok kolaylıklar sağlamasına karşın; toplumsal, siyasal ve kültürel düzlemlerde çok boyutlu olarak tanımlanabilecek birçok sorunu da beraberinde getirmektedir. Genel olarak kapitalist üretim ilişkileri ile örgütlenmiş modern devlet biçimlerinde bilginin, egemen sınıf tarafından kendi iktidar yapısının tesisine dönük merkezleştirilmesi, toplumun denetimini sağlamak amacıyla dezenforme ya da manipüle edilmesi veya standartlaştırılarak tek yanlı olarak “rasyonalize” edilmesi ve tüm bu sürecin yönetilenler tarafından mutlak gerçeklik olarak aklanması, bu sorunlardan birkaçı olarak sıralanabilir. Buradan hareketle günümüzde iktidarlar, içinde yaşanılan toplumsal ve siyasal yapının yeniden üretimi için gerekli bilgiyi üretip taşıyacak “normal bireyler” (ya da özneler) ve aynı zamanda bu bireyleri kontrol altında tutacak kompleks disiplin, denetim ve gözetim mekanizmaları yaratmaktadırlar. Bundan dolayı bilgi ve teknoloji ile denetim/kontrol mekanizmaları sürekli değişiklik gösteren modern iktidarlar arasındaki ilişkinin çözümlenmesi önem arz etmektedir.

Modern İktidarın Çözülmesi

Geçmiş yüzyılın önemli filozoflarından biri olan Michel Foucault'a göre iktidar sadece, toplumun üstünde var olan ve zor mekanizmaları ile bireylerin disiplinini sağlayan ve fiziksel olarak doğrudan bireyi muhatap alan kompakt yapıdaki üstyapı kurumları değildir. Foucault'a göre iktidar; mikrolaşmış, şekilsiz, iç içe geçmiş karmaşık şebekelerden oluşan çok boyutlu bir yapıya sahiptir ve üstelik modernleşmeyle birlikte toplumun sosyal, zihinsel ve bedensel tüm ilişkilerine kadar sirayet etmiştir. Ve iktidar kendisini, ancak özneleş[tiril]miş “özgür” bireyler yaratarak mümkün kılmaktadır. İrasyonel ya da anormal olma potansiyeline sahip bireyi ise okul, aile, kışla, mahkeme, tımarhane, hapisane, hastane gibi rasyonel kurumlar aracılığıyla normalleştirmeye

çalışarak bir disiplin toplumu var etmektedir. Fakat bu disiplinler kurum ve teknikler, iktidarlar için kendilerini yeniden üretmede yeterli görülmemektedir; o nedenle mevcut yapının sürekliliğine ve bekaasına tehdit unsuru oluşturabilecek marjinal/muhafif öğelerin öncelikle gözetlenerek tespit edilmesi ve ardından kontrol altına alınması için bir denetim-gözetim toplumunun tesisine ihtiyaç duyulmaktadır.

Denetim-Gözetim

Denetim-gözetim paradigmasına göre modern iktidarlar, bireyi sistem içerisinde en verimli şekilde kullanabilmeyi amaçlarlar. Bireyi en verimli şekilde kullanabilmenin yolu ise onu; bedeni, ruhu ve tüm faaliyetleri ile bilinebilir, hesaplanabilir (istatistik verisi olarak) bir nesne haline getirmekten geçer. Zira modern çağda devlet tarafından künyesi tutulan birey, yeni kurum ve teknikler yoluyla gözetime tabi tutulmuş, sicil kayıtları yaratılarak fişlenip güncellenmiş, merkezileşmiş bilgi matrislerine (arşivleme) sürekli aktararak depolanmış ve depolanmaktadır. Buna göre modern iktidarın rasyonalize edilmiş tüm bilme ve beğeni biçimlerine kadar belirlenmiş ve standartlaşmış normların ve bunların taşıyıcısı olarak “özgür bireylerin” yeniden üretimi için her şey toplanmış olmaktadır. Bunun sonrasında da analiz edilerek yeniden şekillenen ilişki ve bilme biçimlerinin kitleselleşmiş teknolojik iletişim ağları (medya) ve bunları kullanan “özgür bireyler” ile tekrar topluma sunulması ve tekrar sınanmasını içeren “yinelemeli döngü”sü en verimli (karlı) yapıya doğru evrilmeye devam edecektir.

Yukarıdaki çözümlemelere dayanarak bu teknolojik temelli iktidar mekanizmaların neler olabileceğini görebilmek zor olmayacaktır. En ilkel yapıdaki donanın aygıtlarından (kamera, telefon, RFID dedektörler vb.); akıllı, öğrenen ve karar verebilen en gelişmiş teknolojiye donanım ve analitik yazılım teknolojilerinin (Yapay Zeka, Karar Destek Sistemleri vb.) entegre sistemlerine kadar toplumun bugün büyük bir kuşatmanın içinde olduğu aşıkardır. Gözetim ve denetim kaynakları olarak; sokak

kameraları, telefon, İnternet vb. araçlarla saptama ve veri toplama işlemleri, nüfus bilgi sistemleri, adli sicil bilgi sistemleri, adres bilgi sistemleri, hastane bilgi sistemleri vb. entegre sistemlerle kayıt altına alma işlemleri bir iktidar biçimi olarak devlet kurumları tarafından sürekli işletilerek verili yapı içerisindeki anormaller tespit edilip kontrol altına alınmaktadır. Buradan elde ettiği ampirik veriler doğrultusunda iktidar, bireyin (ya da öznenin) bedenini ve zihnini, mevcut üretim tarzının ihtiyaçlarına uygun düşecek bir şekilde kamuoyunun karşısına nüfus, sağlık, güvenlik ve eğitim politikaları şeklinde sunmaktadır.

Elbette ki teknolojik belirleyiciliğin hakim olduğu bir düzlemde bilgisahibi olanın iktidarsahibi olması anlamı çıkarılabilir. Dolayısıyla iktidarın denetim-gözetim paradigmasını modern devletin kurumsallaşmış yapılarından menkul görmek ve egemen sınıfın üretim tarzı ve ilişkilerinden yalıtılmak eksik bir çözümlene olacaktır. Sermayenin küreselleştiği günümüz küresel kapitalizm koşullarında şirketlerin birçoğu sermaye akışını gerçekleştirdiği ülkenin devlet aygıtının denetleyemeyeceği veri toplamadan analize, analizden karar vermeye hatta “özgür birey” tarafından henüz gerçekleşmemiş bir faaliyetin belirli risk oranları ölçüsünde öngörüsünü yapabilecek ileri teknolojik sistemlere sahiptir.

Tüm bu modern iktidar mekanizmalarının kuşatması altında nesneleşen bireyin özgürlüğünden, küreselleşen ve hizmet sektörüne evrilen endüstri toplumunun bir tezahürü olduğu görmezden gelinerek gündeme getirilen bilgi toplumu kavramının bir devrim olarak görülmesinden bahsetmek mümkün değildir. Siyasal, ekonomik, ideolojik iktidar biçimlerinin iç içe geçtiği günümüz kapitalist toplumunda şekillenen ve yeniden üretilen toplumsal ilişkilerin gün geçtikçe daralan ve sönümlenmeye başlayan sivil toplum alanının ve sivil toplumcu düşünce hareketlerinin genişlemesi ile düzenlenebileceği ve çözüme kavuşabileceği düşüncesinin hayat bulduğu zemini yitirmeye başladığı rahatlıkla söylenebilmektedir.

DİNLEME VE İZLEME YÖNTEMLERİ

Dinleme ve izleme olaylarını günümüzdeki teknolojik gelişmeleri de dikkate alarak 3'e ayırabiliriz:

- 1- Trafik takibi. (Kim, kiminle, ne zaman iletişim kuruyor?)
- 2- Konum belirleme. (Kim nerede bulunuyor, kiminle beraber bulunuyor?/Yer tespiti)
- 3- İçerik takibi. (Kim kime ne diyor?)

Nihai amaç açısından 3'e ayırdığımız dinleme ve izleme uygulamalarını, hangi araçla yapıldığına yönelik olarak ayrıca sınıflandırmak konunun teknik, hukuki ve sosyal boyutlarının anlaşılabilmesi için faydalı olacaktır.

1-TRAFİK İZLEME

İzleme kapsamında değerlendirilen bu uygulama temel olarak, 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. Emniyet Genel Müdürlüğü İstihbarat Daire Başkanlığı'nın (İDB) talebi üzerine Ankara 11. Ağır Ceza Mahkemesi, 25 Nisan 2007 tarih ve 2007/2084 karar sayısı ile Türkiye'deki tüm telefon, cep telefonu, internet vb. haberleşme araçlarının izlenmesi için yetki verdiğinin ortaya çıkması kamuoyunda büyük tepkiye neden olmuştur. Mahkeme kararına göre Telekomünikasyon İletişim Başkanlığı (TİB) 3 aylık dönem için izleme kayıtlarını anlık olarak Emniyet Genel Müdürlüğü İstihbarat Daire Başkanlığı'na iletmıştır.

Emniyet Genel Müdürlüğü İstihbarat Daire Başkanlığı'nın 3 ayda bir aldığı yeni kararlar ile izleme faaliyetlerini sürdürdüğü bilinmektedir. Diyarbakır 6. Ağır Ceza Mahkemesi'nin de benzer bir talep için MİT'e yetki verdiği ve 3'er aylık dönemlerde yeni kararlar ile MİT'in izleme faaliyetlerini sürdürdüğü ortaya çıkmıştır. Ancak Jandarma Genel Komutanlığı'nın 15 Kasım 2007 tarihinde

Ankara 11. Ağır Ceza Mahkemesi'nden aldığı aynı kapsamlı izleme yetkisi ise TİB'in itirazı ve Adalet Bakanlığı'nın başvurusu üzerine Yargıtay 9. Ceza Dairesi tarafından iptal edilmiştir.

Trafik takibi kullanılan araçlara göre farklı yöntem ve uygulamalar içermektedir.

a-Cep telefonları: Cep telefonu işletmecileri; kimin, kimi, ne zaman aradığı ya da kısa mesaj gönderdiği ve kiminle ne kadar süre konuşma yapıldığına ilişkin bilgiye sahip durumda olup, bu kayıtları istenildiği zaman Telekomünikasyon İletişim Başkanlığı'na (TİB) iletmektedirler. Bu kayıtların geriye dönük olarak en az 9 ay süreyle tutulduğu bilinmektedir. Dinleme ve izleme amaçlı olmasa bile cep telefonu işletmecileri faturalandırma yapabilmek ve fatura ayrıntısını kullanıcıya da iletmek üzere bu tür kayıtları zaten tutmaktadırlar. CD-R listeleri denilen bu kayıtlar üzerinden geriye dönük trafik takibi yapılabilmektedir. Bu uygulama, bir telefon numarasına sahip kullanıcıyı rahatsız eden aramaların tespiti gibi hukuki anlamda ve insanların iletişim özgürlüğünün korunması açısından gerekli görülmektedir. Bunun yanında cep telefonları ile trafik takibi, bazı şirketlerin çalıştırdıkları personele yönelik olarak daha kapsamlı yaptıkları dinleme ve izleme sistemleri içerisinde yer alan bir uygulamadır. Cep telefonları içindeki yazılımlarla gelen ve giden aramaların tespiti yapılabilmektedir. Ayrıca dinleme ve izleme olanağı sağlayan her türlü teknik, cep telefonları ile yapılan görüşme ve yazışmalara ilişkin olarak trafik takibi olanağı da sağlamaktadır.

Trafik takip bilgilerinin, cep telefonu işletmelerinde yetkili bulunmayan personel tarafından edinimi ve 3. kişilere aktarımı, aynı şekilde TİB bünyesinde yetkisiz kişilere ve 3. kişilere bu bilgilerin aktarımı yasadışı takip anlamına gelmektedir. TİB'in yasal talep doğrultusunda Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Milli İstihbarat Teşkilatı (MİT) için topladığı trafik kayıt bilgilerinin bu kurumların dışında kişi ve kurumlara aktarımı da yasadışı takip kapsamındadır.

b-Sabit telefon (Ev ve iş telefonları): Cep telefonlarında olduğu gibi sabit telefonla yapılan görüşmelerde de kimin, kimi, ne zaman aradığı, ne kadar süre konuştuğu gibi bilgiler tutulmakta ve istenildiğinde Telekomünikasyon İletişim Başkanlığı'na iletilmektedir. Personel sayısı fazla olan büyük şirketler, çalışanların kimleri aradığını takip amacıyla da bu tür trafik kayıtlarını tutan yazılımları dahili hatların bağlı olduğu şirket santralına yükleyebilmektedirler.

Türkiye'de tek sabit telefon şebeke altyapısına sahip olan Türk Telekom'un yarı hissesinden fazlasının özelleştirilmesiyle birlikte cep telefonu ve uzak mesafe telefon işletmecilerinin de kullandığı telekomünikasyon altyapısı kamudan özel sektöre bırakılmıştır. Sabit telefonlar üzerinden trafik takibi, eğer telefonda hafıza kartı varsa casus yazılımlar yüklenerek de 3. kişi ya da kişiler tarafından da yapılabilmektedir.

c-Bilgisayar üzerinden iletişim takibi: Pek çok teknik yöntem kullanılarak kişisel bilgisayarlar üzerinde yapılan İnternet gezintileri, e-posta trafiği, anlık ileti trafiği tespiti yapılabilmektedir. Bir kişinin İnternet üzerinden hangi siteyi, ne kadar süre ile ziyaret ettiği, kime e-posta gönderdiği, kimden e-posta aldığı, kiminle anlık ileti yoluyla temas kurduğunu tespit etmek üzere çeşitli yöntemlerle bilgisayarlara casus yazılımlar yüklenebilmekte ya da casus klavye, casus hafıza kartı, casus kablo gibi araçlar kullanılabilir. Bu uygulama işyerlerinde de personelin bilgisi dahilinde ya da dışında olarak şirket içinde kullanılan bilgisayarlarla bağlantılı ana bilgisayar işlevi gören sunucular aracılığıyla da yapılmaktadır. Yasal izleme talebi durumunda TİB, İnternet servis sağlayıcı şirketler aracılığıyla bilgisayar üzerinden gerçekleştirilen iletişim trafiğini İnternete çıkışı sağlayan IP (İnternet Protokol numarası) adresi üzerinden takip etmektedir.

d- Posta denetimi: Sanal ortamda değil, matbu ve el yazması şeklinde yapılan yazışmaların posta, kurye, kargo gibi gönderimlerinde; kimin, kiminle iletişim kurduğu tespiti uzun zamandır yasal ya da yasadışı olarak yapılabilmektedir.

2-KONUM BELİRLEME

İzlemek kapsamındaki min, 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. Küresel konum belirleme (GPS) aletleri, baz istasyonları, İnternet'e çıkışı sağlayan numara (İnternet Protokolü-IP), uydu ve uçaklar konum belirleme amacıyla kullanılmaktadır.

a- Küresel konum belirleme (GPS): Yer tespiti konusunda temel bir yöntem olarak görülmektedir. Düzenli olarak bilgi yollayan uydulardan oluşmuş bir ağdan radyo sinyalleri aracılığıyla bilgi alınarak yer tespiti yapılmaktadır. Askeri amaçlı ortaya çıkan bu teknoloji, 1980'lerden sonra sivil ve ticari olarak kullanılmaya başlanmıştır. Bu cihazlar, kişinin bilgisi olmadan arabasına, cep telefonuna yerleştirilebildiği gibi bilgisi dahilinde de kullanılabilir. Trafik belirleme yöntemlerinde olduğu gibi GPS aletlerini şirketler çalıştırdıkları personeli takip amacıyla da kullanılmaktadır. 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 hastaları, çocukların takibi gibi meşru amaçlarla kullanılabilen bu cihazların yasa dışı kullanımı da söz konusudur.

b-İnternet üzerinden yer tespiti: Bir İnternet kullanıcısının İnternet ortamında yaptığı faaliyetler üzerinden nerede bulunduğu tespit edilebilmektedir. Örneğin e-posta ya da anlık ileti gönderimi yapan bir kişinin İnternet'e çıkışı sağlayan numara (İnternet Protokolü-IP) tespit edilerek kişinin bulunduğu il belirlenebilmektedir. IP adresleri İnternet servis sağlayıcıları tarafından kullanıcılara tahsis edilmektedir. İnternet servis sağlayıcısı şirketler hangi IP adresini hangi müşterilerinin kullandığı bilgisine sahip durumda bulunmaktadır. TİB'in hakim kararıyla IP adreslerini izlemesi ve kullanıcılara yönelik yer tespiti yapma yetkisi vardır.

c-Telefon görüşmeleri üzerinden konum belirleme: Sabit telefonla yapılan aramalarda artık kimin aradığını gösteren elektronik aletler, telefonlar yaygınlaşmıştır. Gizli numaralar dışında kişilerin rahatlıkla kendilerini arayanların nerede olduğunu belirleme olanakları varken, gizli telefon numaraları için de yer tespiti yapılabilmektedir.

Cep telefonu kullanımında ise kişinin konumunu belirlemek üzere hangi baz istasyonundan trafiğin gerçekleştiği bilgisiyle yer tespiti yapılmaktadır. Eğer çok sayıda baz istasyonunun bulunduğu şehir merkezi gibi bir bölgeden arama yapılmışsa mahalle, semt, cadde, sokak, hatta bina gibi daha ayrıntılı bir yer tespiti de mümkün olmaktadır. Cep telefonu işletmecileri, ticari hizmet kapsamında bazı şirketlere araç takip sistemleri (fleet management-filo yönetimi) aracılığıyla görüşme ve konum takibi olanağı sağlamaktadırlar. Bunların dışında cep telefonu işletmecileri yasal bir talep olması durumunda konuşmanın yapıldığı yere ilişkin kayıt (lokasyon kaydı) tutmakta ve TİB'e bildirmektedirler.

d-İstihbarat uyduları ve uçakları: Özellikle askeri amaçlı olarak gökyüzünde yörüngeye yerleştirilmiş uydular aracılığıyla yeryüzündeki kişi ve tesislere ilişkin ayrıntılı görsel malzemeler ve çeşitli bilgiler edinilebilmektedir. İnsansız, küçük boyutlu, radara yakalanmayan uçaklarla da aynı uygulama gerçekleştirilmekte olup; bu uygulama daha çok gelişmiş ülkeler tarafından kullanılmaktadır. Uydu ve uçaklar aracılığıyla yapılan yer tespiti, arama-kurtarma gibi afet durumlarına ilişkin çalışmalarda da gündeme gelmektedir. Bu uygulamanın turizm, tanıtma vb. alanlarda ticari amaçlı olarak Google Earth, Virtual Earth gibi kapsamlı ve anlık bilgi iletmeyen biçimleri de bulunmaktadır.

3-İÇERİK TAKİBİ

Yazılı, sözlü ve elektronik ortamda gerçekleştirilen iletişim kapsamında içeriksel takip yapılmasına yönelik olarak değişik uygulamalar bulunmaktadır. Bu tür içerik takipleri yasal talepler dışında günümüzde teknolojinin hızla gelişmesi, İnternet'ten içerik takibi yapabilecek cihazlara erişim kolaylığı, düzenleme ve denetim yetersizliği nedeniyle kişilerin rahatlıkla gerçekleştirebileceği uygulamalara dönüşmüşlerdir. Teknolojik aletlerin gelişmişliğine paralel olarak içerik takibi teknolojileri de giderek karmaşıklaşmış, uzman olmayan kişilerin fark etmesinin mümkün olamayacağı bir noktaya ulaşmıştır. Fark edilmesi giderek zorlaşırken, uygulaması da ters orantılı olarak giderek kolaylaşmakta ve ucuzlamaktadır. Bu durum gelişen teknolojiden yararlanmak isteyenlerin eğitimi, yani teknoloji okuryazarlığının geliştirilmesi ihtiyacı ve hukuki önlemler yanında kullanıcı etiğini geliştirecek kültürel bir dönüşüm gerekliliğine işaret etmektedir.

Yasadışı dinlemeler santraldan, panodan, apartman girişinden, anten ve uydu aracılığıyla havadan yapılabildiği gibi lazer dinleme, casus yazılımlar, monitör dinleme, kablo dinleme, vakumlama, casus klavye gibi araç ve yöntemlerle de gerçekleştirilmektedir.

a- Yazılı iletişimde içerik takibi: En eski yöntem olarak yazılı iletişime yönelik içerik takibi halen yapılmaktadır. Matbu yazışmaların, el yazısı ile hazırlanmış mektup gibi metinlerin elde edilerek okunmasıdır. Halen bu uygulama örneğin cezaevlerinde ve askeriyede yapılmaktadır. Yasal bir talep olması durumunda da posta ile yapılan gönderimlerde uygulanan bir yöntemdir.

b-Sözlü iletişimde içerik takibi: Telefon konuşmalarının dinlenmesi ve ortam dinlemesi şeklinde gerçekleştirilmekte olup bunlara yönelik olarak çok çeşitli teknolojik yöntemlere başvurulmaktadır.

Yasal İçerik Takibi

Yasal olarak bakıldığında hakim kararı doğrultusunda TİB devreye girerek, cep telefonu ve sabit telefon işletmecilerinin altyapıları üzerinden telefon görüşmelerini kaydetmekte ve bu telefon şebekeleri ile TİB arasındaki arayüz üzerinden doğrudan aktarım gerçekleşmektedir. İstihbari amaçlı dinlemeler görüşmenin yapıldığı sırada doğrudan MİT'e aktarılırken, adli dinlemeler Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı'na aktarılmak üzere kaydedilmektedir. Bu kurumlar TİB'den kayıtları aradaki sistem üzerinden paketlenmiş şekilde alırken, TİB'in mahkemenin verdiği tedbir süresinin bitiminden itibaren 10 gün içinde bu kayıtları yok etmesi gerekmektedir.

TİB'in kuruluşuyla birlikte 23 Temmuz 2006 tarihinden itibaren MİT, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı tarafından yapılmış ve kayıtları bulunan sesler TİB'e aktarılmış ve dinlemeler temel olarak TİB aracılığıyla yapılmaya başlanmıştır. Hakim kararıyla yapılan bu dinlemelerde yasal dinleme kategorilerine aykırı bir karar olduğu düşünülüyorsa itiraz etmesi için TİB'e yetki verilmiştir. Ancak itiraz edilirken, dinleme işlemine de başlanmaktadır. İtirazın kabul edilmesi durumunda kayıtların yok edildiği, itirazın reddedilmesi durumunda ise kayıtların ilgili birime iletildiği belirtilmektedir. TİB, yaklaşık 2 yıllık süreç içinde 4 bin itirazda bulunduğunu ve yüzde 90 itirazın kabulü yönünde sonuç alındığını bildirmiştir.

TİB ve telefon şirketleri kelime bazlı tarama yaparak görüşme kaydı tutmadıklarını ya da kaydedilen görüşmelerin içeriği üzerinde herhangi bir işlem yapmadıklarını belirtmektedirler. Ancak bu kaydedilen görüşmelerin başka kişiler tarafından yasadışı olarak edinilemeyeceği anlamına gelmemektedir.

Denetim Sorunu

Teknik olarak cep telefonu işletmecileri, sabit telefon işletmecileri ve TİB bünyesinde dinleme yapabilir. TİB'in bu tür yasadışı dinlemeleri takip etme olanağı bulunmamaktadır. Bu anlamda yasa dışı dinlemelere karşı bir denetim söz konusu

değildir. Teknik olarak buna uygun altyapı da bulunmamaktadır. TİB'in ve telefon işletmecilerinin yalnızca kendi personeline yönelik bir denetimi söz konusu olabilmektedir. Bu denetim de dinlenmesi istenen numaranın hukuki olarak kayıt altına alınması zorunluluğu ve buradan gelen numaraya yönelik dinleme kaydı yapan kişilere yönelik denetimle sınırlı kalmaktadır. Bunun dışında telefon işletmecilerinin personele yönelik şifre, giriş yasağı, dinlemeye olanak veren komut kümelerinin kapatılması gibi denetimleri bulunmaktadır. Cep telefonu şirketleri dinleme konusunda tek çıkışı TİB'e verdiklerini, bunun dışında yapılan dinlemeleri teknik olarak fark edemediklerini belirtmektedirler.

Dinlemelere yönelik genel bir denetim ve incelemeden söz edilemezken, kişilerin şikayeti durumunda dinleme yapılıp yapılmadığına yönelik araştırma yapılabilmekte, bu da kesin dinleme yapıldığını göstermediği gibi yalnızca bir olasılık sunabilmektedir. Çünkü dinleme yapan kişi, iki kişinin konuşmasına 3. bir görüşme hattı olarak giriyor görüntüsü vermektedir. Bu nedenle TİB ya da telefon işletmecilerinin ancak bu tür görüşmelerinin yapıldığını belgelemeleri söz konusu olabilmektedir. Ancak bu belgeleme tarafların bilgisi dahilinde konferans yöntemiyle 3 kişilik bir görüşme yapıldığı olasılığını da içermektedir.

Dinlemenin Boyutları

Türkiye'de son zamanlardaki tartışmalarla paranoya düzeyine yükselen 70 milyon kişinin aynı anda dinlenmesi ise mevcut teknik altyapı ile mümkün değildir. Tüm görüşmelerin trafik takibinin yapılmasına uygun altyapı bulunmasına karşın, tüm görüşmelerin içerik takibinin yapılmasına uygun bir altyapı yoktur. TİB'in verdiği bilgiye göre yasal olarak yapılan dinlemeler nüfusun binde 1'i düzeyindedir. Özellikle dakika bazında aynı anda yapılan binleri aşan görüşmenin içeriğinin anlık olarak kaydedilip dinlenmesi mümkün değildir. Bu durum, seçilen kişilerin görüşmelerinin dinlenemeyeceği anlamına da kesinlikle gelmemektedir. Üstelik telefon görüşmeleri için yurtdışından

dinleme olanağı da teknik olarak mümkün görünmektedir. Özellikle sabit telefonda yurtdışından ithal edilen santrallara ithalatçı firmanın bağlanıp yönlendirme yapabilme olanağı bulunmaktadır. Cep telefonu işletmecileri santrallarına yurtdışından ithalatçı firmaların giriş olanağının bulunmadığını ifade ederlerken, ancak cep telefonu işletmecilerinin sabit telefon hatları ve uydu aracılığıyla görüşmeler yaptırdıkları dikkate alındığında bu aşamada dinlenmelerinin mümkün olduğu ortaya çıkmaktadır.

Cep telefonlarıyla birlikte daha çok tartışma konusu olan dinleme uygulamaları, sabit telefonlarda da daha bilindik yöntemlerle gerçekleştirilmektedir. Sabit telefonlar teknik olarak, santraldan, panodan, apartman girişinden yapılan bağlantılarla dinlenebilirler. Santral ve panodan girişlere karşı güvenlik önlemlerini telefon işletmecisi alırken, apartman girişleri görece daha zayıf noktaları oluşturmaktadırlar. Santraldan sokak başlarında görebileceğiniz telefon panolarına kadar olan bakır kablolar üzerinde herhangi bir müdahale olduğunda algılamaya yönelik olarak gaz basıncıyla kontrol sistemi bulunmaktadır. Bu sistem altyapı çalışmaları sırasında arıza gören yeri tespit etmek için de kullanılmaktadır. Telefon ahizesi veya kablosuna dinleme aparatı yerleştirilmesi de sabit telefonları dinlemek amacıyla uygulanan yöntemlerden biridir. Bu yöntem ortam dinleme için de kullanılabilir. Ayrıca yeni gelişen teknoloji ile birlikte hafıza kartı olan sabit telefonlara da dinleme amaçlı casus yazılımlar yüklenebilmektedir.

Casus Yazılımlar

Telefon görüşmelerine yönelik yasa dışı dinlemeler kapsamında en çok gündemde bulunan casus yazılım uygulamasıdır. Dinlemeye olanak sağlayan casus yazılımlar, birkaç yolla telefon kullanıcılarına ulaşmaktadır. En basit yöntem casus yazılımı içeren bir cep telefonunu kullanıcıya vermek ya da armağan etmektir. İkincisi cep telefonuna tamirat sırasında ya da kullanıcının haberi olmadan casus yazılımın yüklenmesidir.

Üçüncü yöntem ise kullanıcıya casus yazılım içeren bir dosya gönderimidir. Gönderilen müzik, resim gibi bir dosyayı kullanıcı kabul edip telefonuna indirirken, casus yazılım da görünmeden telefonda kurulumunu gerçekleştirmektedir. Casus yazılımlar öyle gelişmiş bir düzeye ulaşmıştır ki, kullanıcının telefonunda herhangi bir ışık, titreşim, menüde değişiklik, görüşme sırasında cızırtı gibi belirti göstermeksizin çalışabilmektedir. Java tabanlı uygulamalarla casus yazılım geliştiriminin çok daha kolay olduğu bilinmektedir.

Casus yazılımlar çok gelişkin özelliklere sahip olup, her türlü izleme, kayıt işini yapabilmektedir. Casus yazılımlar aracılığıyla, cep telefonundan yapılan görüşmeler aynı anda aktarılabilirdiği gibi kaydedilip paket halinde gönderimi de olanaklıdır. Kimin kiminle, ne zaman, ne konuştuğu; ne zaman hangi yazılı kısa ileti alımı ve gönderimi yapıldığı, cep telefonuna indirilen dosyalar, cep telefonundan yapılan İnternet erişimleri, bu çerçevede her türlü elektronik iletişim (e-posta, anlık ileti) içeriksel olarak takip edilebilmektedir. Hatta casus yazılımlar aracılığıyla sim kart değişiklikleri rapor edilmekte, cep telefonunun bulunduğu ortamdaki konuşmalar da dinlenmekte, kayıt altına alınabilmektedir. Casus yazılımlar işlevini yerine getirmesinin ardından kendini sistemden silmek üzere de programlanabilmektedirler.

Casus yazılımlar, ancak cihaz üzerinde ayrıntılı inceleme ile ortaya çıkarılabilirler. Bu incelemeler sonucunda casus yazılımın göndericisi konusunda fikre ulaşmak mümkün olmayabilir. Casus yazılımlar barındıran cep telefonları 200 YTL gibi oldukça düşük fiyatlara satışa sunulmaktadır. İnternet üzerinden alışveriş olanağıyla da kolaylıkla edinilebilmektedir.

Havadan Dinleme

Cep telefonu görüşmelerinin dinlenmesine yönelik olarak anten aracılığıyla havadan dinlemeler yapılabilmektedir. Belli bir mesafe içerisinde yapılan cep telefonu görüşmelerini havadaki GSM elektromanyetik dalgaları bir kodlama programıyla deşifre

ederek kaydetmektedirler. Antenlerin ciddi bir mesafede etkin olabildikleri ifade edilirken, bu cihazlarla bölge içindeki çok sayıdaki cep telefonu görüşmesi kaydı tutulabildiği gibi görüşmelere ilişkin olarak kelime bazlı kayıt tutulması olanağı da bulunmaktadır. Yani içinde belirli kelimeler geçen görüşmeler seçilerek bunun kaydı gerçekleştirilebilmektedir.

Cep telefonu görüşmelerinde kablo altyapısının bulunmaması durumunda baz istasyonları uydu bağlantısıyla ses aktarımını gerçekleştiriyor. Bu durumlarda uydu üzerinden de görüşmelerin dinlenme olanağı bulunmaktadır.

Ortam Dinleme

Böcek; cep telefonlarına yüklenen casus yazılımlar; lazer dinleme; vakumlama; mikrofonu olan bilgisayarlara yüklenen yazılımlar; casus kulaklık; sabit telefon, çiçeklik, saat gibi aletlere takılabilen aparatlar ile o ortamda yapılan konuşmalar dinlenip, kayıt edilebilmektedir. Minik boyutlarda görüntü alıcı ve aktarıcı kamera sistemleriyle de dinlemenin yanında görüntü kayıtları da yapılabilmektedir. Ortam dinleme amacıyla böcek gibi aparatların kullanımı oldukça bilindik bir yöntem olmakla birlikte cep telefonlarına yüklenen yazılımlar giderek gelişmiştir. Cep telefonlarının kapalı olması durumda bile çalışan ve ortamdaki konuşmaları aktaran sistemler geliştirilmiştir. Ortamda bilgisayar bulunması durumunda da yapılan konuşmaların dinlenme ve kaydedilme olanağı vardır. Bilgisayarlara yerleştirilecek aparatların yanı sıra bilgisayarlara yüklenen casus yazılımlarla da ortam dinlemesi yapılabilmektedir.

Vakumlama yönteminde çanağa benzer bir alet söz konusudur. Çanağın dinlenmek istenen yöne çevrilmesiyle çanaktaki mikrofonda toplanan ses dalgaları kaydedilmektedir. Açık alandaki konuşmaların dinlenmesi için kullanılacak bir sistemdir.

Lazer dinleme yöntemi ise çanağa benzer bir aletin yanında lazer tabancasının doğrultulduğu yerdeki sesin yaydığı titreşimlerin algılanması esasına dayanmaktadır. Bu yöntemde

Elektronik Ortamda

lazer ışığı içerdeki konuşmaların yaydığı ses dalgalarının pencere ve camdaki titreşimlerini algılayarak dinlemeyi yapana göndermektedir. Cihaz da lazerle dönen ışını ses dalgalarına dönüştürerek deşifreyi gerçekleştirmektedir. Uzak mesafeden kapalı bir alandaki konuşmayı dinlemek için uygun bir sistemdir.

Bu uygulamalar yasal bir talep doğrultusunda yapılabildiği gibi yasadışı dinlemelerde de yaygın olarak kullanılmaktadır. Cihazların alım-satımına yönelik olarak herhangi bir yasa bulunmamakta, İnternet üzerinden rahatlıkla edinilmesi mümkündür. Telefon ve elektronik ortama yönelik iletişimde gerçekleştirilen yasal dinleme ve kayıtlardan farklı olarak ortam dinleme de TİB devre dışıdır. Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve MİT kendi olanaklarıyla ortam dinleme faaliyetlerini sürdürmektedir.

c- Elektronik iletişimde içerik takibi: Elektronik ortamda gerçekleştirilen yazılı, sözlü ve görüntülü her türlü iletişim biçimine yönelik olarak içerik takibi yapılabilmektedir. Bilgisayar üzerinden elektronik ortamda gerçekleştirilen iletişimin içeriksel olarak takibi, casus yazılımlar, casus klavye, bilgisayarın kasasına, kablosuna takılabilecek kayıt aletleri ile yapılabilmektedir. Bunların yanında anten aracılığıyla bilgisayar ya da klavyede herhangi bir aparat olmadan uzaktan yapılan işlemleri algılayıp kaydeden sistemler geliştirilmiştir.

Bilgisayarda takip ve ele geçirmeye yönelik 49 farklı grupta kötücül yazılım olduğu belirtilmektedir. İnternet'ten çoğu ücretsiz edinilebilen 500'den fazla casus yazılım olduğu bilinmektedir. Casus yazılımların, kullanıcıya ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının haberi ve isteği olmadan alınıp üçüncü taraflara veya kötü niyetli kişilere aktarılmasını sağlayan yazılım türleridir. Tanımdan da anlaşıldığı gibi bu tür casus yazılımların bilgisayara yüklenmesiyle kişinin bilgisayar üzerindeki yazdığı her türlü yazı, gezindiği İnternet siteleri, gönderdiği ve aldığı e-postalar, yine gönderdiği ve aldığı anlık iletiler, İnternet üzerinde kullandığı şifreler, fare tıklamaları, bilgisayar

üzerindeki görüntüler elde edilip, başka bir yere aktarılmaktadır. Bilgisayarlara yüklenen bu tür yazılımlar örneğin bilgisayara giriş şifresinin elde edilmesinin ardından kendisini yok etmek üzere de programlanmış olabilmektedir. Bu tür casus yazılımlar, bankacılık işlemlerinde ya da şifreli girişlerin yapıldığı sitelerde kullanılan sanal klavyenin sağladığı güvenliği de aşarak şifreyi ele geçirebilmektedir.

Casus programlar aracılığıyla ekrandaki görüntülerin kaydı yapılabildiği gibi klavye tuşlarının hareketi de aktarılabilmektedir. Bilgisayardakamerabulunması durumundakameragörüntülerinin aktarımı da yapılabilmektedir. Bunların her biri için ayrı programlar bulunabileceği gibi tüm bu işlevleri yerine getiren yazılımlar da piyasada satılmaktadır. Bazı casus yazılımlar bu tür işlemler için bilgisayardaki bluetooth özelliği ile bağlantılı olarak aktarımı gerçekleştirmektedir. Kablosuz İnternet erişiminde güvenliğin zayıf olması durumunda da rahatlıkla herhangi bir bilgisayar üzerindeki verilerin edinimi mümkündür. Herhangi bir bilgisayar monitöründeki görüntüler, herhangi bir izleme aparatı ya da bağlantı olmaksızın belli bir mesafe içerisinde lazer yöntemiyle kopyalanabilmektedir.

Casus klavyeler, bilgisayar kasasına, klavyelere, klavye ile bilgisayar kasası arasındaki kabloya yerleştirilebilen aparatlar ile de casus yazılımların yapabildiği her türlü bilgi aktarımı yapılabilmektedir.

Butür yazılım ve aparatlar şirketler tarafından ana bilgisayara yerleştirilerek yapılabildiği gibi tek tek kişilerin bilgisayarlarına yerleştirilerek de kullanılmaktadır. Böylece çalışanların, hangi siteleri ziyaret ettiği, hangi sitede ne kadar süre kaldığı, kiminle ne yazdığı ve bilgisayarında yaptığı tüm veri girişlerini kontrol etmektedirler. ABD gibi ülkelerde şirketler tarafından yaygın olarak kullanıldığı bilinmektedir.

Elektronik ortamdaki iletişim yasal olarak yine TİB aracılığıyla takip edilmekte, kaydedilmektedir. Telefon dinleme durumunda olduğu gibi hakim kararı gerektirmektedir. Yasal olarak TİB'in

ELEKTRONİK GÜZALİH DÜNYASI

dışında elektronik ortamdaki verilere delil anlamında ulaşım da söz konusu olabilmektedir. Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı bünyesinde bilgisayarlar ve CD'lere el konulması da, TİB'in devrede olmadığı geçmişe dönük olarak elektronik ortamdaki iletişimin izlenmesini kapsayan bir uygulamadır.



İLETİŞİM ÖZGÜRLÜĞÜNÜN KORUNMASI VE İSTİSNASININ SINIRLARI

İnsanların maddi ve manevi varlıklarını geliştirebilmeleri, çeşitli hak ve özgürlüklere ne derecede sahip olduklarıyla orantılıdır. Sosyal bir varlık olarak insan, özgürce düşünebildiği, tasarladıklarını özgürce ifade edebildiği, yaşama geçirebildiği ölçüde yaratıcı ve üretici yeteneklerini ortaya koyabilir. Toplumlar da, refah ve mutluluklarını, ekonomik, sosyal, kültürel gelişimlerini bireylere tanınan özgürlükler üzerinden sağlarlar. Günümüzün gelişmiş toplumlarında, hangi ideolojik-politik sistem söz konusu olursa olsun, artık hak ve özgürlüklerin ön plana alındığı, önem verildiği bir aşamaya ulaşılmıştır. Farklı ekonomik ve politik sistem savunucuları, farklı sistemlerde de olsa, birey ve toplulukların özgürlüklerinin artırıldığı modellere vurgu yapmaktadırlar. Nitekim insanların kendilerini özgürce ifade edemedikleri toplumların, tarihsel gelişim içerisinde yıkılıp, yok oldukları ya da mutsuz ve perişan bir yaşama mahkum oldukları görülmektedir.

Kişi hak ve özgürlükleri, yaşam hakkından başlamak üzere, konut edinme, seyahat etme, çalışma, dilediği gibi iletişim kurma, düşündüklerini açıklama ve yayma gibi, insan iradesiyle gerçekleştirilebilecek her türlü hareket tarzının güvence altına alınmasını içermektedir. Bu özgürlükler, başta uluslararası sözleşmeler olmak üzere, ülkelerin anayasa ve yasalarıyla çeşitli düzeylerde koruma altına alınmaktadır.

İnsan hak ve özgürlükleri, kişilerin iradelerini serbestçe oluşturabilmeleri ve bu serbest iradeleri doğrultusunda hareketlerini, etkinliklerini yönlendirebilmelerini içermektedir. Dolayısıyla irade özgürlüğünün korunması, bu özgürlüklere yönelebilecek her türlü hareketin yasaklanmasını ve önlenmesini de beraberinde getirmektedir. Böylece sahip olunan özgürlüklere bir sınırlama getirilmiştir. Bu sınırlamalar, kişisel hakların korunmasını içerebileceği gibi, toplumun ortak

değerlerinin korunmasını da amaçlayabilmektedir. Toplum içerisinde kişilere kimi hak ve özgürlükler tanınması, anayasal ve yasal düzeyde, özellikle devlet organlarına belirli görev ve yükümlülükler getirilmesi anlamını taşımaktadır. Devlet tarafından yerine getirilecek yükümlülükler, öncelikle sahip olunan hak ve özgürlüklerin kullanılabilmesi için gerekli tedbirlerin alınmasını gerektirmektedir.

İletişim Çağında Özgürlüklerin Anlamı

İçinde yaşadığımız çağ, teknolojide yaşanan gelişmeler nedeniyle, iletişim çağı olarak da adlandırılmaktadır. İletişimin ulaştığı boyut, dünyamızı adeta şeffaflaştırmış ve yaşam tarzına etki edecek gelişmelere neden olmuştur. Dünyanın en ücra köşelerine kadar yayılan fiberoptik kablolar ve son derece gelişmiş uydular aracılığıyla, neredeyse her dakika naklen yayın yapan sayısız televizyon kanalıyla dünya ayaklarımıza kadar ulaşırken, bilgisayar ve İnternet'in gelişimi ve yaygınlaşması, bu alanda tek tek bireylerin aktör haline geldiği sosyal diyalog ortamı yaratmıştır. Cep telefonları üzerinden her türlü iletişimin sağlanabilir olması ise haberleşmenin her türlü mekandan bağımsızlaşmasını beraberinde getirmiştir.

İnternet ortamının yarattığı sınırsız olanaklar, kişileri zorunlu olarak içerisine çeken, onsuz olmaz bir yapıya neden olmuştur. Kişilerin bir anda meşhur olabildikleri, onbinlerce kişinin birkaç saat içerisinde sokağa dökülmesine aracı olabilen, topluma mal olmuş kişilerin dahi bu ortamdaki uzak kalmaları halinde tanınmaz olduğu yeni bir toplumsal yaşam alanı ortaya çıkmıştır.

İletişim alanında yaşanan bu gelişmeler, kişi hak ve özgürlükleri içerisinde ön sıralarda yer alan haberleşme özgürlüğüne yeni bir boyut ve anlam kazandırmıştır. Bu yeni ortam, yeni davranış biçimlerini olduğu kadar, yeni suç biçimlerini ya da devletler açısından yeni denetim biçimlerini de gündeme getirmiştir. Mevcut hukuk kurallarının, bu yeni yaşam alanları üzerinden yeniden ele alınarak, kişisel hak ve özgürlüklerin korunmasının yeni yol ve yöntemlerinin gündeme alınması

kaçınılmaz olmaktadır.

Oysa kişisel özgürlüklere ilişkin hukuksal düzenlemeler, halen eski kavram ve kuralların bir miktar revize edilmesinin ötesinde yenilenmemektedir. Bu durum, bir yandan kişisel ya da toplumsal mağduriyetler yaratacak başıboşluk doğururken, diğeryandan bu durumla mücadele adına toptan yasakçı uygulamalara neden olabilmektedir. Hukuk alanında ortaya çıkan yetersizlik, yalnızca yeni iletişim olanakları açısından kimi olumsuzlukların değil, diğer hak ve özgürlüklerin de adeta kullanılamaz hale geldiği ortam yaratmaktadır. Kişisel sır olarak görülecek her türlü bilginin zorunlu olarak teknolojik araçlar üzerinden paylaşıldığı günümüzde, bu iletişim ortamlarına başkaları tarafından ulaşılmasının da son derece kolay hale gelmesi nedeniyle, insanlar kendilerine sansür uyguladıkları bir pasifiğe sürüklenmektedir.

Türkiye'de İletişim Özgürlüğü

İletişim özgürlüğü açısından ülkemizin sahip olduğu hukuksal düzenlemeler de son derece yetersiz kalmaktadır. Son yıllarda kimi yeni yasal düzenlemeler yapılmış olmakla birlikte, iletişim güvenliğinin sağlanamadığı, bu alandaki toplumsal kaygıların en üst safhaya ulaştığı bir süreç yaşıyoruz. Gerek ülkemizin de taraf olduğu Avrupa İnsan Hakları Sözleşmesi'nde, gerekse Anayasamızda özel hayatın ve haberleşmenin gizliliğine vurgu yapılmış ve hangi durumlarda, hangi organlar eliyle, nasıl istisnaların uygulanacağı da kesin bir şekilde belirlenmiştir. Ancak gizliliği korumaya yönelik tedbirler almakla görevli resmi makamların ortaya koyduğu kimi uygulamalar, bizzat kamu görevlilerince gizliliğin ihlal edildiği kuşkularını doğurmakta ve toplumda bir otosansür mekanizmasının işlemesine neden olmaktadır. Toplumda giderek artan bu kuşkulara yol açan uygulamaların önüne geçilmesine yönelik herhangi bir adım atılmamakta, aksine daha da derinleşmesine neden olacak açıklamalar yapılabilmektedir.

Yasalar çerçevesinde yapılan ve belirli suçların işlenmesinin önlenmesine ya da suç delillerinin toplanmasına yönelik

ELKTRONİK GÜZALTI DÜNYASI

dinlemelerin amacından sapmış olması kuşkularının yanı sıra kimi dinleme kayıtlarının özellikle İnternet gibi iletişim araçları üzerinden servis edildiğine tanık olunmaktadır. Bu dinlemelerin yalnızca resmi görevlilerce yapılmadığı, sivil unsurların da teknolojinin getirdiği olanaklarla yaygın dinleme yapabildiği görülmektedir. Hukuk dışı dinlemelere karşı etkin bir hukuksal mücadele yürütülmemesi ve suç teşkil eden bu fillerin artması, iletişim güvenliğinin yok olması sonucunu doğuracaktır. Bu nedenle, öncelikle yasalarla kendilerine yetki verilmiş olan görevlilerin amacını aşan uygulamalarının ortadan kaldırılmasına yönelik etkin tedbirlerin alınması gerekmektedir.

İletişimin hukuk dışı dinlenmesinin önlenmesiyle ilgili olarak, suçtan mağdur olan kimselerin yapabilecekleri son derece sınırlıdır. Nitekim iletişimin dinlenmesi de gizli yapılmaktadır ve genellikle mağdurun suçtan haberdar olması söz konusu değildir. Ancak iletişim kayıtlarının yayınlanmasıyla suçtan haberdar olunabilmektedir. Bu aşamada ise failin suçtan beklediği yarar gerçekleşmiş olacağından, uygulanacak bir yaptırımın da önemi kalmayabilmektedir. Özellikle ticari ya da mesleki sırların elde edilmesi gibi gizlilik ihlallerinde kayıtların yayınlanması söz konusu olmadığından, mağdurun da suçu öğrenme olanağı bulunmayacaktır.

Nitekim Anayasa'nın "Temel hak ve hürriyetlerin korunması" başlıklı 40. Maddesi'nde, "Anayasa ile tanınmış hak ve hürriyetleri ihlal edilen herkes, yetkili makama geciktirilmeden başvurma imkanının sağlanmasını isteme hakkına sahiptir" denilmiştir. Dolayısıyla devletin, kişilerin özel hayatlarının gizliliğine ve dokunulmazlığına yönelecek her türlü ihlale karşı kişilerin başvuru yollarını kolaylaştırıcı önlemleri almak zorunluluğu bulunmaktadır.

Yine Anayasa'nın 40. Maddesi'nin son fıkrasında "Kişinin, resmi görevliler tarafından vaki haksız işlemler sonucu uğradığı zararda, kanuna göre, Devletçe tazmin edilir. Devletin sorumlu olan ilgili görevliye rücu hakkı saklıdır" denilmiştir. Bu hüküm

doğrultusunda, özel sırları ve iletişimi hukuka aykırı olarak resmi görevliler tarafından dinlenen, kayıt altına alınan ya da ifşa edilen kişilerin uğradıkları maddi ve manevi zararların tazminini devletten isteme hakkı bulunmaktadır.

İletişimin gizliliğinin ve bu gizliliğin ihlal edilmesinin sınırları, Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesi'nde şu şekilde yer almıştır:

“Madde 8- Özel hayatın ve aile hayatının korunması

1. Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2. 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 koşuluyla söz konusu olabilir.”

Haberleşme Özgürlüğü Anayasal Hak

Türkiye Cumhuriyeti Anayasası'nın “Haberleşme hürriyeti” başlıklı 22. Maddesi'nde ise “Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır” denilerek, kişilerin birbirleriyle özgürce iletişim kurmaları teminat altına alınmıştır. Haberleşmenin gizliliğinin esas olması, yurttaşlara bu alanda bir dokunulmazlık anlamına gelirken, devlete de bu dokunulmazlığın gereğinin yerine getirilmesi görevi yüklenmiştir. Haberleşme özgürlüğünün kısıtlanması ya da takip altına alınmasına yönelik her türlü girişimin, yasal düzenlemelerle ve kamu gücü kullanılmak suretiyle engellenmesi, tüm kişi özgürlüklerinin korunmasında olduğu gibi, devletin temel sorumlulukları arasındadır. Dolayısıyla bu alanda yapılacak düzenlemelerin, öncelikle haberleşme özgürlüğünün gereği gibi kullanılmasına yönelik tedbirleri içermesi gerekmektedir.

Anayasa'nın 22. Maddesi'ndeki düzenlemenin devamında, bu temel özgürlüğün hangi amaçla ve nasıl kısıtlanacağına yönelik istisnaya yer verilmiştir. Buna göre; “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 hakim onayına sunulur. Hakim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.”

Haberleşme özgürlüğünün gizliliğinin ihlali, ancak ve istisnai olarak Anayasa ile koruma altına alınan milli güvenlik, kamu düzeni, genel sağlık, genel ahlak ya da yurttaşların hak ve özgürlüklerinin korunması gibi değerlerin ihlal edilmesini önlemek amacıyla söz konusu olabilir ve bunun da devletin görevli organları aracılığıyla yapılabileceği öngörülmüştür. Bu istisnanın kişi hak ve özgürlüklerini zedelemekten kullanılabilmesi amacıyla da, yasama ve yürütme organlarının güçlerini dengeleyen yargı organının karar ve denetimi altında gerçekleşmesi Anayasa hükmü olarak güvence altına alınmış ve usulüne ilişkin ayrıntılı bir anlatıma yer verilmiştir.

Ayrıca Anayasa'nın “Temel hak ve hürriyetlerin sınırlanması” başlıklı 13. Maddesi'nde, yurttaşlara tanınan bütün anayasal hak ve özgürlüklerin sınırlandırılmasında uyulacak esaslara yer verilerek; “Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz” denilmiştir. Buna göre, haberleşme özgürlüğünün gizliliği esasına istisna teşkil edilecek uygulamaların yapılması, 22. Madde'de belirtilen amaçlarla sınırlı ve 13. Madde'de belirtilen usullerin dışına taşmadan olacaktır. Haberleşme özgürlüğünün gizlilik esasının zorunlu olarak ihlal edilmesinde, bu anayasal hakkın

kullanılmasını ortadan kaldıracabilecek aşırı uygulamalar da kesin olarak yasaklanmıştır.

Anayasa'nın 22. Maddesi'ndeki haberleşmenin gizli olacağı esası ile bu duruma getirilen istisnalar birlikte değerlendirildiğinde, kişilere hak olarak tanınan ve öncelikle gözetilmesi gereken hususun, "gizlilik ilkesinin korunması" olduğu görülmektedir. İstisna olarak getirilen haberleşmenin engellenmesi ya da gizliliğinin ortadan kaldırılması, haberleşme özgürlüğüne feda edilecek değerde bir başka hak ve özgürlüğün ya da kamu düzeninin ihlal edilmesinin önlenmesi amacıyla ve gerektiği ölçüde ancak ilgili yargı merciinin kararıyla gerçekleştirilebilir.

TCY'DE HABERLEŞME ÖZGÜRLÜĞÜNÜN İHLALİ SUÇLARI

5237 sayılı Türk Ceza Yasası'nın (TCY) 2. Kitap 2. Kısmı'nın "Hürriyete Karşı Suçlar" başlıklı 7. Bölümü'nde yer alan 124. Madde'nin başlığı "Haberleşmenin engellenmesi" şeklindedir. TCY, haberleşmenin engellenmesi suçuna, düzenlendiği bölüm ve düzenleniş şekli itibariyle, Anayasa'da olduğu gibi kişi hak ve özgürlükleri arasında yer vermiştir. 124. Madde'nin 1. Fıkrası'na göre; "Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adli para cezasına hükmolunur."

Haberleşmenin Gizliliğini İhlal

Haberleşmenin gizliliğinin ihlali, TCY'nin "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı, 2. Kitap, 2. Kısmın, 9. Bölümü'nde yer alan 132. Madde'de düzenlenmiştir. Maddenin 1. Fıkrası'nda "Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur" denilmiştir. Buna göre, "kişiler arasındaki iletişimin dinlenmesi suretiyle gizliliğin ihlali" suçun basit şeklini, dinlemenin ötesine taşarak, "iletişimin içeriğinin kayıt edilmesi" ağırlaştırıcı şeklini oluşturmakta ve cezanın ağırlaştırılması öngörülmektedir.

Maddenin diğer fıkralarında başkaca ağırlaştırıcı nedenlere de yer verilmiştir. 2. Fıkra'da, haberleşmenin gizliliğini ihlal eden kimsenin elde ettiği verileri ifşa etmesi halinde, bir yıldan üç yıla kadar olması öngörülmüş; dördüncü fıkrada ise haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması halinde cezanın yarısı oranında artırılacağı düzenlenmiştir.

Kendileriyle yapılmış olan haberleşmeleri, karşı tarafın rızası olmaksızın alenen ifşa eden kişilerin eylemi de, gizliliğin ihlal edilmesiyle aynı suç oluşturmuştur.

Maddede anılan haberleşme, posta, telefon, telgraf, faks ya da bilgisayar gibi tüm haberleşme araçları üzerinden yapılacak iletişimleri içerir.

Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması

Haberleşmenin gizliliğinin ihlali yanında, TCY'nin 133. Maddesi'nde, ortam dinlemesi olarak da bilinen, "kişiler arasındaki konuşmaları dinlemek ve kayda almak" suç olarak tanımlanmıştır. Buna göre; dinleme yapılan kişilerin konuşmaları aleni olmayacak, dinleme ve kayda alma kişilerin rızası dışında gerçekleşecek ve fail konuşmaları herhangi bir aletle dinleyecek ya da ses alma cihazına kaydedecektir. Bu suç için iki aydan altı aya kadar hapis cezası öngörülmüştür.

Aynı maddede, kişilerin katıldıkları aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan kayda alan kişinin de cezalandırılması hüküm altına alınmıştır. Böylece yalnızca kişiler arasında basit haberleşme değil, topluluk halinde düşüncelerini paylaşma özgürlüğü de teminat altına alınmıştır.

Bu maddede düzenlenen fillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini sağlayanlar da cezalandırılacaktır.

Özel Hayatın Gizliliği

TCY 134. maddesinde kişilerin özel hayatının gizliliğini ihlal edenlerin cezalandırılacağı düzenlenmiştir. Gizlilik ihlalinin görüntü

ya da seslerin kayda alınması suretiyle gerçekleşmesi ile bunların ifşa edilmesi ağırlaştırıcı bir neden olarak belirtilmiştir. Böylece haberleşmenin ve kişiler arasındaki konuşmaların gizliliğinin ihlalinin yanında, "özel hayatın ihlali" ayrı bir suç tipi olarak ceza yasasında yer almıştır.

Kişisel Verilerin Kaydedilmesi

TCY 135. Madde, hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verileceğini öngörmüş ve kişilerin siyasi, felsefi veya dini görüşlerine; ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine; cinsel yaşamlarına; sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimselerin de, aynı hükme göre cezalandırılacağına yer vermiştir. 136. Madde'de ise, "kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması ya da ele geçirilmesi" ayrı bir suç olarak tanımlanmış ve daha ağır bir ceza öngörülmüştür. Bu maddelerde tek tek sayılan veriler dışında yer alan ve kişilere ait veri olarak kabul edilecek her türlü bilgi madde kapsamında değerlendirilmelidir. Özellikle kamu görevlileri tarafından, fişleme olarak anılan ve kişilere atfedilen kimi özelliklerin hukuka aykırı bir şekilde kayıt altına alınması madde kapsamındadır. Bu bölümde yer alan diğer suçlarda olduğu gibi, kişisel verilerin kaydedilmesinde de, failin kamu görevlisi olması halinde, cezanın yarısı oranında artırılarak uygulanması söz konusudur.

Şikayet

TCY 139. Madde "Şikayet" başlığını taşımakta, bu maddede "kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme" suçları dışındaki suçların soruşturulmasının ve kovuşturulmasının şikayete bağlı olduğu belirtilmiştir. Böylece haberleşmenin gizliliğinin ihlali başta olmak üzere, kişilerin özel hayatlarına yönelik gizlilik ihlallerinin faileri hakkında soruşturma yapılması ve yargılanabilmeleri için, suçtan mağdur olanların şikayette bulunmaları zorunludur. Suçtan mağdur olanların şikayeti olmaksızın, savcıların kendiliklerinden

harekete geçerek, suçun faili hakkında cezai takip başlatması olanağı bulunmamaktadır.

İLETİŞİMİN DENETLENMESİNE YÖNELİK YASAL DÜZENLEMELER

Anayasa'nın 22. Maddesi'nde yer alan haberleşmenin gizliliği ilkesinin istisnasına yönelik usul ve esaslara ilişkin genel düzenleme 5271 sayılı Ceza Muhakemesi Yasası'nda (CMY) yer almıştır.

CMY 135. Madde'de, "Bir suç dolayısıyla yapılan soruşturmalarda, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkanının bulunmaması durumunda, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir ve kayda alınabilir" denilmiştir. Bu maddeyle iletişimin dinlenmesinin sınırları belirlenmiş ve kararın yargı yerlerince verilmesi öngörülerek güvenceye kavuşturulmuştur. Uygulamada iletişimin dinlenmesi yolu, CMY'de belirlenen kuvvetli şüphe sebepleri ve başka suretle delil elde edilmesi imkanının bulunmaması sınırlamasının aşılması, kimi olaylarda yalnızca dinleme kayıtlarına dayanılarak dava açıldığı görülmektedir. Oysa dinleme kayıtlarının tek başına bir delil oluşturması adil yargılama açısından sakınca doğurabileceği gibi, yasayla belirlenmiş durumların dışına taşan, yaygın dinleme yapılması sonucuna da götürmektedir.

Nitekim yasalarla kendilerine dinleme yetkisi verilmiş olan kimi kurumlara, bütün yurttaşları dinlemeye yönelik genel kararlar çıkartıldığı kamuoyuna da yansımış bir gerçektir. 135. Madde'nin 3. Fıkrası'nda, dinleme kararının içereceği hususlar açıkça belirtilmiştir. Buna göre "Birinci fıkra hükmüne göre verilen kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespiti imkan veren kodu, tedbirin türü, kapsamı ve süresi belirtilir. Tedbir kararı en çok üç ay için verilebilir; bu

süre, bir defa daha uzatılabilir." Düzenlemeden de anlaşılacağı gibi, dinleme kararı, belirli bir kişiye yönelik olacak, ilgiliye yüklenen suçun türü, iletişim aracının bütün özellikleri, tedbirin türü, kapsamı ve süresi açıkça kararda belirtilecektir. Bu hükme aykırı olarak alınmış genel dinleme kararları hukuken geçersiz sayılacak ve herhangi bir yargılama sırasında delil olarak da kullanılamayacaktır. Bu hukuki gerçeğe rağmen çıkartılan genel dinleme kararlarıyla yapılan dinlemelerin, Anayasa ve yasayla belirlenmiş kamusal yararların dışında, kimi hukuka aykırı yorum nedeniyle olduğu düşünülmektedir.

Kimlerin İletişimi Dinlenemez

CMY'nin 135. Maddesi'nin 2. Fıkrası'nda, şüphelinin tanıklıktan çekinebilecek kimselerle yaptığı iletişimin kayda alınamayacağı düzenlenmiştir. Buna göre şüphelinin nişanlısıyla, evlilik bağı kalmasa bile eşiyle, kanyada kayın hısımlığından altsoyu ve üstsoyuyla, üçüncü derece dahil kan veya ikinci derece dahil kayın hısımlarıyla, aralarında evlatlık bağı bulunanlarla sağlanan iletişim kayda alınmaz ve delil olarak da kullanılamaz. Ayrıca meslek ve sürekli uğraşları nedeniyle tanıklıktan çekinebilecek olanlarla kurulan iletişim de bu kapsamda dinlenemeyecektir. Bu kapsamda avukat veya stajyerlerinin veya yardımcılarının; hekimler, diş hekimleri, eczacılar, ebeler ve bunların yardımcılarını; diğer bütün tıp meslek veya sanatları mensuplarının; mali işlerde görevlendirilmiş müşavirler ve noterlerin bu sıfatları dolayısıyla hizmet verdikleri kişilerle olan mesleki iletişimleri yer almaktadır.

İletişimin Tespit ve Kayda Alınabileceği Suçlar

CMY'nin 135. Maddesi, iletişimin tespit ve kayda alınabileceği suçları saymak suretiyle sınırlamıştır. Burada sayılanların dışındaki suçlar açısından tespit ve kayda alma işlemi yapılamayacağı gibi, yargılamalarda delil olarak da kullanılamaz. Bu suçlardan TCY'de yer alan "göçmen kaçakçılığı ve insan ticareti, kasten öldürme, işkence, cinsel saldırı, çocukların cinsel istismarı, uyuşturucu veya uyarıcı madde

imal ve ticareti, parada sahtecilik, suç işlemek amacıyla örgüt kurma, ihaleye fesat karıştırma, rüşvet, suçtan kaynaklanan mal varlığı değerlerini aklama, silahlı örgüt veya bu örgütlere silah sağlama, devlet sırlarına karşı suçlar ve casusluk" olarak 13 suç tipi sayılmıştır. Ayrıca, Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Yasa'da tanımlanan silah kaçakçılığı (Madde 12) suçları, Kaçakçılıkla Mücadele Yasası'nda tanımlanan ve hapis cezasını gerektiren suçlar ile Kültür ve Tabiat Varlıklarını Koruma Yasası'nın 68 ve 74. maddelerinde tanımlanan suçlarla ilgili olarak da dinleme ve kayda alma tedbirleri uygulanabilecektir.

135. Madde'nin son fıkrasında ise, "Bu maddede belirlenen esas ve usuller dışında hiç kimse, bir başkasının telekomünikasyon yoluyla iletişimini dinleyemez ve kayda alamaz" denilerek, dinleme ve kayda almayla usulün kesin sınırları belirlenmiş olmaktadır.

CMY'nin 137. Maddesi'nin birinci fıkrasına göre; iletişimin tespit ve kaydına yönelik "verilecek karar gereğince 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; yerine getirilmemesi halinde zor kullanılabilir. İşlemin başladığı ve bitirildiği tarih ve saat ile işlemi yapanın kimliği bir tutanakla saptanır."

2. Fıkra'ya göre, "karar gereğince tutulan kayıtlar, Cumhuriyet Savcılığınca görevlendirilen kişiler tarafından çözümlenerek metin haline getirilir. Yabancı dildeki kayıtlar, tercüman aracılığı ile Türkçeye çevrilir."

3. Fıkra'ya göre, "kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hakim onayının alınamaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhal son verilir. Bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç on

gün içinde yok edilerek, durum bir tutanakla tespit edilir.”

4. Fıkra'ya göre ise, “tespit ve dinlemeye ilişkin kayıtların yok edilmesi halinde, en geç on beş gün içinde, Cumhuriyet Başsavcılığı, tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgisine yazılı olarak bilgi verir.”

CMY'nin 138. Maddesi'nde ise tesadüfen elde edilen delillere yer verilmiştir. Buna göre, “arama veya el koyma koruma tedbirlerinin uygulanması sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhal bildirilir. Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ve ancak, 135. maddenin altıncı fıkrasında sayılan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhal bildirilir.”

Postada El Koyma

CMY'nin 129. Maddesi, suçun delillerini oluşturduğundan şüphe edilen ve gerçeğin ortaya çıkarılması için soruşturma ve kovuşturmada adliyenin eli altında olması zorunlu sayılıp, posta hizmeti veren her türlü resmi veya özel kuruluştaki bulunan gönderilere, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararı ile el konulabileceğine hükmetmiş ve bu uygulamanın usulüne ilişkin ayrıntıları düzenlemiştir.

Teknik Araçlarla İzleme

Ortam dinlemesi olarak adlandırılan teknik takiplere, CMY'nin 140. Maddesi'nde yer verilmiştir. Maddede “(1) Aşağıdaki suçların işlendiği hususunda kuvvetli şüphe sebepleri bulunması ve başka suretle delil elde edilememesi halinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir:

a) Türk Ceza Kanununda yer alan;

1. Göçmen kaçakçılığı ve insan ticareti (madde 79, 80),

2. Kasten öldürme (madde 81, 82, 83),
 3. Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188),
 4. Parada sahtecilik (madde 197),
 5. Suç işlemek amacıyla örgüt kurma (iki, yedi ve sekizinci fıkralar hariç, madde 220),
 6. İhaleye fesat karıştırma (madde 235),
 7. Rüşvet (madde 252),
 8. Suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282),
 9. Silahlı örgüt (madde 314) veya bu örgütlere silah sağlama (madde 315),
 10. Devlet Sırlarına Karşı Suçlar ve Casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337), Suçları.
 - b) Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (madde 12) suçları.
 - c) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar.
 - d) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74 üncü maddelerinde tanımlanan suçlar.
- (2) Teknik araçlarla izlemeye hakim, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından karar verilir. Cumhuriyet savcısı tarafından verilen kararlar yirmidört saat içinde hakim onayına sunulur.
- (3) Teknik araçlarla izleme kararı en çok dört haftalık süre için verilebilir. Bu süre gerektiğinde bir defaya mahsus olmak üzere uzatılabilir.
- (4) Elde edilen deliller, yukarıda sayılan suçlarla ilgili soruşturma ve kovuşturma dışında kullanılamaz; ceza kovuşturması bakımından gerekli olmadığı takdirde Cumhuriyet savcısının gözetiminde derhal yok edilir.
- (5) Bu madde hükümleri, kişinin konutunda uygulanamaz.” denilmiştir.
- Buna göre, kişiler hakkında, yukarıda belirtilen suçlarla sınırlı

olmak üzere, başka yollarla delil elde etme olanağı bulunmaması halinde, ilgilinin yalnızca kamuya açık yerlerdeki ya da işyerindeki faaliyetleri izlenecek, ses ve görüntüleri kayda alınabilecektir. Şüphelinin kişisel alanı olan konutundaki faaliyetlerinin bu yolla takip edilmesi kesin olarak yasaklanmıştır ve bu tür bir ortamda yapılan kayıtların delil olarak değerlendirilmesi söz konusu değildir.

Verileri Yok Etmeme Suçu

TCY'nin 138. Maddesi "Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediğinde altı aydan bir yıla kadar hapis cezası verilir" hükmünü taşımaktadır. Buna göre, yukarıda belirtilen usullere göre kayıt altına alınan iletişim bilgilerinin, suç unsuruna rastlanmaması gibi nedenlerle yok edilmesi gerektiği halde, bunları süresi içerisinde yok etmeyen kamu görevlilerine uygulanacak yaptırım belirlenmiştir. Bu suçun takibi şikayete bağlı değildir. Cumhuriyet savcılarının, böyle bir suçun oluştuğunu tespit etmesi halinde, ilgilinin şikayeti olup olmamasına bakmaksızın soruşturma başlatması ve failin cezalandırılması istemiyle dava açması gerekmektedir.

İLETİŞİMİN DENETLENMESİNDE GÖREVLİ BİRİMLER

İletişimin denetlenmesiyle ilgili olarak çeşitli yasalarla çeşitli kurum ve kişilere yetki verilmiştir. 2559 sayılı Polis Vazife ve Selahiyet Yasası'nın Ek 7. Maddesi'ne göre polis, Ceza Muhakemesi Yasası'nın casusluk suçları hariç, 250. Maddesi'nin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla, hakim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişimi tespit edebilir, dinleyebilir, sinyal bilgilerini değerlendirebilir, kayda alabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, 24 saat içinde yetkili ve görevli hakim onayına sunulur. Hakim, kararını en geç 24 saat içinde verir. Sürenin dolması veya

hakim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde 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.

Hakim tarafından verilecek kararda ve yazılı emirde, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tesbite imkan veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenler belirtilir. Kararlar, en fazla 3 ay için verilebilir; bu süre aynı usulle 3'er ayı geçmeyecek şekilde en fazla 3 defa uzatılabilir. Ancak terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hakim 3 aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir.

İstihbarat faaliyetlerinde, bu maddede belirtilen suçların önlenmesi amacıyla ve hakim kararı alınmak koşuluyla, teknik araçlarla izleme de yapılabilir.

Bu madde hükümlerine göre polis teşkilatı tarafından yürütülen faaliyetler çerçevesinde elde edilen kayıtlar, maddede belirtilen amaçlar dışında kullanılamaz. Elde edilen bilgi ve kayıtların saklanması ve korunmasında gizlilik ilkesi geçerlidir. Elde edilen kayıt ve bilgileri başka amaçlarla kullananlar ve gizlilik ilkesini ihlal edenler hakkında, görev sırasında ve görevden dolayı işlenmiş olsa bile Cumhuriyet savcılarınca doğrudan soruşturma yapılır.

Polis teşkilatına verilen bu yetkiler, 2803 sayılı Jandarma Teşkilatı, Görev ve Yetkileri Yasası'nın Ek 5. Maddesi'yle Jandarma Teşkilatı'na ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Yasası'nın 3. Maddesi'yle MİT'e de verilmiştir. Polis ve Jandarma Teşkilatı'na verilen dinleme yetkisiyle ilgili TCY hükümleri incelendiğinde, bu suçların özel görevli ağır ceza mahkemelerinin alanına giren örgütlü suçlarla sınırlı olduğu görülmektedir. MİT'in dinleme ve kayıt tutma görevi ise, devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması

ve devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesi gibi daha geniş bir alanı kapsamaktadır.

Telekomünikasyon İletişim Başkanlığı

2559 sayılı Polis Vazife ve Selahiyet Yasası'nın Ek 7. Maddesi'nde, gerek bu yasa gerekse CMY 135. Maddesi kapsamında yapılacak dinlemelerin, Telekomünikasyon Kurumu bünyesinde, Kurum başkanına doğrudan bağlı Telekomünikasyon İletişim Başkanlığı adıyla kurulan tek bir merkezden yürütülmesi hüküm altına alınmıştır.

Telekomünikasyon İletişim Başkanlığı'nda dinlemeyle görevli kurumlar olan Milli İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı'nın ilgili birimlerinden birer temsilcinin bulundurulması öngörülmüştür.

Telekomünikasyon İletişim Başkanlığı'nın kuruluş, görev ve yetkileri, Başbakanlık tarafından yürürlüğe konulan ve 10 Kasım 2005 tarihli, 25989 sayılı Resmi Gazete'de yayımlanan Yönetmelik ile düzenlenmiştir.

Yönetmelik Telekomünikasyon İletişim Başkanlığı'nın görevlerini şu şekilde belirlemiştir:

a) 2559 sayılı Kanunun ek 7. maddesi, 2803 sayılı Kanunun ek 5. maddesi ve 2937 sayılı Kanunun 6. maddesi uyarınca, telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına yönelik iş ve işlemleri tek bir merkezden yürütmek.

b) 5271 sayılı Kanunun 135. maddesi kapsamında yapılacak iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine yönelik iş ve işlemleri tek bir merkezden yürütmek.

c) (a) ve (b) bentleri kapsamındaki taleplerin 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 Milli İstihbarat Teşkilatı Müsteşarlığına, Emniyet Genel Müdürlüğüne

ve Jandarma Genel Komutanlığına, talep etmeleri halinde mahkemeye ve Cumhuriyet başsavcılıklarına iletmek.

e) Bu Yönetmelik çerçevesinde yapılacak tespit, dinleme, sinyal bilgilerinin değerlendirilmesi ve kayda alınması faaliyetlerini olanaklı kılacak her türlü teknik altyapının, 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) 11 inci maddenin üçüncü fıkrası, 12. maddenin ikinci fıkrası ile 15. maddenin üçüncü fıkrası saklı kalmak kaydıyla, Başkanlık faaliyetleriyle ilgili olarak kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşlar ile işletmecilerden gelen her türlü bilgi, belge ve kayıtların bilgi güvenliği kriterlerine uygun olarak arşivlenmesini sağlamak.

g) Görev alanına giren konularla ilgili mevzuatta ulusal ve uluslararası alanda meydana gelen gelişmeleri takip etmek.

h) Başkanlık faaliyetleri için yurt içinden ve yurt dışından teminine ihtiyaç duyulan her türlü malzeme, sistem, yazılım ve donanımı belirleyerek Kurum Başkanına bildirmek.

i) Başkanlık faaliyetleriyle ilgili olarak talep ettiğinde derhal Başbakana bilgi vermek.

j) Kanunlarla verilen diğer görevleri yerine getirmek."

Yönetmeliğe göre, iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi yönünde usulüne uygun olarak alınan kararlar, Cumhuriyet Savcısı veya görevlendireceği adli kolluk görevlileri tarafından Başkanlığa iletilir. Kararlar işletmecilere gönderilmez, ilgili kurum görevlileri ve Başkanlık çalışanları aracılığıyla teknik uzmanın nezaretinde yerine getirilir. İşlemin başladığı ve bitirildiği tarih ve saat ile işlemi yapanın kimliği bir tutanakla saptanır.

Kayıtların yok edilmesi işlemleri, özel görevli ağır ceza mahkemesi nezdindeki Cumhuriyet Savcısının denetimi altında en geç on gün içinde yok edilerek durum bir tutanakla tespit

edilir.

Anayasa Mahkemesi Kararı

Telekomünikasyon İletişim Başkanlığı ile ilgili düzenlemeler, 3 Temmuz 2005 tarihli ve 5397 sayılı Yasa ile yapılmış, bu Yasa'yla getirilen hükümler 2559, 2803 ve 2937 sayılı yasalara eklenmiştir. Daha sonra 4 Mayıs 2007 tarih ve 5651 sayılı Yasa ile yapılan değişikliklerle son haline kavuşmuştur. 5397 sayılı Yasa ile yapılan düzenlemede yer verilen kimi ibare ve tümceler, Cumhurbaşkanı Ahmet Necdet Sezer ile 116 milletvekili tarafından ayrı ayrı iptal istemiyle Anayasa Mahkemesi'ne götürülmüştür.

Anayasa Mahkemesi 2005/85 E. 2009/15 K. Ve 29.01.2009 tarihli kararıyla, Yasa'da yer alan kimi ibare ve tümcelerin iptaline karar vermiştir.

5397 sayılı Yasa, iletişimin tespit ve dinlenmesiyle ilgili faaliyetlerin denetimini, sıralı kurum amirleri, Emniyet Genel Müdürlüğü ve ilgili bakanlığın teftiş elemanları ve Başbakanın özel olarak yetkilendireceği kişi veya komisyon tarafından yapılmasını öngörmüş, Anayasa Mahkemesi ise, "Başbakanın özel olarak yetkilendireceği kişi veya komisyon" ibaresini Anayasa'ya aykırı bularak iptal etmiştir.

İptal gerekçesi şu yoruma dayandırılmıştır:

"Anayasa'nın 128. Maddesi'nde 'Devletin, kamu iktisadî teşebbüsleri ve diğer kamu tüzelkişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği asli ve sürekli görevler, memurlar ve diğer kamu görevlileri eliyle görülür. Memurların ve diğer kamu görevlilerinin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülükleri, aylık ve ödenekleri ve diğer özlük işleri kanunla düzenlenir. Üst kademe yöneticilerinin yetiştirilme usul ve esasları, kanunla özel olarak düzenlenir' denilmektedir.

5397 sayılı Yasa'nın 1., 2. ve 3. maddelerinde telekomünikasyon yoluyla iletişimin yasada belirtilen usul ve esaslara uygun yapıp yapılmadığının denetimi Başbakanın özel olarak yetkilendireceği kişi ya da komisyona da verilmektedir.

Anayasa'nın kişinin dokunulmazlığı, maddi ve manevi varlığını koruma hakkına ilişkin 17., özel hayatın gizliliğinin korunmasına ilişkin 20., haberleşme hürriyetine ilişkin 22., düşünceyi açıklama ve yayma hürriyetine ilişkin 26. maddeleri gibi bir çok temel hak ve hürriyetle ilgisi olan denetim kapsamındaki faaliyetlerin, kamu düzeni ve kamu güvenliğine ilişkin olduğu, Devletin genel idare esaslarına göre yürütmekle yükümlü bulunduğu kamu hizmetlerinin gerektirdiği asli ve sürekli görevlerden olması nedeniyle memurlar ve diğer kamu görevlileri eliyle yürütülmesi gerektiği açıktır.

Anayasa'nın 128. Maddesi'nin birinci fıkrası kapsamındaki görevleri yürüten bütün personelin nitelikleri, atanmaları, görev ve yetkileri, hakları ve yükümlülüklerinin yasayla düzenlenmesi gerekir.

İptali istenilen ibarelerde telekomünikasyon yolu ile iletişimin tespitine dair faaliyetlerin denetimiyle görevli kılınan Başbakan tarafından yetkilendirilecek kişi ya da komisyon üyelerinin denetim yetkisinin gerektirdiği nitelikleri taşıyan kişiler arasından belirlenmesi gerekir. Bu ibareler, Başbakan tarafından yetkilendirilecek kişi ya da komisyon üyelerinin niteliklerini açık bir şekilde belirlemediğinden Anayasa'nın 128. Maddesi'ne aykırıdır.

Anayasa'nın 2. Maddesi'nde belirtilen hukuk devletinin temel unsurlarından birisi de hukuk güvenliğini sağlamasıdır. Hukuk güvenliği, kurallarda belirlilik ve öngörülebilirlik gerektirir. Belirlilik ve öngörülebilirlik özellikleri taşımayan ve dolayısı ile hukuki güvenlik sağlamayan kurallar Anayasa'nın Türkiye Cumhuriyetinin bir hukuk devleti olduğunu ifade eden 2. Maddesi ile bağdaşmaz. İptali istenilen kural takdire bağlı ve belirsiz bir yetki içerdiğinden hukuk devleti ilkesine de aykırıdır.

Açıklanan nedenlerle '...Başbakanın özel olarak yetkilendireceği kişi veya komisyon' ibareleri Anayasa'nın 2. ve 128. maddelerine aykırıdır. İptali gerekir."

5397 sayılı Yasa, "Telekomünikasyon İletişim Başkanı,

Telekomünikasyon Kurumu Başkanının teklifi üzerine Başbakan tarafından atanır” hükmünü getirmişti. Bu ibareyi de iptal eden Anayasa Mahkemesi, şu gerekçeye dayanmıştır:

“Anayasa'nın 8. Maddesi'nde 'Yürütme yetkisi ve görevi, Cumhurbaşkanı ve Bakanlar Kurulu tarafından, Anayasaya ve kanunlara uygun olarak kullanılır ve yerine getirilir' denilmekte, 104. Maddesi'nde de 'kararnameleri imzalamak' Cumhurbaşkanının yürütme alanındaki görev ve yetkileri arasında sayılmaktadır. Anayasa'nın 104. Maddesi'nde sözü edilen 'kararnameler', Kanun Hükmünde Kararnameler ile Bakanlar Kurulu'nun çeşitli kararnamelerinin yanında üst düzey yöneticilerin atanması ile ilgili müşterek kararnameleri de kapsamaktadır. Yürütme yetkisi ve görevi, Cumhurbaşkanı ve Bakanlar Kurulunca yerine getirileceğinden, söz konusu kararnamelerin hukuksal geçerliği için her iki tarafın da katılımı gerekmektedir.

Buna göre, kamu politikasının tayinine katılan, etkin bir otoriteye sahip olan, kuruluşların amacının gerçekleşmesinde önemli yetki ve sorumluluklarla donatılan, planlama, örgütlenme, personel ve kadrolarını yöneten, denetim ve temsil gibi işlevleri yerine getiren kamu görevlilerinin, üst düzey yönetici konumunda olmaları nedeniyle bunların atamalarının da müşterek kararname ile yapılması anayasal zorunluluktur. 5397 sayılı Yasa gereğince telekomünikasyon yolu ile iletişimin tespiti, 5651 sayılı Yasa'ya göre İnternet yoluyla yapılan yayınlara erişimin engellenmesi kararının verilmesi ve uygulanması konularında kamu düzeni ve kamu güvenliğiyle ilgili görevleri bulunan kurumun başkanlığını yürüten Telekomünikasyon İletişim Başkanının önemli yetki ve sorumluluklarla donatıldığı, bu nedenle üst düzey yönetici kapsamında bulunduğu ve atamasının da müşterek kararname ile yapılması gerektiği açıktır.

Açıklanan nedenlerle kural, Anayasa'nın 8. ve 104. maddelerine aykırıdır, iptali gerekir.”

NASIL VE NELER YAPILMALI?

- 1- Teknolojik gelişmelerin yararlar yanında yarattığı sıkıntıların çözümünde öncelikle özgürlükleri kısıtlayıcı değil, genişletici bir bakış açısıyla hareket edilmesi gerekir.
- 2- Anayasal güvenceye sahip iletişim özgürlüğünün korunması temel prensip olmalıdır.
- 3- İletişim özgürlüğüne zarar veren yasadışı dinleme ve izleme olaylarına karşı denetim yükümlülüğü öncelikle kamuya aittir. Buna yönelik denetim mekanizması ve altyapı sağlanmalıdır.
- 4- İletişim hizmetini sağlayan şirket ve kurumlara da iletişim özgürlüğünün korunmasına yönelik olarak sorumluluklar yüklenmeli ve gerekli denetim mekanizması kurulmalıdır.
- 5- Teknoloji kullanımı konusunda kamunun bilinçlendirilmesi gerekmektedir. Türkiye'de teknoloji okuryazarlığı yükseltilmelidir.
- 6- Dinleme ve izleme cihazlarının satışı, yurda girişi denetim altına alınmalı, kontrollü yapılmalıdır. Kaçak girişler önlenmeye çalışılmalıdır.
- 7- Casus yazılımlara karşı yasaklayıcı bir zihniyetin İnternet dünyasında geçerliliği yoktur. Bu nedenle bu tür yazılım kullanımlarına karşı öncelikle toplumda teknoloji etiğinin yerleştirilmesi önemlidir.
- 8- Casus yazılım gönderimini engelleyebilecek yazılımlar da cep telefonu satan şirketler, cep telefonu hizmeti veren şirketler ve kamunun ortak sorumluluğuyla yaygınlaştırılabilir.
- 9- Cep telefonlarına yüklenebilecek yazılımların kimliklendirilmesi ve insanların onay listesinde olmayan yazılımların o kullanıcıya gönderimini engelleyecek bir sistem kurulabilir.
- 10- Casus yazılımın var olup olmadığına ilişkin telefon kontrol hizmeti ve casus yazılımlara karşı anticasus program kurulum hizmeti verilmelidir. Yurttaşlara bu tür hizmetleri verecek kamusal birimler oluşturulmalıdır.
- 11- Anticasus yazılımların geliştirilmesi, casus programların indirilmesini engelleyici güvenlik duvarları yerleştirilmesi konusunda

TÜBİTAK kamu adına sorumluluk üstlenebilir.

12- Bedava cep telefonları ve bilgisayar alınmamalıdır.

13- İzleme ve dinlemeye karşı pasif odalar, frekans önleyici cihazlar kullanılabilir.

14- Anlık ileti gönderiminde ve İnternet üzerinde sesli görüşmelerde şifreleyerek konuşma ve mesajletimi gerçekleştiren sistemler tercih edilmelidir.

15- Cep telefonlarında da şifreleme yazılımları kullanılarak, dinlemeye karşı kişiler kendileri önlem alabilirler.

16- Ortam dinlemesi yapan cihazlar olduğundan şüpheleniyorsanız vericileri bulmak için geliştirilmiş aygıtlar edinebilirsiniz.

17- Bilgisayar kullanımında kişisel güvenliğinizi için almanız gereken temel önlemleri mutlaka sağlayın. Antivirüs yazılımları, güvenlik duvarları, şifreleme, yedekleme, geriye dönük izleme yapmayı engelleyecek şekilde güvenli silme yazılımları kullanın ve bu yazılımların güncellemelerini takip edin.

SOSYOLOJİK AÇIDAN TEKNOLOJİ ODAĞINDA GÜNCEL SORUNLARIN YORUMLANMASI

Prof. Dr. Aytül KASAPOĞLU -Araş. Gör. Yonca ODABAŞ
(Ankara Üniversitesi; Sosyoloji Derneği; SBE Enstitüsü)

Sosyolojinin önemli kavramlarından biri olarak “toplumsal değişme”nin temelinde iki itici gücü vardır. Bunlardan biri “nüfus” ikincisi ise “teknoloji”dir. Nitekim ilk çağ Filozofu Aristo’dan başlayarak ve ünlü Sosyolog Durkheim ile devam ederek, hemen hemen tüm sosyal düşünürler toplumsal değişimin ortaya çıkmasında artış ya da azalış halindeki nüfus hareketleri kadar, Gordon Childe’in işaret ettiği gibi teknolojinin etkisini kabul etmişlerdir. (Kongar,1979) Söz konusu teknoloji ise, basit alet/edevattan gelişmiş ileri bilgi/enformasyon teknolojilerine (IT) kadar uzanan geniş yelpazede ortaya çıkma potansiyeline sahiptir.

Öte yandan sosyal bilimlerin incelendiğinde, toplumsal değişmeye yol açarak insanları geleneğin boyunduruğundan kurtardığı ve dolayısıyla özgürleştirdiği için teknoloji genelde olumludur. Ancak, “negatif diyalektik” ile insanları hem özgürleştiren hem de bağımlı kılan özellikleri birarada taşıması yüzünden eleştirilmektedir. Bunun en güncel örneği medyanın hem iletişimi sağlaması hem de insanın düşünme/sorgulama yeteneklerini sınırlandırarak tek-düzeleştirilmesi, farklılıkları törpülemesi hatta giderek “yabancılaştırma”sıdır (alienation). İnsanların kendileri etraflarında olup bitenler hakkında yapacak birşeyleri olmadığını düşünmeleri (powerlessness); etraflarında olup bitenlere bir anlam verememeleri (meaninglessness); yapmaması gerekenleri sürekli yapar hale gelmeleri (normlessness); etrafları insanlarla dolu olduğu halde kendilerini yalnız hissetmeleri (social isolation) gibi yabancılaşma bileşenlerinin (Middleton,1963; Kasapoğlu;1999) tüm teknolojik gelişmelere rağmen insanlarda giderek yaygınlaşması diyalektik bir bakış açısıyla sosyolojinin teknolojiyi

sorgulamasına yol açmaktadır. Aslında diyalektik düşünce “Karşıtların Birliği” (Unity of Opposits) ilkesi uyarınca işlemekte ve formel/biçimsel mantığın, “özdeşlik”, “çelişmezlik”, “üçüncü seçeneğin olanaksızlığı” gibi ilkelerine meydan okumaktadır. Toplumsal yaşamda “İkili Karşıtlıklar”ın (Binary Opposits) aynı anda ve birlikte yaygın olarak bulunmasını formel mantık ile kavramak mümkün olmadığından, diyalektik düşünce, yöntemsel ve ussal olarak çok daha geniş olanaklar sağlayarak üstünlük kazanmaktadır. Kısaca bir teknoloji, örneğin cep telefonu aynı zaman aralığında yararlı ve/veya zararlı ya da kuşkulu özelliklere, diyalektik bakış açısına göre sahip olabilir. Nitekim günümüzdeki birçok durum, başta iletişim teknolojisindeki gelişmeler/sıkıntılar olmak üzere, böyledir.

Sosyolojinin teknolojiye ilgisine yönelik yazın incelendiğinde, tartışmaların önemli boyutlarda diyalektik özellikler taşıdığı gözlenmektedir. Örneğin Munir ve Jones (2004), belirli teknolojik icatların diğerlerine karşı olan üstünlüğü üzerine yaptıkları çalışmada, söz konusu baskınlığın, salt teknolojik etmenler ile açıklanamayacağı, analizlere teknolojik olmayan diğer etmenlerin –sosyopolitik dinamikler ve sponsor olan kişi, grup, organizasyon ya da kurumlar- dahil edilmesinin gerekliliğine vurgu yapmaktadır ve bu süreci açıklamada sıklıkla kullanılan beş temel yaklaşımdan bahsetmektedirler: Evrimsel Model (Arthur, 1994), Kurumsal Teori (Meyer ve Rowan, 1977), Sosyal Hareket Teorisi (Mueller, 1992), Yapılaşma Teorisi (Giddens, 1979) ve Aktör İlişkiler ağı Teorisi (Latour, 1987; Law, 1992). Söz konusu önerme, neden bazı teknolojik ürünlerin daha fazla tercih edildiği sorusuna da uyarlanabilir. Farklı bir deyişle, toplum içinde teknolojik ihtiyaçların belirlenmesinde etkili olan faktörlerin neler olduğunun ortaya çıkarılmasında benzer bir yaklaşım kullanılabilir. “Evrimsel Model”, söz konusu seçimin bütünü ile rastlantısal olduğunu ifade ederken, en güçlü olanın hayatta kalması görüşüne paralel olarak, en iyi teknolojik icadın daha baskın olacağını ileri sürmektedir. Diğer bir deyişle, teknolojik ihtiyaçların

belirlenmesinde kontrol edilemeyen, doğal bir seçiciliğe vurgu yapmaktadır. Teknolojinin sosyal ve politik faktörlerden bağımsız olduğunu ileri süren teknolojik determinizm ile benzer noktaları olan Evrimsel Model'e eleştirel bakan "Kurumsal Teori ve Sosyal Hareketler Teorisi" ise, bu süreç içindeki paydaşlar olarak sanayi ve politik sistemlere vurgu yapmaktadır. Kişiyi pasif olarak algılayan bu yaklaşımlara alternatif olan "Yapılaşma Teorisi" ise, ajan ile yapı arasındaki etkileşime dikkati çekmek istemektedir: Politik ve ekonomik yapı ihtiyaçların belirlenmesinde önemli rol oynarken, ajan olarak birey ya da farklı paydaşlar söz konusu gereksinimlerde değişiklik yapma potansiyeline sahip olabilirler. Burada dile getirilen teorilerin ortak özelliği, modernist düşüncenin temel özelliği olan "ikilik"ler(dualities) yaratma eğilimine sahip olmalarıdır. Her ne kadar Giddens(1984)'ın Yapılaşma Teorisi, söz konusu ikililiği aşmaya çalışsa da, her iki uç arasında kurmaya çalıştığı bağın araçsal nitelikte olması nedeni ile sosyal gerçeklik içindeki ilişkileri ortaya çıkarmada sınırlı kalmaktadır.

Modernitenin ikilikler yaratma şeklinde baskın olan eğilimine karşın, bilim ve teknoloji çalışmaları özelinde ortaya çıkan yeni bir sosyal teori olan "Aktör İlişkiler Ağları Kuramı" (Latour,1998; Law, 1992; Callon,1986), doğa/toplum, yapı/kültür, insan/insan olmayan arasındaki ilişkilere dikkati çekmeye çalışmaktadır. Bu kuramın temel ilkesi olarak kabul edilen "genelleştirilmiş simetri"ye göre, "aktör" (actor) ve "aktant" (actant) olarak da kavramsallaştırılabilen, insan ve insan olmayan(non-humanal) tüm varlıklar, oluşumlar eşit derecede eylemde bulunma kapasitesine sahiptir. Rasyonel olan ve olmayan arasındaki ayrımı da reddeden yaklaşım, Weber'in "özel rasyonalitesin e"(substantive rationality) benzer şekilde, aktant olarak ifade edilen "insan olmayan" varlık ve oluşumların kendilerine ait bir rasyonalitesi olduğunu ifade etmektedir. Teknoloji, bilgisayar, laboratuvar malzemelerinden insana kadar geniş bir yelpaze içinde tanımlanabilecek olan bu aktör ya da aktantlar, kendi çıkarları doğrultusunda ilişki ağlarını oluşturmak için diğer aktör ya

da aktantlara gereksinim duymaktadırlar. “Tercüme” (translation) olarak kavramsallaştırılan ilişki ağlarının bu oluşum süreci, dört aşamadan oluşmaktadır (Callon, 1986): “problemlleştirme” (problematization), “dahil etme” (interessement), “ikna” (enrollment) ve “ittifakların mobilizasyonu” (mobilization of allies). Buna ek olarak yine bu aşamalar içinde işlevsel özelliği olan bir diğer kavram ise “zorunlu geçiş noktaları” (obligatory passage points) dir:

Problemlleştirme: Baş aktör ya da aktant, diğer aktör ya da aktantlara kendi amaçlarını tanıtmakta ve bu amaçlara ulaşma nedenlerini problem olarak sunmaktadır.

İkna Etme: Diğer aktör ya da aktantların, baş aktör ya da aktant tarafından kendi amacının meşruluğu konusunda ikna edilmesi girişimleri bu aşamada yer almaktadır. Bu süreç içinde diğer üyeler, baş aktör ya da aktant tarafından belirlenen noktalara yönlendirilir ve bu noktalar zorunlu geçiş noktalarıdır.

Dahil Olma: İkna olan diğer üyeler, baş aktör ya da aktantın hedefleri doğrultusunda oluşturduğu ilişki ağına girmeye başlamaktadırlar.

İttifakların Mobilizasyonu: Baş aktör ya da aktantın kurduğu ilişki ağına giren diğer üyeler, yeni kimlikleri ile ilişki ağı içinde dolaşıma başlarlar.

Tercüme sürecinin sonunda, ilişki ağı durağanlık kazanır ve bu durum “kara kutu” olarak kavramsallaştırılır. Baş aktörün meşruluğunun sorgulanması ile bu kara kutu açılır ve ilişki ağı yıkılır ya da dönüşüme uğrar.

Ulrich Beck (2002) ve Giddens(1998), “Risk Toplumu” kavramsallaştırmalarında, bilimin “düşünümselliği”(reflexivity) özelliğinden bahsetmekte ve bilimin sorunlara çözüm bulmaya çalışırken yeni sorun/risk alanları yarattığını ifade etmektedirler. Bilimin “Janus Yüzü” (ikiyüzlü mabut) olarak da ifade edilen bu durum, teknoloji özelinde de uyarlanabilmektedir. Diğer bir deyişle, teknoloji, modern yaşamın karmaşıklığını azaltma konusunda kolaylıklar sağlarken, özgürlükler yaratırken, aynı zamanda

bağımlılıklar, denetim ve kontrol mekanizmaları (panoptikon gibi), yeni ihtiyaç alanları ve baskı araçları da sağlamaktadır ve bu durum, daha önce de belirtildiği gibi ancak diyalektik düşünce ile kavranabilir. Teknolojinin bu özelliğini içeren ilişki ağlarının nasıl oluştuğu Aktör İlişkiği Kuramı'na dayanılarak şu şekilde ifade edilebilir:

Problemlleştirme: Baş aktör ya da aktant olarak teknoloji, yeni ihtiyaçların varlığından bahsederek, bunların giderilmesinin özellikle yaşam kalitesinde artışa neden olacağını ileri sürebilir. Teknolojinin temel amacı, denetleme (cep telefonları örneğinde olduğu gibi) ya da pazar yaratmak olabilir.

İkna etme: Bu amaç doğrultusunda, ilişki ağının diğer üyelerinden olan insan aktörler, zorunlu geçiş noktaları olarak belirlenen ihtiyaç alanları (farklı teknolojik özelliklerin yaşam kalitesine katkıları)ni kullanarak, diğer üyeleri ikna etmeye çalışır.

Dahil Olma: Söz konusu ihtiyaçlar konusunda, kişi olarak insan aktörler ikna olurlar.

İttifakların Mobilizasyonu: İkna olan bu aktörler, yeni kimlikleri ile (farklı teknolojik özelliklere sahip ürünlere sahip olma gibi), ilişki ağı içinde dolaşıma devam ederler.

Kara kutu olarak, üretilen/inşa edilen ihtiyaçların varlığının meşrulaştırılması, bu durumu sorgulayan başka bir ilişki ağı/aktör ya da aktantın müdahalesine kadar devam eder.

Söz konusu ihtiyaçlar, “meta” ve “değer” tartışmalarını da gündeme getirmektedir. Yukarıda ifade edilmeye çalışılan ilişki ağı, ‘kullanım değeri’ söylemi üzerinden “değişim değerinin” inşa edilmesini içermektedir. Dolayısıyla başta da belirtildiği gibi, insanın kendi ihtiyaçları için üretmesi aşamasından (kullanım değerinden) pazarda mübadale için (değişim değeri) üretime geçmesi, yabancılaşmasının da başlangıcı olarak görülebilir ve herşeyin metalaştığı bir evreye denk gelmesi yüzünden de geniş ölçüde kapitalizm eleştirisini gerektirir. Ancak bu yazının sınırları dışında kaldığından bu yönlere değinilmemiştir.

KAYNAKÇA

Beck, U. (2002) *The Terrorist Threat World Risk Society Revisited, Theory, Culture & Society*, 19(4): 39-55

Callon, M. (1986) "Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St-Brieuc Bay." *J. Law (Yay. Haz.) Power, Action and Belief: A New Sociology of Knowledge? İçinde* (ss. 196-233). London: Routledge and Kegan Paul.

Giddens, A. (1998) *Risk Society: The Context of British Policies*, iç. *The Politics of risk Society*, (J. Franklin Ed.), Oxford: Polity Press.

Kasapoğlu, A. (1982;1999) *Sağlık Örgütlerinde Personelin Sosyal İlişkileri*. İç. *Sağlık Sosyolojisi: Türkiye'den Araştırmalar* (der. M. Ecevit). Ankara: Ümit (ss.14-124).

Kongar, E. (1979) *Toplumsal Değişme*. Ankara: Remzi

Latour, B. (1998) *Keynote Speech: On Recalling ANT*, <http://comp.lancs.ac.uk/sociology/stslatour1.html>.

Law, J. (1992) *Notes on the theory of the actor Network: ordering, strategy and heterogeneity*, <http://www.lancs.ac.uk/fass/sociology/papers/law-notes-on-ant.pdf> ET: 10.01.2009

Middleton, A. (1963;1975) *Alienation*. İç. *Measures of Social Psychological Attitudes* (der. J.)

Robinson ve P.R.Shaver. Michigan: University of Michigan Press.

Munir, K.A., Jones, M. (2004) *Discontinuity and After: the Social Dynamics of Technology Evolution and Dominance*, *Organization Studies*, 25(4): 561-581