

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

**TÜRKİYE’DE EMNİYET TEŞKİLATI’NDA TEKNOLOJİK YENİDEN
YAPILANMA: DENETİM VE GÖZETİMİN DEĞİŞEN DOĞASI**

Özgür GÜNAYDIN

SİYASET BİLİMİ VE KAMU YÖNETİMİ YÖNETİM BİLİMLERİ ANABİLİM DALI
YÜKSEK LİSANS TEZİ

2014 - ANKARA

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

**TÜRKİYE’DE EMNİYET TEŞKİLATI’NDA TEKNOLOJİK YENİDEN
YAPILANMA: DENETİM VE GÖZETİMİN DEĞİŞEN DOĞASI**

Özgür GÜNAYDIN

SİYASET BİLİMİ VE KAMU YÖNETİMİ YÖNETİM BİLİMLERİ ANABİLİM DALI
YÜKSEK LİSANS TEZİ

DANIŞMAN

Prof. Dr. Gamze Yücesan ÖZDEMİR

2014 - ANKARA

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI
YÖNETİM BİLİMLERİ BİLİM DALI

EMNİYET TEŞKİLATINDA TEKNOLOJİK YENİDEN YAPILANMA:
DENETİM VE GÖZETİMİN DEĞİŞEN DOĞASI

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Prof.Dr.Gamze YÜCESAN ÖZDEMİR

Tez Jürisi Üyeleri

<u>Adı ve Soyadı</u>	<u>İmzası</u>
Prof. Dr. Gamze Yücesan Özdemir	
Prof. Dr. Ahmet Albayrak	
Doç. Dr. İpek Özkul Sayan	

Tez Sınavı Tarihi 16.04.2014

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bu belge ile, tezdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu beyan ederim. Bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi ayrıca beyan ederim.(29.04.2014)


Özgür GÜNAYDIN

İÇİNDEKİLER

KISALTMALAR.....	i
ŞEKİL LİSTESİ	iii
GİRİŞ.....	1

BİRİNCİ BÖLÜM

KÜRESELLEŞME VE GÖZETİM.....	4
I. GÖZETİMİN ALTYAPISI: DENETİM	7
1. Denetimin Kaynağı: Bilgi	7
2. Denetim, Yönetim ve İktidar	11
2.1. Taylor: Bilimsel Yönetim Yaklaşımı	12
2.2. Weberyian Bürokrasi ve Denetim.....	14
2.3. Marksist Emek Süreci Teorisi ve Denetim.....	16
2.4. Teknoloji, Denetim ve İktidar.....	20
II. GÖZETİMİN DEĞİŞEN DOĞASI	23
1. Denetimin Temel Bileşeni Olarak Gözetimin Tarihsel Zemini	24
2. Modern Gözetimin Değişen Yüzü: Panoptikondan Büyük Biradere	31
3. Bilgi ve İletişim Teknolojilerinden Gözetim Teknolojilerine.....	41
3.1. Gözetim Teknolojileri ve Dijital Kültür	48
3.2. Yeni Gözetim Sistemleri	54
3.3. Gözetim Sistemlerinin E-Kapısı: E-Devlet	62

İKİNCİ BÖLÜM

GÖZETİM TOPLUMU VE GÜVENLİK: OLASILIKLAR VE SINIRLILIKLAR.....	68
I. GÖZETİM TOPLUMU	70
II. GÖZETİME MAHKUMİYET SEBEBİ: GÜVENLİK	78
1. Güvenlik ve Gözetim Teknolojisi	82
1.1. Kameralı Gözetim	90
1.2. Biometrik Gözetim.....	99
III. GÖZETİME DAİR ELEŞTİREL BİR DEĞERLENDİRME	107
1. Topluma Bakan Yönüyle Gözetim Tartışması.....	108
2. Mahremiyet Sorunsalı.....	115

3. Veri Güvenliđi Tehlikesi	124
4. Etik Boyutu	131
5. Biliřim Suçları.....	139
ÜÇÜNCÜ BÖLÜM	
TÜRKİYE’DE GÖZETİM VE GÜVENLİK: TÜRKİYE EMNİYET TEŞKİLATI.....	148
I. TÜRKİYE’DE DENETİMİN VE GÖZETİMİN ARKAPLANI.....	150
1. Türkiye’de Bilgi Toplumu Süreci	152
2. Türkiye’de E-Devlet Uygulamaları.....	156
3. Türkiye’de Gözetim Toplumu Tehlikesi	165
II. TÜRKİYE EMNİYET TEŞKİLATI’NDA TEKNOLOJİK DÖNÜŞÜM	172
1. Emniyet Teřkilatı’nın Örgütsel Yapısı	173
2. Emniyet Teřkilatı’nda Bilgi ve İletişim Teknolojileri.....	179
2.1. Polnet.....	179
2.2. Mobese	186
III. EMNİYET TEŞKİLATI’NDA TEKNOLOJİK DÖNÜŞÜMÜN SONUÇLARI:	
TEHDİTLER, RİSKLER VE ÖNERİLER	190
1. Kuruma Yönelik Tehditler	194
1.1. Güvenlik Paranoyası	194
1.2. Proaktif Polislikten Düşünce Polisliğine	196
1.3. Gözetleyenlerin Gözetimi.....	198
1.4. Veri Güvenliđi Sorunu	200
1.5. Etik Sorunlar	202
2. Topluma ve Yurttařa Yönelik Tehditler	205
2.1. Mobese, Polnet ve Suçla Mücadele İliřkisi	205
2.2. Paranoyak Toplum	215
2.3. Özel Hayatın Gizliliđi Sorunu	217
2.4. Bireye Ait Verinin Güvenliđi Sorunu	221
3. Gözetimin Yönetimine Yönelik Öneriler	224
3.1. Gözetim Kontrol Birimi	225
3.2. Şeffaflık Raporları.....	231
SONUÇ	234
KAYNAKÇA	238
ÖZET	252
ABSTRACT	253

EK I.....	254
EK II	255
EK III.....	256
EK IV	257

KISALTMALAR

AB	: Avrupa Birliđi
ABD	: Amerika Birleşik Devletleri
AET	: Avrupa Ekonomik Topluluđu
AFIS	: Automatic Fingerprint Identification System (Otomatik Parmak İzi Belirleme Sistemi)
a.g.k	: adı geçen kaynak
a.k	: aynı kaynak
AR-GE	: Araştırma-Geliştirme
ARPANET	: Advanced Research Projects Agency Network (Amerikan Gelişmiş Savunma Araştırmaları Dairesi Ađı)
ASBİS	: Asayiş Bilgi Sistemi
ATM	: Automated Teller Machine (Bankamatik)
AVM	: Alışveriş Merkezi
BİT	: Bilgi ve İletişim Teknolojileri
BM	: Birleşmiş Milletler
CBS	: Coğrafi Silgi Sistemleri
CCTV	: Closed Circuit Television
CD ROM	: Compact Disc Read-Only Memory
CHP	: Cumhuriyet Halk Partisi
CIA	: Central Intelligence Agency (Merkezi İstihbarat Teşkilatı)
Çev.	: Çeviren
DNA	: Deoksiribonükleik Asit
DPT	: Devlet Planlama Teşkilatı
DVD	: Digital Versatile Disc
Ed.	: Editör
E-Devlet	: Elektronik Devlet
EDGE	: Enhanced Data Rates for Global Evolution (Kûresel Evrim İin Gelişmiş Veri Oranları)
EGM	: Emniyet Genel Mûdûrlüđu
ENIAC	: Electronic Numerical Integrator And Computer (Elektronik Sayısal Entegreli Hesaplayıcı)
ETK	: Emniyet Teşkilatı Kanunu
FBI	: Federal Bureau of Investigation (Federal Soruşturma Bûrosu)
GATT	: General Agreement on Tariffs and Trade (Gûmrûk Tarifeleri ve Ticaret Genel Anlaşması)
GBT	: Genel Bilgi Toplama
GİMOP	: Gûmrûk İdarelerinin Modernizasyonu Projesi
GPRS	: General Packet Radio Service
GPS	: Global Positioning System (Kûresel Konumlama Sistemi)
GSM	: Global System for Mobile (Kûresel Cep Telefonu Sistemi)
HTML	: Hyper Text Markup Language
IMEI	: International Mobile Equipment Identity (Uluslararası Mobil Cihaz Kodu)
IP	: Internet Protocol
İLEMOD	: İl Envanteri Modernizasyonu
İng	: İngilizce

İSS	: İnternet Servis Sağlayıcısı
KCK	: Koma Civaken Kurdistan (Kürdistan Topluluklar Birliği)
KDTS	: Kapalı Devre Televizyon Sistemleri
KOM	: Kaçakçılık ve Organize Suçlarla Mücadele
MEB	: Milli Eğitim Bakanlığı
MEBBİS	: Milli Eğitim Bakanlığı Bütünleşik Yönetim Bilgi Sistemi
MERNİS	: Merkezi Nüfus İdaresi Sistemi
MERSİS	: Merkezi Sicil Kayıt Sistemi
MİT	: Milli İstihbarat Teşkilatı
MOBESE	: Mobil Elektronik Sistem Entegrasyonu
MOBİL-K	: Mobil-K Ünitesi
NASA	: National Aeronautics and Space Administration (Ulusal Havacılık ve Uzay Dairesi)
NATO	: North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması Örgütü)
NSA	: National Security Agency (Ulusal Güvenlik Dairesi)
ODTÜ	: Ortadoğu Teknik Üniversitesi
OECD	: Organisation For Economic Co-Operation And Development (Ekonomik Kalkınma ve İşbirliği Örgütü)
ÖSYM	: Ölçme, Seçme ve Yerleştirme Merkezi
PC	: Personel Computer (Kişisel Bilgisayar)
PKK	: Partiya Karkeren Kurdistan (Kürdistan İşçi Partisi)
POLNET	: Polis Network
PTT	: Posta ve Telgraf Teşkilatı Genel Müdürlüğü
PVSK	: Polis Vazife ve Salahiyetleri Hakkındaki Kanun
RFID	: Radio-Frequency Identification (Radyo Frekansı ile Tanımlama)
s.	: sayfa
SES	: Sağlık Bakanlığı Sağlık Enformasyon Sistemleri
SMS	: Short Message Service (Kısa Mesaj Hizmeti)
SSCB	: Sovyet Sosyalist Cumhuriyetler Birliği
TAKBİS	: Tapu Kadastro Genel Müdürlüğü Bilgi Sistemi
TBMM	: Türkiye Büyük Millet Meclisi
TDK	: Türk Dil Kurumu
TUENA	: Türkiye Ulusal Enformasyon Altyapısı Ana Planı
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜİK	: Türkiye İstatistik Kurumu
UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UYAP	: Ulusal Yargı Ağı Projesi
vd.	: ve diğerleri
VEDOP	: Vergi Daireleri Otomasyon Projesi
WAP	: Wireless Application Protocol (Kablosuz Uygulama Protokolü)
WTO	: World Trade Organization (Dünya Ticaret Örgütü)
YSK	: Yüksek Seçim Kurulu
yy	: yüzyıl

ŞEKİL LİSTESİ

<u>Sekil No</u>	<u>Sayfa</u>
Şekil-1. Coğrafi Bölgelere Göre Dünya İnternet Kullanım Yaygınlığı Oranları - 2012	136
Şekil-2. Emniyet Genel Müdürlüğü Örgütsel Yapısı	177
Şekil-3. Polnet İletişim Altyapısı ve Üzerinde Çalışan	183
Şekil-4. Mobese Projesi Bileşenleri	187
Şekil-5. İngiltere Gözetim Komisyonu Başkanlığı	226
Şekil-6. Gözetim Kontrol Daire Başkanlığı	229

GİRİŞ

“Mahremiyete değer vermeyen ve kişisel verilere ucuz bir eşya muamelesi yapan toplumlar, er ya da geç, vatandaşlarına da aynı şekilde davranırlar.”
John Grace, 1982
(Kanada’nın İlk Mahremiyet Komiseri)

Gözetim faaliyetleri günlük hayatın doğal bir parçası rutinliğinde bireyin davranışlarının, ilişkilerinin, görüşmelerinin, dijital izlerinin sistematik olarak takip edilmesini ifade etmektedir. Bu kapsamda birey duygularından soyutlanmış bir meta olarak gözetimin nesnesi konumundadır. Gözetim, tarihin her döneminde farklı şekillerde kendini göstermiştir. Zira gözetimin varlığı iktidarın birey ve toplum üzerinde hakimiyetini kurmasında bir denetim aracı olarak vücut bulmaktadır. Bu bakımdan şekli, dönemlere göre değişse de gözetimin öznesi hep iktidar odakları olmuştur. Günümüzde bilgi ve iletişim teknolojilerindeki gelişmelere paralel olarak gözetim araçlarının giderek çeşitlilik ve artış göstermesi ile gözetim faaliyetleri hayatın her alanına nüfuz edebilen güce kavuşmuş ve daha organize, etkili, yoğun hale gelmiştir. Türkiye de gözetim faaliyetlerinin bu etki alanı içinde yer almaktadır. Ülkemizde gözetim faaliyetleri başta Emniyet Teşkilatı olmak üzere güvenlik birimleri önderliğinde yürütülmektedir. Dolayısıyla bu çalışmanın konusunu Emniyet Teşkilatı’ndaki bilgi ve iletişim teknolojileri kapsamında denetim ve gözetim araçlarının belirlenmesi, gözetim pratiklerinin etkilerinin etik, suçla mücadele, toplumsal yankılar, gözetim toplumu perspektifinde ortaya konulması oluşturmaktadır.

Bu çalışmanın önemi dört başlık altında ifade edilebilir. Birinci olarak çalışmanın gözetim yazınına katkı sağlayacağı düşünülmektedir. Zira Türkiye’de gözetim çalışmaları sınırlıdır.¹ İktidar, birey ve toplum üzerinde muktedir olmak amacıyla “bilgiye hakim olma araçlarını” gözetim teknolojisi üzerinde her geçen gün arttırmakta ve geliştirmektedir. Hızla ilerleyen bu yükselişte ülkemizde gözetim toplumu distopyadan gerçeğe doğru evrilmektedir. Bu bakımdan günümüzde yolsuzluk, terörizm gibi önemli sorunlara yakın vadede gözetim tehdidinin de ekleneceği değerlendirilmektedir. Hem gözetim toplumu tehlikesine dikkat çekmek hem de gözetim faaliyetlerinin birey nazarında normalleşmesine engel olmak

¹ YÖK Ulusal Tez Merkezi’nde “Gözetim Toplumu” konulu beş adet; “Mobese” konulu bir adet, “Polnet” konulu beş adet tez bulunmaktadır. Ulusal Akademik Ağ ve Bilgi Merkezi’nde tüm veritabanlarında yapılan aramalarda “Mobese” konulu iki adet makale, “Polnet” konulu üç adet makale, “Gözetim Toplumu” konulu beş adet makale olduğu tespit edilmiştir.

amacıyla bilimsel yazında “gözetim” ile ilişkili alana önem verilmesi gerektiği düşünülmektedir. Hazırlanan çalışmanın bu bakımdan önemli olduğu ifade edilebilir.

İkinci olarak çalışmanın Emniyet Teşkilatı özelinde gözetim teknolojilerine yönelik olması önemlidir. Nitekim yapılan araştırmalarda günümüze kadar gözetim faaliyetlerine yönelik Emniyet Teşkilatı özelinde herhangi bir bilimsel çalışmanın olmadığı tespit edilmiştir.² Bu bakımdan çalışmanın özgün olduğu değerlendirilmektedir. İktidarın gözetim faaliyetlerini toplumsal algıda normalleştirebilmesinin en önemli aracı suçla mücadele ve güvenliğin sağlanmasıdır. Ülkemizde suç oranlarının artan bir ivmeyle yükselmesi kurumsal ve toplumsal bakışta Emniyet Teşkilatı’nın gözetim teknolojileriyle donatılmasını haklı göstermektedir. Bu kapsamda Teşkilat içerisinde gözetim faaliyetleri yükselen bir trende dönüşmüştür. Bu gidişin neticesinde özel hayatın gizliliği ve suçla mücadele dikatomisinde özel hayatın gizliliğinin yok sayılması tehlikesine ve keyfi uygulamalara karşın bunun gibi bilimsel çalışmaların yapılması gerektiği değerlendirilmektedir.

Üçüncüsü yönetim yazınında gözetim sürecinin hem kurumsal bir yönden hem de bu kurumu toplumun içine yerleştirip toplum ve yurttaş açısından öneminin vurgulanmasıdır. Son olarak çalışmanın önemi kurumsal yapılanmada çıkacak sorunlar yüzünden bir örgütsel yapı önerisinde bulunularak gözetimin yönetimine somut bir çözüm ortaya konulmasıdır.

Çalışmanın amacı; Türkiye’nin güvenlik alanında gözetim toplumunun neresinde olduğu sorusunun yanıtını aramak, Emniyet Teşkilatı’nın bilgi ve iletişim teknolojileriyle birlikte değişim ve dönüşümünü ortaya koyabilmek, bu değişim ve dönüşümün yönetsel, toplumsal ve bireysel etkilerini objektif olarak tespit etmektir.

Bu amaca yönelik olarak çalışmada şu sorulara cevap aranmaktadır. Türkiye gözetim toplumu mudur? Süreç nasıl işlemektedir? Türkiye’de Emniyet Teşkilatı’ndaki teknolojik dönüşüm araçları nelerdir? Bu araçların gözetim toplumu ve bilgi toplumu ilişkisi nasıldır? Polnet, Mobese nedir? Bileşenleri, kapasiteleri, etkinlikleri, teknik durumları nasıldır? Günümüz suçla mücadelesinde yerleri ve önemleri nedir? Denetim ve gözetimin etik boyutu nasıldır? Mobese ve Polnet uygulamalarının etik değerlendirmesi nasıl yapılmalıdır?

Bu sorulara cevap aramak amacıyla çalışmayaliteratür taraması ile başlanmıştır. Bu çerçevede konuyla ilgili kitaplar, makaleler, raporlar, gazete köşe yazıları, resmi belgeler incelenmiştir. Konuyla ilgili yerli literatürün sınırlı olması nedeniyle ağırlıklı olarak yabancı

² YÖK Ulusal Tez Merkezi’nde ve Ulusal Akademik Ağ ve Bilgi Merkezi’nde Emniyet Teşkilatı’nda denetim ve gözetim faaliyetlerine yönelik hazırlanmış tez veya makale bulunmamaktadır.

kaynaklara başvurulmuştur. Çalışmada Emniyet Teşkilatı'na yönelik kurumsal arkaplan alınmıştır. Polnet ve Mobese sistemleri ile bunların fonksiyonları bizzat incelenmiştir. Ayrıca konuya derinlik katması amacıyla kurumdan üç kişiyle görüşülmüştür.(Ek-1) Bu görüşme sırasında derinlemesine soru formu kullanılmıştır.(Ek-2)

Çalışma üç ana bölümden oluşmaktadır. Birinci bölümde iktidar güçlerinin denetim aracı olarak gözetim ve gözetim faaliyetlerinin küreselleşmenin etkisiyle modern dönemlerden bilgi ve iletişim teknolojileri hızlı treniyle günümüze doğru olan evrilişi incelenmiştir. Öncelikle gözetimin altyapısı olarak denetim faaliyetleri ele alınmıştır. Denetimin iktidarın bir aracı olarak aldığı şekiller Frederick Taylor'un "Bilimsel Yönetim Yaklaşımı", Max Weber'in "Bürokrasi Kuramı" ve "Egemenlik Anlayışı", Karl Marx'ın "Emek Süreci Teorisi" ve Micheal Foucault'nun "İktidar" kuramları çevresinde incelenmiştir. Sonrasında denetim ve gözetim ilişkisi değerlendirilerek gözetimin tarihsel gelişimi ortaya konulmuştur. Bu kapsamda gözetim faaliyetlerinin lokomotif olarak bilgi ve iletişim teknolojilerinin gözetim sistemlerine dönüşümü de konu edilmiştir.

İkinci bölümde sanayi toplumu sonrası sürecin bilgi toplumuna yönelimi; bilgi toplumunun distopik olarak gözetim toplumuna evrilişi; gözetim toplumunun varoluş göstergeleri, bireyin mahremiyetine verdiği tahribat, etik boyutu, kendi içinde barındırdığı veri güvenliği tehlikesi ele alınmıştır. Ayrıca gözetimin bütün tehlikelerine rağmen varlığını vazgeçilmez seviyede tutan "güvenliği sağlama" gerekçesi tartışılmıştır.

Çalışmanın son bölümünde diğer bölümlerde anlatılan gözetim faaliyetlerinin bir sentezi olarak Türkiye genelinde gözetim süreci anlatılmış ve gözetim toplumu tehlikesine dikkat çekilmiştir. Sonrasında daha özele inilerek Türkiye Emniyet Teşkilatı'nda bilgi ve iletişim teknolojilerinin gelişim seyri ve bunların gözetim teknolojilerine evrilmesiyle ortaya çıkan Polnet, Mobese projeleri değerlendirilmiştir. Çalışmada bu projelerin birer gözetim teknolojisi olduğu ve yeni gözetim teknolojilerinin de altyapısını oluşturduğu iddia edilmiştir. Bu çerçevede belirtilen projelerin yurttaş bakan ve kurumsal yönleriyle oluşturduğu tehditler ifade edilmiştir. Ayrıca kurumsal olarak gözetimin yönetimine dair yapısal önerilerde bulunulmuştur.

BİRİNCİ BÖLÜM

KÜRESELLEŞME VE GÖZETİM

“Yeni bir dünya sisteminin adı”³ olarak tanımlanabilecek olan küreselleşme günümüz dünyasında en çok konuşulan ve günlük yaşamımızı bütün yönleriyle derinden etkileyen bir olgudur. Özellikle son yıllarda dünya konjonktüründeki küreselleşme odaklı teknolojik, sosyo-politik, sosyo - psikolojik, sosyo - ekonomik, sosyo - kültürel alanlarda yaşanan hızlı gelişim ve değişimler devlet, toplum ve insan hayatının her alanına nüfuz etmiştir.

1980’den itibaren başladığı kabul edilen ve Sovyetler Birliği’nin dağılmasıyla hız kazanan küreselleşmeyi kavramsal olarak incelediğimizde kelime olarak İngilizce karşılığının “globalisation” olduğunu görürüz. Bunun etimolojik olarak kökünde, üç boyutlu yuvarlak bir fiziksel şekli ve dünyayı ifade eden “globe” sözcüğü yer almaktadır. Ayrıca Meydan Larousse’nin tarifine göre global, “tümüyle ele alınmış olan” manasına gelmektedir.⁴ Küreselleşmenin ekonomik, siyasal ve sosyo - kültürel olmak üzere üç temel boyutu dikkate alınarak farklı tanımlamalarda bulunulabilir. Bu çerçevede ekonomik küreselleşmenin; ülkeler arasında ekonomik duvarların kalkıp, üretim ve pazarlama süreçlerinin dünya pazarları ekseninde yeniden örgütlenmesi, malların ve hizmetlerin ülkeler arasında daha kolay bir şekilde dolaşabilir hale gelmesi, ekonomik yapıların serbest piyasacı bir mantıkla yeniden düzenlenmesi sürecini ifade ettiği söylenebilir.⁵

³ Birgül Ayman Güler, 23 Ocak 2004 tarihinde TRT 2 “45 Dakika” haber programında sunucu Burcu Duru Altınyeleklioğlu ile yaptığı “Küresel Sömürgecilik” konulu söyleşisinde küreselleşme ile ilgili şu tespitlerde bulunmuştur: “...küreselleşme dünyanın bir küçük köye dönüşmesi, dünyanın bilim teknolojideki gelişmeler nedeniyle iki yakasının bir araya gelmesi, global köy haline gelmesi biçiminde genellikle tanımlanır, dolayısıyla bu gelişmeler nedeniyle kaçış yoktur, burada yaşanacak ve bunun gerekleri de bütün dünyada gözler önündedir, bunlar yapılacak. Akıllı insan bunları bir an önce yapmaya başlayandır, tren kaçıyor aman yakalayım, ne kadar erken yakalarsanız o kadar iyi vagonda yol alırsınız... Bir tarafında bu var. Bir çeyrek yüzyıldır duyduğumuz şey bu. Bu bir masaldır. Çünkü, herhalde tekerlek iyi bir başlangıçtır, insanoğlu tekerleği icat ettiğinden bu yana, şimdi hızlı trenlere ve muhteşem otomobillere, hele hele bu uydu teknolojisine vardığımızdan bu yana..o zamandan beri dünya küreselleşiyor, eğer küreselleşme böyle tanımlanacaksa. Bu günküün ne farkı var? Yalnızca hızı yüksek demektir. Bu çok yetersiz bir algılayış tarzı. Küreselleşme, bir yeni dünya sisteminin adıdır. Yeni bir dünya sistemini yaratan sürecin adıdır. ve bu sürecin başlangıcı 1980’li yıllardır. Daha öncesinde dünyanın kendine özgü düzenleri vardı, 1930’lardan başlayıp 1945’den itibaren kurulan bu düzen modern sömürgecilikti, 1930, 1945 öncesinde bu düzen klasik sömürgecilikti. Baştan alırsam 1800’lü yılların sonundan 1945’e kadar klasik sömürgecilik dünya düzenin adı, dünya yine küreselleşiyor, küçülüyor o dönemde, 45’den 80’lere doğru modern sömürgecilik denilen bir dünya düzeni, 1980’den itibaren de, küreselleşme ile biraz meşrulaştırılmaya çalışılan o terimle küresel sömürgecilik denebilir. Şöyle tanımlayabiliriz onu, küreselleşme 1980’den itibaren inşa edilmeye çalışılan yeni bir dünya düzenin adından ibarettir. Şimdi bu tanım kendi içerisinde çok şey anlatıyor. Yeni bir dünya düzenin inşası, zorunluluk, olgu, kaçınılmazlık değildir, bir politikadır, bir vizyondur (görüş), bir ideolojidir (düşünce biçimi) başka deyişle. ...”

⁴ http://www.genbilim.com/index.php?option=com_content&task=view&id=3922, (Erişim Tarihi: 10.10.2012).

⁵ a.k

Siyasal anlamda küreselleşme; dış ülkelerin ve uluslararası kuruluşların ülkelerin iç politikalarına daha kolay müdahale edebilir hale gelmesi gayeli ulus devletin gücünün ve öneminin aşınmasını, egemenlik ve bağımsızlık kavramlarının içerik ve şekil değiştirmesini ifade etmektedir. Sosyo - kültürel küreselleşme ise insanların kendi öz kültürlerinin şekil ve mana değiştirmesi, bu ekseninde küresel kültür formlarının oluşması ve ulusların öz kültürlerini baskı altına alacak çeşitli araçların gelişmesi süreci olarak açıklanabilir.⁶

Günümüzde küreselleşme taraftarları ve küreselleşme karşıtları bulunmaktadır. Her iki tarafın da kendilerine göre bazı argümanları bulunmaktadır. Bu argümanlar ne olursa olsun, her iki tarafın da kabul ettiği bir gerçek vardır ki o da, küreselleşmenin hayatımızı, günlük yaşantımızı, zaman - mekan algımızı büyük ölçüde değiştirdiği, buna paralel olarak toplumsal ve kamusal yapıları da değiştirmeye zorladığı, dolayısıyla yeni bir dünya sistemi oluşturma sonuçlu ilerlediğidir. Bu yeni dünya sisteminden bilgi ve iletişim teknolojileri de payını almış, dolayısıyla bilgi ve iletişim teknolojileriyle doğrudan bağlantılı olan gözetim faaliyetleri ve gözetim teknolojileri de etkilenmiş, hatta şekil ve içerik değiştirmiştir. Bundan da ötesi gözetim faaliyetleri sağlanan teknolojik gelişmelerden cesaret alarak engellenemez, görülemez formlarda toplumun geniş kitlelerine nüfuz edecek ve onları kontrol altına alacak şekilde değişime uğramıştır.

Bilgi ve iletişim teknolojilerindeki gelişmeler küreselleşmenin bir sonucu olduğu gibi aynı zamanda küreselleşmenin de bir nedenidir. Nitekim Manuel Castells bu durumu “küresel ağ etkisi” olarak şöyle ifade eder. “Küreselleşme, hükümetleri, kültürleri ve kurumsal yapıları farklı biçimlerde birbirine bağlayan enstrümantal bir enformasyon ağıyla işleyiş kazanmaktadır.”⁷ Küresel ağ oluşturacak nitelikteki bilgi ve iletişim teknolojilerinde meydana gelen bu gelişmeler dünyada ülkelerarası coğrafi sınırları anlamsız hale getirmiş, bir anlamda dünyayı ticaret, finans ve üretim sektörlerinin ortak pazarı haline dönüştürmüştür. Bu noktada iletişim çeşitlenmiş ve kolaylaşmıştır. Bu nedenle de iletişim, gözetlenmesi gerekli bir metaya dönüşmüştür.⁸

Küresel gözetimin, genel olarak küreselleşme olarak adlandırılan, dünyanın pek çok yerine yayılmış olan kapitalizmin ekonomik yeniden yapılandırılmasının ana bölümünü oluşturduğu söylenebilir. Sonuçları bölgeden bölgeye ve sektörden sektöre değişiklik gösterse

⁶ a.k

⁷ Özgür Uçkan, *E-Devlet, E-Demokrasi ve Türkiye Kamu Yönetiminin Yeniden Yapılanması İçin Strateji ve Politikalar*, Literatür Yay., İstanbul, 2003, s.70.

⁸ Oktay Öksüzler, Ali R. Özdemir "Bilgi ve İletişim Teknolojilerinin Kamu Sektörünün Büyüme Hızı Üzerine Etkileri: Bir OECD Panel Verileri Regresyon Analizi", s.389. www.iibf.ogu.edu.tr/kongre/bildiriler/09-03.pdf, (Erişim Tarihi: 10.09.2012).

de, uluslarüstü nitelik kazanmış olan gözetleme işlemleri önemli her sosyal, ekonomik ve politik sektörde görülebilir. Küreselleşmeyle birlikte artık gözetime, toplumsal denetimi sağlama aracı olmasının çok daha ötesinde işlevler biçilmiştir.⁹

Gözetim teknolojileri küreselleşmenin biraracı olarak kapitalist üretim ilişkilerinde önemli yer edinmiştir. Bu nedenle özel sektörün müşterilerinin verilerini elde etmek için birbirleri ile anlaştıklarını ve veri çeşitliliklerini arttırmak için de gelişmiş bilgi ve iletişim teknolojilerini kullandıkları görülmektedir.¹⁰ Diğer taraftan gözetleme teknik ve metotlarının istihbarat gibi özel alanlarda olsa dahi, küreselleşme ile başka devletlerin aktörlerinin eline geçebildiği görülmektedir. Bu noktada gözetleme teknik ve teknolojileri de küreselleşmektedir. Bununla paralel olarak gözetleme verileri de küresel alanlarda özgürce dolaşmaya başlamıştır. Pek çok durumda küresel gözetimin amacının uluslararası uyuşturucu trafiği ve uluslararası terörizmle mücadele gibi yüksek profilli güvenliği geliştirmek ve tehlikeyi azaltmak olduğu iddia edilmektedir.

Yukarıda belirtilen masumane amaçlar için olsa da kişisel verilerin küresel gözetleme araçlarıyla küresel boyutta mahremiyetinin ihlal edildiği yadsınamaz bir gerçektir. Diğer taraftan güvenlik eksenli kullanıma elbisesi altında olan gözetleme verilerinin küreselleşmesinden daha tehlikeli olanı *Facebook*, *Twitter*, *Msn*, *Linkedn* gibi arkadaşlık ve profil paylaşma sitelerine olan ilginin giderek artış göstermesi ve insanların çekinmeden her türlü özel bilgilerini bu küresel bilgi toplama merkezlerine bırakmasıdır.

Bu bölümde birinci olarak küreselleşmeyle gözetimin değişen doğasını ortaya koyma hedefli olarak öncelikle gözetimin arkaplanında yer alan “denetim” olgusu ele alınacaktır. Yurttaş kontrol altında tutma manasında değerlendirilen denetim faaliyetleri, denetimin iktidar güçleri tarafından araçsallaştırılması Karl Marx, Max Weber, Frederich Taylor, Micheal Foucault bakışında değerlendirilecek ve günümüze bakan yönüyle gözetimin aracı haline dönüşmüş olan teknoloji ilişkiselliği ortaya konulacaktır.

İkinci olarak öncelikle gözetimin kavramsal çerçevesi ve tarihsel evrilişi gösterilmeye çalışılacaktır. Sonrasında küreselleşmeyle gözetimin değişen doğasının omurgasını oluşturan bilgi ve iletişim teknolojilerinin gözetim teknolojilerine eklemlenmesi ve bu şekilde ortaya çıkan yeni gözetim sistemleri tartışılacaktır. Son olarak, gözetim sistemlerinin devlet - yurttaş ilişkisinde ortaya çıkan verileri toplama aracı olarak e-devletleşme sürecine bakılacaktır.

⁹ Hakan Yıldırım, vd., *E-Devlet Başa*, Macar Yayıncılık, Ankara, 2006, s.36.

¹⁰ a.k

Çalışmanın ikinci bölümünde anlatılacak olan günümüz gözetim toplumlarının tabanında yer alan temel bileşenler ve yaklaşımlar, gözetim evreni bu bölümde tartışılmış olacaktır.

I. GÖZETİMİN ALTYAPISI: DENETİM

Gözetim ve denetim kavramları birbiriyle iç içe geçmiş, birbirinin hem sebebi hem de sonucu olan kavramlardır. Denetimde kontrol altında tutma ağır basarken, gözetimde kontrol altında tutulana kontrol etme söz konusu olduğu ifade edilebilir. Denetim ve gözetim faaliyetlerinin ortaya çıkışı ile ilgili farklı değerlendirmeler olsa da aşıkâr olan bu faaliyetlerin bireyin tek başına hayatını idame ettiremeyeceği gerçeğinden yola çıkarak diğer bireylerle birlikte yaşama, gündelik faaliyetlerinde diğerlerine ihtiyacı olma içgüdüsünden; yani sosyalleşme mecburiyetinden dolayı ortaya çıkan toplumsal yapının bir sonucu olmasıdır. Emile Durkheim'ın ifade ettiği gibi sosyal kontrolün sağlanması için birilerinin diğerlerinin sosyal kurallara, toplumsal düzene uyup uymadığını denetlemesi gerekmektedir.¹¹ Bu noktada esasında gözetim faaliyetleri toplumsal denetimi temin etme gayesinin bir aracı konumunda olagelmıştır. Toplumsal düzeni sağlamak için denetim; bir anlamda kontrol altında tutma, bunun için de hedef kitleyi gözetleme söz konusu olmuştur.

Bireyin yaşamı göz önünde bulundurulduğunda ömrü boyunca kendi kurallarına sahip olan bir kuşatma mekanından öbürüne geçip durduğu görülür. Önce aile, sonra okul, ardından kışla, sonra fabrika; genel olarak hastane, hapishane, kamusal alanlar gibi çeşitli kuşatılmış çevrelerde varlığını sürdürür.¹² Bu süreçte her yapı içinde kurallara uyma zorunluluğundan dolayı denetim altında tutulmaya, bu kapsamda da gözetlenmeye mahkum olur. Kuralların uygulanmasını sağlayanlar sahip oldukları gözetleme araçları ve iktidar güçleri paralelinde daha çok gözetlerler.

Bu bölümde gözetim - denetim kavramlarının ontolojik varlıklarını arayışta iktidar olgusunun önemli bir yeri oluşu tartışılacaktır. Bu kapsamda iktidarın muktedir olabilmesi için “bilgiye hakim olma” becerisine sahip olması gerektiği, bu beceriyi kazanmada denetim ve gözetim faaliyetlerini araçsallaştırdığı ortaya konulmaya çalışılacaktır. Sonrasında da temel yönetim yaklaşımları çevresinde denetim ve iktidar olgusu sorgulanacaktır.

1. Denetimin Kaynağı: Bilgi

Denetim ile gözetim kavramları birbirini tamamlayan süreçleri ifade ederken; denetim kavramı gözetime göre daha geniş anlam taşımaktadır. Hatta gözetimi kapsayıcı ve gözetim

¹¹ http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Social_control.html, (Erişim Tarihi: 15.12.2013).

¹² Michel Foucault, *Hapishanenin Doğuşu*, Çev. Mehmet Ali Kılıçbay, İmge Yayınları, Ankara, 2006, s.286.

etkinliklerini araçsallaştırıcı bir özellik de içerdiği söylenebilir. Nitekim görmenin, görülenin bilgisine sahip olmanın, gören için bir güç unsuru olması gözetimi tarihsel ve toplumsal süreçlerde bir denetim aracı haline dönüştürdüğü bir gerçektir.

Denetim (*İng; control*) kelime anlamı olarak; *Merriam Webster* sözlüğünde, “bir şey veya kimseleri sınırlandırma veya üzerlerinde doğrudan etki oluşturma”¹³ şeklinde, Oxford sözlüğünde, “bir faaliyetin, eğilimin veya olayın sınırlandırılması”¹⁴ şeklinde, Türk Dil Kurumu sözlüğünde ise “denetlemek işi, murakabe, kontrol”¹⁵ olarak tanımlanmaktadır. Çalışmamızda denetim kavramı “kontrol altında tutma, kişiler üzerinde sınırlandırma faaliyetleri” anlamında kullanılmıştır.¹⁶

Denetim ile iktidar birbirine gebe iki kavramdır. Tarih boyunca denetimi gerçekleştirenler, iktidarı elinde bulunduranlar veya iktidarı kazanmak isteyenler olagelmıştır. Bu bağlamda iktidarın var olabilmesi için de iktidar kurulacak olan kişilere; yani denetim ve kontrolün muhataplarına ihtiyaç duyulmaktadır. Diğer taraftan iktidar, denetim, bilgi arasında da ontolojik bağlantı bulunmaktadır. İktidar ilişkilerinin ve bu ilişkiler kapsamında denetim süreçlerinin var olabilmesi için bilginin tespiti, toplanması ve analiz edilmesi gerekmektedir.

İktidarla bilgi arasında çok sıkı bir ilişki bulunmaktadır. Yapısal olarak her iktidar bilgiye gereksinim duyar. Bauman’a göre bu yapısal bakışta bilgi, iktidara meşruluk ve etkinlik kazandıran bir etmendir. Dolayısıyla iktidar olmak bilgiye sahip olmaktan geçmektedir.¹⁷ Denetim odaklarının herhangi bir nesneyi, bireyi ya da toplumu kontrol etmek amaçlarına ulaşabilmesi için öncelikle kontrol konusu şeyi iyi tanıması gerekir. Bunun için de kontrol edilmek istenen nesnenin, bireyin ya da toplumun gözetlenmesi, takip edilmesi süreçleri gerekmektedir. Bu nedenle iktidarlar toplumu kontrol etmek için onu daha çok tanımak ve bilmek isterler. Bu durumda da mümkün olduğu kadar toplumu gözetlerler ki

¹³ <http://www.merriam-webster.com/dictionary/control>, (Erişim Tarihi: 17.02.2013).

¹⁴ http://oxforddictionaries.com/view/entry/m_en_gb0176220#m_en_gb0176220, (Erişim Tarihi: 17.02.2013).

¹⁵ <http://www.tdksozluk.com/index.php?qu=denetim&ne=a>, (Erişim Tarihi: 17.02.2013).

¹⁶ Denetim kavramını açıklamada Foucault örnek olarak cinsel denetim faaliyetlerini göstermektedir: “*Cinsel Denetim; mastürbasyon denetimi şeklinde Avrupa’da on sekizinci yüzyılda başlamıştır. Aniden, panik yaratan bir tema ortaya çıktı: Gençler mastürbasyon yapıyor. Bu korku adına çocukların bedeni üzerinde – aileler aracılığıyla; ama kaynağında aileler yoktu - bir denetim oluşturuldu, cinsellik gözetlenmeye, bedenlere işkence edilmesi yoluyla nesnellik altına alınmaya başlandı. Fakat gözetim ve denetimin hedefi olarak, bir kaygı ve analiz nesnesi haline gelen cinsellik, aynı zamanda, herkesin kendi bedeni için, kendi bedeninde ve kendi bedeni üzerinde duyduğu arzuların yoğunlaşmasına yol açtı... Beden, çocuklarla aileler arasında, çocukla denetim mercileri arasında bir mücadele konusu haline geldi. Cinsel bedenin isyanı bu gelişmenin karşı-etkisidir. İktidarın buna yanıtı nedir? Erotikleşmeyi, bronzlaşma ürünlerinden porno filmlere kadar iktisadi (ve belki de ideolojik) olarak sömürmek... Hatta bedenin isyanına yanıt olarak, artık denetim - baskı biçiminde değil, denetim-teşvik biçiminde kendini gösteren yeni bir kuşatmayla karşılaşsınız: ‘Çırılçıplak soyun... ama zayıf,güzel,bronz tenli ol!..’*” Michel Foucault, *İktidarın Gözü*, Ayrintı Yayınları, İstanbul, 2003, s.40.

¹⁷ Zygmunt Bauman, *Yasa Koyucular ile Yorumcular*, Çev. Kemal Atakay, Metis Yayınevi, İstanbul, 1996, s.62.

toplum hakkında bilgi edinebilsinler. Bu bağlamda iktidarla bilgi arasında güçlü bir bağ bulunduğu ifade edilebilir.

Bauman'ın yaklaşımındaki bilgi - iktidar arasındaki tek yönlü etkileşime karşın Foucault'a göre bilgi ile denetimin sahibi olan iktidar arasında düalist organik bir bağ bulunmaktadır. Yani, bu iki kavram arasındaki ilişki sadece tek yönlü değildir. Bilgi ya da bilmek, iktidarın varlığı ve devamlılığı için zorunluyken; iktidarın da bilgi ürettiği görülmektedir. Salt bilimsel bilginin gelişimi bile iktidar ilişkilerine bağlı olarak evrilmektedir. Dolayısıyla iki kavram arasında çift yönlü bağ vardır. Nitekim bu durumu Foucault şu şekilde ifade etmektedir:¹⁸

“İktidarın bilgiye, bilginin iktidara sürekli eklemlendiği kanısındayım ve ben bunu ortaya çıkarmayı denedim. İktidarın falanca keşfe, filanca bilgi biçimine ihtiyacı olduğunu söylemekle yetinmemeli, iktidar işleyişinin bilgi nesneleri yarattığı, bunları ortaya çıkardığı, enformasyon biriktirdiği ve kullandığı da söylenmelidir. İktidarın, iktisadi iktidarın gündelik olarak nasıl işlediği bilinmezse iktisadi bilgiden hiçbir şey anlaşılamaz. İktidarın işleyişi sürekli olarak bilgi yaratır ve aksi yönde, bilgi de iktidar etkilerine yol açar. Bilgi olmadan iktidarın sürdürülmesi olanaksızdır, bilginin iktidar doğurmaması olanaksızdır.”

Foucault, iktidar ilişkilerinin bilgi üretimine etkisini ise şu şekilde ifade etmektedir:¹⁹

“İkisinin (iktidar ve bilginin) kesin biçimde birbirine bağlı olduğunu söylemedim. Platon'dan bu yana, bilginin iktidardan tamamen bağımsız olarak var olamayacağı bilinmektedir. Bu, bilginin siyasi iktidara tabi olduğu anlamına gelmez, çünkü nitelikli bir bilgi bu koşullardan doğamaz. Bilimsel bir bilginin gelişimini, iktidar mekanizmalarındaki değişimler dikkate alınmadan anlamak olanaksızdır. Tipik örnek, ekonomi bilimidir. Fakat biyoloji gibi bir bilim de tarımdaki gelişmeler, dış ülkelerle ilişkiler ya da sömürgelerdeki tahakküm gibi karmaşık unsurlara göre evrildi. İktidar mekanizmalarını düşünmeden bilimsel bilginin ilerlemesi düşünülemez.”

Toplum veya kişiler üzerinde kontrolü temin etmek için bilgi toplamak, bilgiyi ele geçirmek için de denetimin temel araçlarından birisi olarak gözetleme faaliyetleri yapılmaktadır. Dolayısıyla bilgi, gözetim ve gözetim toplumu için de önemli bir kavramdır. Şu ana kadar anlatılanlar bilginin denetim faaliyetlerindeki önemi üzerine odaklanmıştır. Bu aşamadan sonra “bilgi” kavramı üzerine yoğunlaşılacaktır. Öncelikle bilgi kavramından neyin anlaşılması gerektiğini ortaya koymak yerinde olacaktır. Türk Dil Kurumu Sözlüğü, bilişim anlamında bilgiyi “kurallardan yararlanarak kişinin veriye yönelttiği anlam” olarak tanımlamaktadır.²⁰

Bilgi, olguları ve olayları tanıma, anlama ve özellikle açıklama amacı güden eğitim, gözlem, araştırma, deneyim gibi araçlarla elde edilen ve bütün bunların insanın zihinsel eleğinden geçmesi neticesinde ortaya çıkan olgular veya fikirlerdir. Bilgiye, işlenmiş - değerlendirilmiş enformasyon da denilebilir. Örneğin, kredi kartı sahiplerinden temin edilen

¹⁸ Michel Foucault, *a.g.k.*, 2003, s.35 - 36.

¹⁹ *a.k.*, s.248.

²⁰ <http://www.tdk.org.tr/SozBul.aspx?Kelime=bilgi>, (Erişim Tarihi: 04.04.2013).

“enformasyon” kullanılmak suretiyle kredi kartı sahipleri hakkında yaş, cinsiyet, gelir durumlarına göre harcama alışkanlıkları, genelde faaliyet gösterdiği semt veya bölge konusunda bilgi sahibi olunabilir.²¹

Enformasyon, bir sistemin, kendi durumunu başka bir sisteme bildirmesi olarak ifade edilebilir. Bu bildirim, sistemin her durum için farklı bir biçime evrilebilecek bir işaret veya sinyal göndermesi şeklinde olmaktadır.²² Enformasyon yalnızca dil çevresinde bir bildirim değil sibernetik ve fiziksel bir işaret şeklinde de olabilir.²³ Enformasyon teknolojisi ise henüz işlenmemiş bilginin, yani enformasyonun belirli bazı amaçlar doğrultusunda toplanması, iletilmesi, bilgiye dönüşüm sürecinde işlenmesi ve depolanması amacıyla kullanılan donanım ve yazılımları ifade etmektedir.²⁴ Günümüzde enformasyon teknolojileri sadece yazı değil ses, görüntü, video şeklindeki enformasyon aktarım süreçlerini hızlı ve basit bir şekilde yapabilecek hale gelmiştir.

Kavramsal olarak enformasyon, veriyi ifade etmektedir. Bundan dolayı da enformasyon sınıflandırılabilme, doğrulanabilme, işlenebilme ve depolanabilme özelliklerine sahip olmaktadır. Daniel Bell enformasyona örnek olarak istatistikleri, raporları, vergi cetvellerini, mahkeme kararlarını göstermektedir.²⁵ Bilgiyi ise bazı sistematik formlar içinde, iletişim araçları yoluyla başkalarına aktarılan, temellendirilmiş yargılar ya da deneysel sonuçlar sunan, organize edilmiş gerçek ve düşünsel ifade bütünü olarak açıklamaktadır.²⁶ Bell bilgi kavramını kolektif bir üretimin sonucu olarak değerlendirmekte ve bundan dolayı da onu herkesin faydalanabileceği bir sonuç olarak görmektedir.²⁷

Manuel Castells’e göre ise bilgi, “mantıklı bir yargı ya da deneysel bir sonuç sunan, başkalarına sistemli bir biçimde iletişim aracıyla aktarılan olgulara ya da düşüncelere ilişkin örgütlü ifadeler dizisi”dir.²⁸ Bu kapsamda enformasyon ise örgütlenmiş ve iletilen bir veriyi

²¹ Hasan Gürak, “Teknolojik Yenilik ve Büyüme”, <http://www.hasmendi.net>, (Erişim Tarihi: 25.09.2012).

²² Aykut Göker, “Enformasyon Toplumu Üzerine Kavramsal Bir Yaklaşım Denemesi”, <http://www.inovasyon.org/pdf/AYK.Mulkiye.Der.Ag.01.pdf>, (Erişim Tarihi: 04.04.2013).

²³ Bedia Akarsu, *Felsefe Terimleri Sözlüğü*, TDK Yayınları, 1975.

²⁴ Nevzat Güldiken, “Türkiye’de Sanayi -Teknoloji - Kobi Politikalarına Eleştirel Bir Yaklaşım”, *C.Ü. İktisadi ve İdari Bilimler Dergisi*, Cilt 7, Sayı 2, 2006, s.143.

²⁵ Gürol Irzık, “Bilgi Toplumu mu, Enformasyon Toplumu mu? Analitik - Eleştirel Bir Yaklaşım”, *Bilgi Toplumu Geçiş: Sorunsallar, Görüşler, Yorumlar, Eleştiriler ve Tartışmalar*, Der. İlhan Tekeli. vd., Türkiye Bilimler Akademisi Yayınları, No.3, Ankara, 2002, s.54.

²⁶ Daniel Bell, “İletişim Teknolojisi: Gidişat Daha İyiye mi Yoksa Daha Kötüye mi?”, Çev. Ahmet Sevimli, *Sosyo-Ekonomik Perspektif*, Der. Uğur Dolgun, Asa Yayıncılık, Bursa, 2001, s.309.

²⁷ a.k, s.310.

²⁸ Manuel Castells, *Ağ Toplumu Yücelişi*, Çev. Ebru Kılınç, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2008, s.20.

ifade etmektedir.²⁹ Bilgi her şeyden önce bilen özne ile bilinen şey arasındaki ilişkinin konusudur. Bu bakımdan öznesiz bilgi olamaz ve bilgi yalnızca öznenin zihninde var olabilir. Özne açısından değerlendirildiğinde enformasyon yanlış olabilir ancak bilgi yanlış olamaz. Enformasyon öznesiz olabilir ve bilgisayar ortamı gibi çeşitli biçimlerde ya da ortamlarda var olabilir. Bu durumda bilgiyle enformasyon farklı şeylerdir.³⁰ Enformasyon doğrulanabilme ve değerlendirilme süreçlerinden geçip öznenin zihninde yer tutmaya başladığında bilgi haline evrilmiş olur.

Bilgi ve enformasyon kavramlarının yanında veya kavram kargaşası içerisinde onların yerine kullanılan “veri”nin ne olduğunu ve neyi kapsadığını ortaya koymak yerinde olacaktır. Bu kapsamda veri sayısal veya mantıksal her türlü değeri ifade etmektedir. Veri kendi başına değersizdir. Veri, bilgi işleme sürecinin temel hammaddesini oluşturur ve çeşitli sembol, rakam, harf, işaretlerle temsil edilen, ham, işlenmemiş gerçekler veya izlenimleri kapsar.³¹ Veri; miktarları, olguları, öğeleri temsil eden, rasgele bir araya gelmemiş bulunan sembollerden ve kavramlardan oluşan bir grup olarak da ifade edilebilir.³²

Yukarıda ifade edilen tanımlamalar ve değerlendirmeler paralelinde bilginin; verinin ve enformasyonun tecrübeler, algılar, düşüncüler, sezgiler, duygular, değerler, uzman görüşleri, üretim sonuçları ve doğal yetenekler gibi araçlar kullanılarak analiz, karar verme, planlama, karşılaştırma, değerlendirme, çözümleme, sentez gibi süzgeçlerden geçirilerek ortaya çıkan son şekli ifade ettiği söylenebilir.

2. Denetim, Yönetim ve İktidar

Denetim ve denetimle özdeşleşmiş olan gözetim, iktidarın gücünü pekiştiren bir unsur olarak tarihin her döneminde var olagelmıştır. Denetim faaliyetlerinin yönü ilk çağlarda daha çok şiddet ve baskı şeklindeyken; modern toplumların oluşmasıyla birlikte, denetim ve gözetim faaliyetlerinin yönü şiddet ve baskıdan yönetime kaymış ve sistematik bir hal almıştır. Günümüzde ise bilgi ve iletişim teknolojileri aracılığıyla toplumun her alanına derinlemesine nüfuz eder şekilde kendini göstermektedir.

Bu bölümde öncelikle Frederich Taylor’un “Bilimsel Yönetim Yaklaşımı” ve bununla üretim sürecinde kurmuş olduğu denetim, sonrasında Max Weber’in “Bürokrasi Yaklaşımı” denetime bakan yönüyle incelenecek ve akabinde de Karl Marx’ın “Kapitalist Emek

²⁹ a.k

³⁰ a.k, s.54.

³¹ Adem Ögüt, *Bilgi Çağında Yönetim*, Nobel Yayın Dağıtım, Ankara, 2001, s.9.

³² Recep Türkoğlu, “Bilişim Teknolojilerinden Bilgi Yönetiminde Yararlanma Düzeyi”, 01 Mayıs 2006. http://www.turkoglu.name.tr/by_makale.htm, (Erişim Tarihi: 25.10.2012).

Süreci”ne olan eleştirisi ve sermayenin emekçiden kazandığı artı - değer ile tekrar emekçi üzerinde kurmuş olduğu denetim, son olarak da bütün bu süreçlerin iktidara bakan yönü tartışılacaktır.

2.1. Taylor: Bilimsel Yönetim Yaklaşımı

Amerikalı bir mühendis olan Frederick Winslow Taylor, 1873 yılındaki kriz esnasında, motor işçisi olarak staj yapmış, değişik fabrikalarda görev almış ve çalıştığı fabrikada nihai olarak başmühendisliğe kadar yükselmiştir.³³ Bu süreçte yaptığı gözlemler neticesinde işletmelerde üretim sürecinde insan gücünden yeterince faydalanılamadığı düşüncesiyle işin yapılmasında etkili bilimsel yöntemlerin kullanılmasının gerekliliğini savunmuş ve bilimsel yönetim ilkeleri belirleyerek bilimsel yönetim yaklaşımını geliştirmiştir.

Taylor, her ne kadar bir teorisyen değil de pratisyense de işin yeniden örgütlenmesi ile ilgili geliştirdiği “bilimsel yönetim yaklaşımı” geniş etki uyandırmış, üretim sürecini tüm dünyada derinden etkilemiştir.³⁴ Nitekim geliştirdiği bu yaklaşım ilk olarak kendisini Ford’un 1908 yılında ürettiği ilk ucuz otomobil “Model T”nin üretim bantlarında göstermişken, 1930’lu yıllara gelindiğinde dünyadaki çoğu sanayi kuruluşlarının üretim sürecinin temelini oluşturmuştur.³⁵

Taylor, bilimsel yönetim yaklaşımını 1911 yılında yayımladığı “Bilimsel Yönetimin İlkeleri” (*İng; Principles of Scientific Management*) isimli kitabında açıklamaktadır. Buna göre Taylor bilimsel yönetimin ilkelerini dörde ayırır.³⁶ Birincisi, eski gelişigüzel yöntemlerin aksine işçinin her bir işlemini şekillendirecek bilimsel yöntemlerin kullanılması gerektiği ilkesidir. İkincisi, eskiden olduğu gibi işçinin yapacağı işi kendisi seçip, buna göre kendi yapabildiği kadar kendisini geliştirmesi yerine; her işçinin bilimsel olarak seçilip bilimsel olarak eğitilip, bilimsel olarak geliştirilmesi gerekliliğidir.

Üçüncüsü, önceden belirlenmiş olan bilimsel ilkelere uygun olarak işçilerin birbirleriyle uyumlu halde işbirliği içinde çalışmasıdır. Dördüncüsü, yönetim ile işçiler arasında eşit bir görev ve sorumluluk dağılımının gerekliliğidir. Eskiden görev ve sorumluluklar büyük oranda işçi üzerindeyken artık, yönetim işçilerden daha iyi yerine

³³ Hasan Şimşek, *Örgütler, Yönetim ve Liderlik: Liderliğe Çoklu Bakış*, ODTÜ Eğitim Fakültesi Eğitim Bilimleri Bölümü Yayını, Ankara, 2005, s.10.

³⁴ Fuat Man, “Kapitalist Emek Süreci Teorisi ve Dönüşümü”, *E-Akademi*, Aralık 2009, Sayı 94.

³⁵ <http://www.modelt.ca/background.html>, (Erişim Tarihi: 18.04.2014).

³⁶ Frederick W. Taylor, *a.g.k.*, s.23.

getirebileceği konularda işin tümünü devralır. Bu ilkeye göre işçilerin yönetimin görev alanına giren konulardan elini çekmesi gerekir.

Taylor tarafından belirlenen bu ilkeler çerçevesinde esasında yapılmak istenen şey, işçilerin performansları üstünde tam bir kontrol kurarak emek gücünden maksimum fayda sağlamaktır. Bu bakımdan Taylor üretimin zihinsel yanı ile fiziksel yanını birbirinden ayırmış ve üretim sürecini vasıfsız işçiler tarafından da yapılabilecek şekilde çok küçük parçalara bölmüştür. Bu şekilde eskiden olduğu gibi vasıflı işçilerin üretim sürecindeki kontrollerine son verilmiş, hem de vasıfsız daha az ücrete çalışan işçilerin her birinin çok küçük parçalara bölünmüş olan üretim sürecinin sadece kendisine uygun olan çok küçük parçalardan birisini yapması sağlanarak ve bunu süreklileştirerek işçiler bir anlamda robotlaştırılmıştır. Böylece aynı işi defalarca yapan işçi bunu sistematik haline dönüştürmüş ve üretim sürecinden daha çok çıktı, yani ürün alınmaya başlanmıştır. Dolayısıyla üretim sürecinde verimlilik sağlanmıştır.³⁷

Bilimsel yönetim yaklaşımı çerçevesinde işçiler makinenin birer çarkı gibi görülmüştür ve bundan dolayı üretim sürecine mekanik bir anlayış hakim olmuştur. Birey çevresinden soyutlanmış ve bireyin toplumsal çevresi dikkate alınmamıştır.³⁸ Diğer taraftan işçi kar peşinde koşan ekonomik bir varlık olarak değerlendirilmiştir. Nitekim bilimsel yönetim yaklaşımına göre işçilerin yüksek üretim yapması sonucu verimlilik artacak, bu artış sermayenin karını arttıracak, bu da işçilerin maaşlarına yansiyarak onların yüksek ücret almasını sağlayacaktır. Böylece işçinin üretim sürecinde işveren gibi daha çok doyuma ulaşacağı ileri sürülmüştür.³⁹

Taylor'un geliştirdiği bilimsel yönetim modeli işçinin ve üretim sürecinin yoğun bir şekilde denetim altına alınmasını içermektedir. Esasında Taylor'un bu modeliyle bir anlamda denetim ve gözetim faaliyetleri tam anlamıyla sistematikleştirilmiş ve pratiğe dökülmüştür.⁴⁰ Bilimsel yönetim modelindeki denetim halini Munck şöyle ifade eder:⁴¹

“Zor her zaman vardır: makine, montaj hattı, denetçi, içerde ve dışarıda saat tutulması ve fabrika rejiminin denetim aygıtının bütünü. Mekanikleşmenin kendisi ve emek sürecinde mekanikleşmeye bağlı olarak gerçekleşen değişimler, denetim araçları olarak işleyebilirler.”

³⁷ Yusuf Zamir, “1917 Devriminin Boğuluşu”, *Yaşayan Marksizm*, Sayı 3, İstanbul, Ocak 2012, s.127.

³⁸ Erol Eren, *Örgütsel Davranış ve Yönetim Psikolojisi*, Beta Yayınları, İstanbul, 2008, s.13 - 14.

³⁹ a.k

⁴⁰ Phil Slater, *Frankfurt Okulu*, Kabalcı Yayınları, İstanbul, 1998, s.176., akt., Aslıcan Kalfa, Hakan Topateş, “Çalışma İlişkilerinde Denetimin Gizilleşmesi Bağlamında Elektronik Gözetim Pratiklerinin Otoritesi”, *Sosyal Haklar Ulusal Sempozyumu*, s.438., www.sosyalhaklar.net, (Erişim Tarihi: 03.02.2013).

⁴¹ Ronaldo Munck, *Uluslararası Emek Araştırmaları*, Öteki Yayınları, Ankara, 1995, s.218., akt., Aslıcan Kalfa, Hakan Topateş, a.g.k, s.438.

Taylor'un ilkelerinin üretim süreci üzerindeki denetimi öyle güçlüdür ki bu özelliğinden dolayı, işyerinde denetimi sağlama amaçlı olarak kapitalist ülkelerde olduğu kadar, eski SSCB ve Doğu Avrupa ülkelerinde de yaygın bir şekilde uygulanmıştır. Bu durum da şunu göstermektedir ki bilimsel yönetim modeli kar etme aracı olduğu kadar işyerinde denetim kurmanın da aracı olarak uygulanmıştır.⁴² Bu denetim gücünün kaynağı da bilimsel yönetim modelindeki tasarımı ve uygulamayı birbirinden ayırarak, tasarımı yani üretime ait bilgi tekeliyi yönetime devretmesinden kaynaklanmaktadır. Böylece yönetim, üretim sürecinin araçları olarak görülen işçiler üzerinde doğrudan ve teknik denetim yapma gücüne haiz olmuştur.⁴³

2.2. Weberyen Bürokrasi ve Denetim

Bürokrasiyle ilgili Max Weber'in yaklaşımını incelemek için öncelikle "Weberci egemenlik"⁴⁴ anlayışını anlamak gerekir. Weber, egemenlik kavramını bir ya da birden fazla kişinin bir toplumsal eylem içinde, o eyleme katılan başkalarının direnişine karşın da olsa, kendi iradelerini gerçekleştirme şansı olarak ifade etmektedir.⁴⁵ Egemenlik üç kategoride ele alınmıştır. Birinci kategori, geleneksel olarak gücü elinde tutan ve kullananların, halkın gözünde süregelen meşruiyetine dayanan "geleneksel egemenliktir". Bu egemenlik toplumsal kalıtsal üstünlüklere bağlıdır. İkinci kategori "karizmatik egemenliktir"; bu egemenlik, kutsallığa, kahramanlığa, olağanüstü karaktere dayalıdır. Son kategori "rasyonel - hukuki egemenliktir"; bu egemenlik kuralların yasallığına ve bu kurallara göre yönetimi elinde tutanların emir verme hakkı olduğuna inanmaya dayanır.⁴⁶

Yukarıda ifade edilen egemenlik türlerinden rasyonel - hukuki egemenlik diğerlerinden daha üstündür. Bunun nedeni de egemenliğin doğruluğuna herkesçe inanıldığından dolayı kabul görmesinden kaynaklanmaktadır.⁴⁷ Nitekim Weber bu durumu şu şekilde ifade etmektedir:⁴⁸

"Rasyonel hukuki otorite normatif kuralların yasallığına olan inanca ve bu kurallar doğrultusunda emirleri vermek üzere yetkilendirilmiş kişilerin hakkı olduğu düşüncesine dayanır."

⁴² Gareth Morgan, *Metafor*, Çev. Gündüz Bulut, Mess Yayınları, İstanbul, 1998, s.38.

⁴³ Gamze Yücesan Özdemir, "Emek Süreci Teorisi ve Türkiye'de Emek Süreci Çalışmaları Üzerine Bir Değerlendirme", *Küreselleşme, Emek Süreçleri ve Yapısal Uyum*, Der. A. A. Dikmen, İmaj Yayıncılık, Ankara, 2002, s.441 - 442.

⁴⁴ Bu ifade doktrinde "Otorite" veya "İktidar" olarak da kullanılmaktadır. Bölüm boyunca "Egemenlik" kavramı kullanılacaktır.

⁴⁵ Max Weber, *Sosyoloji Yazıları*, Çev. Talha Parla, Deniz Yayınları, İstanbul, 2006, s.281.

⁴⁶ Hasan H. Çevik, *Türkiye'de Kamu Yönetimi Sorunları*, Seçkin Yayınları, Ankara, 2004, s.67 - 68.

⁴⁷ Kurthan Fişek, *Yönetim*, Paragraf Yayınevi, Ankara, 2005, s.111.

⁴⁸ Max Weber, *The Theory of Social and Economic Organisation*, Trans. A.M.Henderson, T. Parsons Glencoe, III Free Press, 1947, s.328., akt., Hasan H. Çevik, *a.g.k.*, s.68.

Weber, rasyonel hukuki egemenlik kavramını bürokratik egemenlik ile eşdeğer görür ve bürokrasinin kuruluşunun hukuki, işleyişinin de rasyonel olması gerektiğini ifade eder. Bürokratik egemenliğin işleyişinde yasalar ya da yönetsel yönetmeliklerce düzenlenmiş belirli bir resmi yetki alanları ilkesi olarak ifade edilebilecek olan kurallar hakimdir.⁴⁹ Bürokratik yapının amaçlarının hayata geçmesi için oluşturulan düzenli çalışmalar, resmi görevler olarak belirlenmiş çizgiler ve bu resmi görevleri gerçekleştirecek olan görevlilerin fiziksel, dinsel gibi çeşitli araçlarına yönelik tespit edilen kurallarla net olarak sınırlandırılmıştır. Belirtilen resmi görevlerin düzenli ve devamlı surette yürütülmesi ile bu süreçte kullanılacak olan yetkiler sistematik hükümler altına alınmıştır.⁵⁰ Weber sınıflandırdığı diğer egemenlik türlerinden üstün gördüğü rasyonel - hukuki egemenlik anlayışını bürokrasi ile eklemler ve bürokrasinin bu egemenlik anlayışını temin etmede önemli bir vasıta olduğunu kabul eder; bu bakış açısıyla yönetim bilimlerinde önemli bir yeri olan bürokrasi kuramını oluşturur.⁵¹

“Bürokrasi Kuramı” özellikle kamu yönetimi disiplinde klasik okulda hususi bir yeri olan ve uzun yıllar genel kabul görmüş, getirmiş olduğu ilkelerin de birçok örgütün kurulma ve evrim sürecinde yer tuttuğu bir yaklaşımdır. Bu yaklaşım, işlerin geciktirilmesi, gereksiz uzayıp giden formaliteler, kırtasiyecilik gibi eleştirilerin aksine hiyerarşik örgütsel bir yapıyı ve onun rasyonel çalışması için kabul edilen ilkeleri ifade etmektedir.⁵² Weber tespit ettiği ilkeler ile ortaya koyduğu bürokrasi modelini idealize eder ve örgütlerin bu modelin gereksinimlerine yaklaştıkları ölçüde bürokratik olacaklarını anlatır.⁵³ Ayrıca bürokrasi modelini endüstriyel kuruluşlar, politik örgütler, kilise ve benzeri dinsel örgütler için de geçerli olmakla birlikte daha çok kamusal örgüt yapılanmaları için tasarlamıştır.⁵⁴

Bürokratik örgütlenme diğer tüm öteki örgütlenme biçimlerinden üstündür. Bu üstünlüğünün altında da sahip olduğu teknik özellikleri yatmaktadır. Bu noktada ideal anlamda oluşmuş olan bürokratik yapının üstünlüğünü makineyle yapılan üretimin, makineyle yapılmayan tüm öteki üretim biçimlerine olan üstünlüğüne eşdeğer göstermektedir.⁵⁵ Bürokrasi kuramı çerçevesinde bürokratik örgütlerin mutlaka benimsemesi gerektiği düşünülen ilkeler beş ana başlık altında sınıflandırılabilir. Birincisi; belirli kurallarla düzenlenmiş bir faaliyet ve yetki alanının olmasıdır. Örgüt içindeki devamlılık ve nizam bu

⁴⁹ Max Weber, *a.g.k*, 2006, s.321.

⁵⁰ *a.k*

⁵¹ Kurthan Fişek, *a.g.k*, s.111.

⁵² Tamer Koçel, *İşletme Yöneticiliği*, Beta Yayınları, İstanbul, 1998, s.138 - 139.

⁵³ Kurthan Fişek, *a.g.k*, s.114.

⁵⁴ Claude Lefort, “What is Bureaucracy?”, s.4. www.generation-online.org/h/plefort, (Erişim Tarihi: 10.10.2012).

⁵⁵ Max Weber, *a.g.k*, 2006, s.303.

kurallara bağlıdır. Bu özellik aynı zamanda bürokrasinin biçimsel oluşunu da ifade etmektedir. İkincisi; personelin örgütlenmesinin hiyerarşi esasına dayanmasıdır. Buna göre hiyerarşik yapının bir gereği olarak her bir alt birim, üst birimin denetim, sorumluluk ve gözetimi altına girer ve her bir üst, kendi astlarının eylem ve işlemlerinden, üstlerine karşı sorumludur.⁵⁶

Üçüncüsü, genel olarak resmi faaliyet ile özel yaşam alanının birbirinden ayrılmış olması gerekliliğidir. Dördüncüsü, görevlilerin seçimle değil, işin gereksinimleri çerçevesinde liyakate göre atanarak işe başlamasıdır. Bu kapsamda uzmanlaşmış bürokratik yapıdan bahsedilebilir. Beşincisi; görevlilere hiyerarşik yapıya göre belirlenmiş olan ücretlerinin düzenli ödenmesi gerektiğidir.⁵⁷

Denetim açısından bakıldığında bürokrasinin, onu denetleyenlerin elinde teknik yönden en üstün iktidar aracı olduğu ifade edilebilir.⁵⁸ Denetimin yönü ise yapılan faaliyetlerin önceden belirlenmiş olan kurallara uygun yapılıp yapılmadığı ve bürokratik yapı içerisindeki ilişkilerin hiyerarşik çerçevede olması şeklindedir.⁵⁹ Weber bürokrasiyi rasyonellikle, rasyonelleşme sürecini de mekanikleşme, ilişkilerin ve kuralların boyunduruğu altında çok resmi ve boğucu tekdüze işleyişiyle özdeşleştirmektedir. Bu bağlamda rasyonellik ise kişi üzerinde baskıcı bir etki oluşturarak onun özgürlüğünü kısıtlar görünmektedir.⁶⁰ Nitekim Weber bu durumun da farkında olarak kurallarla çevrelenmiş bürokratik örgütlenmenin “çelik bir kafese” döneceğini ve sıradan insanların bu kafesin içinde avlanmış gibi tutsak kalacağını öngörmüştür.⁶¹

2.3. Marksist Emek Süreci Teorisi ve Denetim

Karl Marx’ın (1818 - 1883) yaşadığı dönem, sanayi devriminin etkisi ile kapitalizmin yükseldiği dönemdir. Bu nedenle kapitalizmi ve kapitalist iktidarı tartışmış, bu tartışmada da kapitalist emek sürecini kapitalizmin ortaya çıkardığı bütün sorunların, bütün eşitsizliklerin temelinde yatan etmen olarak değerlendirmiştir.⁶² Bu bakımdan günümüzde başta işyerinde olmak üzere toplumsal denetim ve gözetim faaliyetlerini doğru analiz etmede Marx’ın emek süreci teorisini ve bakış açısını anlamanın önem arz ettiği düşünülmektedir.

⁵⁶ Bilal Eryılmaz, *Bürokrasi ve Siyaset: Bürokratik Devletten Etkin Yönetime*, Alfa Yayınları, İstanbul, 2004, s.44 - 45.

⁵⁷ a.k

⁵⁸ Max Weber, a.g.k, 2006, s.328.

⁵⁹ Murat Önder, “Toplam Kalite Yönetimi, Kamu Sektöründe Uygulanması ve Karşılaşılan Sorunlar”, *Türk İdare Dergisi*, s. 416, Eylül 1997, s. 119.

⁶⁰ Max Weber, a.g.k, 2006, s.96.

⁶¹ David Murakami Wood, a.g.k, 2006, s.6.

⁶² Gamze Yücesan Özdemir, a.g.k, 2002, s.437.

Bu bölümde Marx'ın emekçi, emek, emek gücü, artı değer, üretim araçları, kapitalist kavramları çerçevesinde kapitalist emek süreciyle neyi ifade ettiği ve bu kapsamda sermaye sahiplerinin emekçinin emek gücünü sömürmesiyle ortaya çıkan artı değer ile emekçiler üzerinde oluşturduğu denetim gücü anlatılmaya çalışılacaktır.

Marx'ın yabancılaşma, toplumsal sınıflar, sınıf çatışması ve devlet kavramlarına olan yaklaşımını, kapitalist düzene olan tavrını, kapitalist emek sürecine olan eleştirisini ve bununla ilgili ortaya koyduğu teoriyi anlamak; yani Marx'ı doğru kavramak için onun emek kavramını nasıl algıladığını, emeğin fonksiyonlarını nasıl değerlendirdiğini bilmek gerekir. Zira onun bütün yaklaşımlarında çıkış noktası olarak merkeze emeği ve emeğin yabancılaşmasını oturttuğu ileri sürülebilir.⁶³

Emek, maddi üretimle sınırlanmaksızın insanın kendi kendisini gerçekleştirdiği, insanın hem düşünsel hem de bedensel yetilerini içeren kapsamlı bir etkinliktir. Bu bakımdan emek, değer özünü ve içsel ölçüsüdür; ancak emeğin kendisinin değeri yoktur. İnsan emeğinin varlığıyla kendisini bir tür olarak doğada ve bir birey olarak toplum içinde gerçekleştirir.⁶⁴

Yukarıda belirtilen emek kavrayışı bakımından Marx, emek kavramını ontolojik (varlıkbilimsel) ve teleolojik (amaç bilimsel) boyutlarıyla ele almaktadır. Emek kavramının ontolojik boyutu emeğin insanın varlığını sürdürmesinde zorunlu bir unsur olması demektir.⁶⁵ Bu durumu kendisi şöyle açıklar:⁶⁶

“Bunun için, kullanım-değerinin yaratıcısı olarak emek, yaralı emektir, bütün toplum biçimlerinden bağımsız olarak, insanoğlunun varlığı için zorunlu bir koşuldur; bu ezeli ve ebedi doğal zorunluluk olmaksızın insan ile doğa arasında madde alışverişi ve dolayısıyla da yaşam olamazdı.”

Emek kavramının teleolojik boyutu ise emeğin salt insana özgü olarak amaçlı bir etkinlik olmasını ifade eder.⁶⁷ Yani insan, emeği aracılığıyla hedeflediği amaç veya amaçlarına ulaşmadan önce onu imgesel olarak planlayabilme yetisine sahiptir. Yani, üretici insan, yapacağı işi hem oluşturacağı ürün hem de bu ürünün üretim süreci açısından önceden tasarlama gücüne sahiptir.⁶⁸ Marx bu durumu da şöyle ifade etmektedir:⁶⁹

“Biz, şimdi burada, bize hayvanı anımsatan ilkel içgüdüsel iş biçimleriyle ilgili değiliz. İnsanın emek-gücünü pazara bir meta olarak satmak için getirdiği durum ile başlangıçtaki içgüdüsel aşamasında olan insan emeğinin durumunu birbirinden ayıran çok büyük bir zaman aralığı vardır. Biz, emeği, salt insana özgü biçimi içerisinde ele alıyoruz. Örümcek, işini dokumacıya benzer şekilde gördüğü gibi, arı da

⁶³ Alaattin Bilgi, *Kapital Okuma Klavuzu*, Evrensel Yayın, İstanbul, 2005, s.203.

⁶⁴ Doğan Göçmen, “Marx'ın Emek Kavramının Bugün Yürütülen Tartışmalar İçin Önemi Üzerine”, 2009, s.4. <http://dogangocmen.wordpress.com>, (Erişim Tarihi: 15.12.2013).

⁶⁵ a.k

⁶⁶ Karl Marx, *Kapital*, Çev. Alaattin Bilgi, Sol Yayınları, Ankara, 1993, s.57.

⁶⁷ Doğan Göçmen, a.g.k, s.4.

⁶⁸ Fuat Man, a.g.k

⁶⁹ Karl Marx, a.g.k, 1993, s.194.

peteğini yapmada pek çok mimarı utandırır. Ne var ki, en kötü mimarı en iyi arıdan ayıran şey, mimarın, yapısını gerçekte kurmadan önce, onu imgesinde kurabilmesidir.”

Emek ve emek gücü kavramları da birbirinden ayrı unsurlar olarak değerlendirilmektedir. Bu ayrımdaki çıkış noktası ise işçinin sattığı şeyin emek değil emek gücü olduğunu ortaya koymasıdır. Marx’a göre emek gücünün emekten farklı olarak bir kullanım değeri bulunmaktadır. Bu durumu şu şekilde ifade eder:⁷⁰

“...paranın, yani gerçekleşmiş emeğin canlı emekle doğrudan değişimi, ya kapitalist üretim temeli üzerinde serbestçe gelişmesine henüz başlamış bulunan değer yasasını, ya da doğrudan doğruya ücretli emeğe dayanan kapitalist üretimin kendisini ortadan kaldırır.”

Emek piyasasında kapitalistin karşısına çıkan emek değil işçi; yani emekçidir ve bu andan itibaren işçi ile kapitalist arasındaki ilişkinin konusu onun emeği olamaz, ancak emek gücü olabilir. Marx bunu şöyle biçimler:⁷¹

“Onun emeği, fiilen harcanmaya başlar başlamaz, artık, ona ait olmaktan çıkmıştır ve bunun için de bu emeğin şimdi onun tarafından satılması söz konusu olamaz. Emek, değer öz ve değer için ölçüsüdür, ama kendisinin değeri yoktur.”

Kapitalist, emek gücünü satın aldıktan sonra tek amacı mümkün olan en yüksek karı elde edebilmek için, emekçinin mümkün olduğu kadar uzun ve en yoğun bir şekilde işletilerek artı değer üretilmesidir. Zaten kapitalist, emek gücünü bu amaçla satın almıştır. Kapitalist, emek gücünü satın aldığı işçiyi çalıştırarak bu emek gücünü tüketir ve belli bir kullanım değeri olan bir nesne üretilmesini sağlar. Bu noktada esasında emek süreci bir üretim faaliyeti, kullanım değerlerini üretme sürecini ifade etmektedir.⁷²

Emek sürecinde denetim işçinin emek gücünü kapitaliste sattığı anda başlar. Denetimin yönü ise işin olması gerektiği gibi yapılması, üretim araçlarının minimum tüketim ve maksimum kar elde edilecek şekilde kullanılmasının ve emek gücünün yoğun bir şekilde işletilmesinin sağlanması şeklindedir.⁷³ Denetimi yapan da kapitalistin, yani emek gücünü satın alanın kendisidir. Emek süreci sonunda üretilen ürün emekçinin, yani üreten işçinin değil kapitalistindir. Kapitalist, emek gücünün zamana göre değerini ödediği takdirde bu gücü o zaman sürecinde kullanma hakkını elde etmiştir demektir. Bu durumda esasında emekçi ve emek gücü metalaşmaktadır.⁷⁴

Buraya kadar olan kısım aslında emek sürecini ifade etmektedir. Zira emekçi, emek gücünü satmakta ve emek gücünün bedeline denk ürün ortaya çıktığında emek süreci

⁷⁰ a.k, s.548.

⁷¹ a.k, s.549.

⁷² Alaattin Bilgi, a.g.k, s.108.

⁷³ Harry Braverman, *Labour and Monopoly Capitalism*, Monthly Review Press, New York, 1974, s.54., akt. Gamze Yücesan Özdemir, a.g.k, 2002, s.440 - 441.

⁷⁴ Karl Marx, a.g.k, 1979, s.201.

bitmektedir. Fakat artı değer üretilmemiştir, dolayısıyla meta üretiminin kapitalist biçimi gerçekleşmemiştir. Nitekim Marx bunu şöyle ifade etmektedir:⁷⁵ “(...) artı değer üretme sürecinin, belli bir noktanın ötesine uzatılmış bir değer yaratma sürecinden başka bir şey olmadığını görürüz.” Bu noktada kapitalist üretim sürecini, kullanım değerleri üreten yararlı emekten ibaret olan emek süreci ile artı değer üretme sürecinin birliği şeklinde ifade edebiliriz.⁷⁶

Kapitalist, kapitalist emek sürecinde, üretimi için kullanılan üretim araçlarının ve emek gücü değerinin toplamından değeri daha fazla olan değişim değeri niteliğine sahip kullanım değerleri üretmeyi hedefler. Dolayısıyla buradan kapitalistin hedefinin sadece kullanım değeri olan bir meta üretmek değil, artı değer üretmek olduğu anlaşılır ki bu durum kapitalist emek sürecinin temel dinamiğini oluşturmaktadır.⁷⁷

Yukarıdaki durumu bir önekle açıklayalım. Örneğin cam kavanoz⁷⁸ imalatında üretilen cam kavanozun değeri, bu ürünün üretilmesinde kullanılan üretim araçları ile emek gücünün değerinin toplamına eşittir. Burada emek gücünün bir günlük değerinin 4 saatlik emek gücüne tekabül ettiğini farz ettiğimizde, emekçiye bir günlük emek gücü değeri olan 4 saatin karşılığı para⁷⁹ olarak ödenir. Burada işçinin dört saat çalışmasıyla üretilen ürünün değişim değeri ile işçinin emek gücünün değeri eşittir. Ancak bu durumda kapitalist kar elde edemeyecektir. Bunun için emekçinin emek gücünü arttırması, yani 4 saat emek gücünün üzerine 5 saat daha emek gücü koyması istenecektir. Fazladan olan bu 5 saatlik emek gücü kapitalist için artı değer üretecektir. Dolayısıyla burada ilk dört saat, emek gücü değerini ifade ederken, diğer 5 saat emek gücü artı değerini ifade etmektedir. Bu artı değer neticesinde ortaya çıkacak olan ürünün değişim değeri tamamen kapitalistin olacak ve özne⁸⁰ olan emekçi ortaya çıkardığı ürün olan nesneden ayrıştırılacaktır.⁸¹

⁷⁵ a.k, s.197.

⁷⁶ Elif Aksu Kaya, *Emek Süreçlerinde Dönüşüm ve Mühendis Emeği*, Elektrik Mühendisleri Odası E-Kitap Yayını, Ankara, 2012, s. 18 - 23. www.emo.org.tr, (Erişim Tarihi: 12.04.2013).

⁷⁷ Alaattin Bilgi, a.g.k, s.110 - 111.

⁷⁸ Marx, artı değeri anlatırken iplik eğirme işini örneklemektedir. Bu süreç farklı bir metafor seçilerek anlatılmaya çalışılmıştır.

⁷⁹ İşçinin emeği karşılığı aldığı ücretin yarattığı yanılsama Marx tarafından “meta fetişizmi” olarak adlandırılmaktadır. Meta fetişizmi, özne olan emekçiden, emekçi tarafından üretilen nesne olan ürünü birbirine yabancılaştırmaktadır. Böylece emek gücü ile ürünler arasındaki ilişki metalararası ilişkiye dönüşmektedir ki bu da emek ile sermayenin eşitsiz ilişkisini gizler. Tülin Öngen, “Marx ve Sınıf”, *Praksis*, Sayı 8, s.18.

⁸⁰ Kapitalist emek sürecinde Marx’a göre üç temel öge vardır. Bunlar; 1) Bir amaca yönelik insan eylemi yani emek, 2) İşin nesnesi (hammadde) ve 3) Üretim araç ve gereçleridir. Bunlardan ilk öge üretimin öznel koşuluken, son iki öge üretimin nesnel koşullarını oluşturmaktadırlar. Bu ögeler, bir üretim için gerekli önkoşullardır. Kaynak: Fuat Man, a.g.k

⁸¹ Alaattin Bilgi, a.g.k, s.110 - 111.

Kapitalist emek sürecinde artı değerin üretimiyle kapitalist sadece kar elde etmez; aynı zamanda denetimde kullanacağı egemenlik gücünü de elde eder. Bu bakımdan kapitalist emek sürecinin, artı değerin üretilmesi sonrasında ortaya çıkan siyasal ve toplumsal süreçlerin ve sömürü ilişkisinin şekillenmesinde de başat rol aldığı ifade edilebilir.⁸²

2.4. Teknoloji, Denetim ve İktidar

İktidarı; Marx sınıf ilişkilerinde; Weber geleneksel, karizmatik ve bürokratik kurumlarda gösterirken; Foucault onu hayatın günlük rutini içinde göstermeyi amaçlar. İktidarı gündelik toplumsal ilişkilerde somutlaştırır. Ona göre her insani ilişki bir sosyal ilişki, her sosyal ilişki bir iktidar ilişkisidir. Foucault çalışmalarına özneyi çözümlemek amacı ile başlamıştır, ancak iktidarın öznenin şekillenmesinde temel öge olduğunu farkedince iktidar kavramı üzerinde yoğunlaşmıştır. Bu durumu şöyle ifade eder:⁸³

‘Hedefim, iktidar fenomenini analiz etmek olmadığı gibi, böyle bir analizin temellerini atmak da değildi. Tam tersine amacım, bizim kültürümüzde, özneye dönüştürülme kiplerinin bir tarihini oluşturmaktır.’

Bu kapsamda iktidar belli bir kişiye ya da kişilere, zümreye ya da gruba ait değildir. Ona göre iktidarın kaynağı belli bir tarihsel dönem içerisinde ortaya çıkan çeşitli kapatma kurumlarıdır.⁸⁴ İktidar, yasalar bütününden ya da bir devlet aygıtından, hegemonik kastlar sorunlarından daha farklı biçimde karmaşık, daha farklı biçimde yoğun ve yaygındır.⁸⁵ Nitekim bireylerin gündelik davranışlarında onların bedenlerine varıncaya kadar genişlemiş, görünmez, sınırsız hareket kabiliyetine sahip bir eylem ve ilişki biçimi halini almıştır.⁸⁶

Foucault’nun iktidar çözümlemesinin önemli bir boyutu, bilgi - iktidar ilişkisidir. Ona göre bilgi, iktidarın en önemli denetim araçlarından biridir ve bu noktada iktidarın bilgi nesnelerini kendisinin oluşturduğunu şöyle ifade eder:⁸⁷

“İktidarın kendisi yeni bilgi nesneleri yaratır ve ortaya çıkmalarını sağlar ve yeni bilgi cisimleri biriktirir... İktidarın uygulanması daimi olarak bilgi yaratır ve buna karşılık olarak, bilgi iktidarın etkilerini pekiştirir... İktidarın bilgi olmaksızın uygulanması imkansızdır, bilginin iktidar yaratmaması imkansızdır.”

⁸² Gamze Yücesan Özdemir, “Despotik Emek Rejimi Olarak Taşeron Çalışma”, *Çalışma ve Toplum*, Sayı 4, 2010, s. 37. Marksist Emek Süreci ve Denetim ilişkisinde ayrıntılı bilgi için Gamze Y. Özdemir’in “Emek Süreci, Denetim ve Emek Rejimleri: Taşeron Çalışma Üzerine İlk Notlar” isimli makalesi ve *İletişim, Emek ve Kalkınma: Ekonomi Politik Yaklaşım* (2008) isimli kitabı incelenebilir.

⁸³ Michel Foucault, *a.g.k.*, 2000, s.57 - 58.

⁸⁴ Joseph Rouse, “Power/Knowledge”, *The Cambridge Companion to Foucault*, Ed. Gary Gutting, Cambridge University Press, Cambridge, 1994, s. 92 - 114., akt., Aslıcan Kalfa, Hakan Topateş, *a.g.k.*, s.435 - 436.

⁸⁵ Michel Foucault, *a.g.k.*, 2003, s.98.

⁸⁶ *a.k.*, s.48.

⁸⁷ Barbara Townley, “Foucault, Power/Knowledge, and Its Relevance for Human Resource Management”, *Academy of Management Review*, 1993, s. 521., akt., Aslıcan Kalfa, Hakan Topateş, *a.g.k.*, s.441.

Bilgi nesnelerini oluşturma konusunda Foucault'nun gayreti yukarıda ifade ettiği gibi bilginin iktidar için vazgeçilmez oluşundan kaynaklanmaktadır. Bu noktada iktidarın sürekliliği bilginin sürekliliği ile paralellik arz eder.⁸⁸ Günümüz bilgi ve iletişim araçları da bu kapsamda değerlendirilebilir. Günümüzde iktidarın bireyleri denetim altında tutabilmek, onlara dair her şeyi bilmek, her şeye hakim olmak için teknolojik gelişmeleri fırsat bildiği ve teknolojiyi yoğun kullanan bireye dair olanları bu araçlarla topladığı söylenebilir.

Marx'a göre "toplum tarihi sınıf mücadeleleri tarihi"dir.⁸⁹ Bu kapsamda iktidar, sınıflar arasında bir bölüşümü ifade etmektedir. Onun açısından bu sınıf mücadelesinin çıkış noktasında sermaye sahiplerinin emekçileri sömürerek elde ettikleri artı değer ile sermayelerini arttırma ve hem üretim sürecinde hem de sahip oldukları ekonomik güç sayesinde toplumsal anlamda diğer sınıflar üzerinde hakimiyet kurma çabaları yer almaktadır.⁹⁰

Weber, Marx gibi iktidarı sınıflar arasında bir bölüşüm olarak görmez; iktidarı, farklı sınıf, statü grupları ve partiler arasında güç etkileşimi ve paylaşımı olarak değerlendirir.⁹¹ Weber'e göre iktidar bir olasılıktır, toplumsal aktörlerden herhangi birinin, gücünü nereden aldığı önemli olmaksızın diğerlerine rağmen kendi iradesini gerçekleştirebilme olasılığıdır. Weber bunu "...Bir toplumsal ilişki içinde, neye dayalı olursa olsun, kendi istencini, dirençleri bile aşıp yerine getirebilme olasılığını anlatır." şeklinde ifade eder.⁹² Bu kapsamda insanlar arasındaki her türlü ilişkinin iktidarın konusunu veya kapsamını oluşturabileceği söylenebilir.

İktidar nicel bir kavramdır, ölçülemez. Örneğin kitap basarak kar etmeyi hedefleyen iki üretici arasında birisi kaliteli kitaplar basarak kar edemezse, diğeri kaliteli kitap üretememesine rağmen kar ederse, bu iki üreticiden hangisinin iktidar sahibi olduğu net değildir. Bu bakımdan iktidar kavramı sosyolojik olarak şekilden yoksundur, onun tam olarak sınırlarını çizmek kolay olmaz.⁹³ Bu bakımdan Weber iktidar ve iktidar ilişkilerini genel olarak incelemek yerine onun daha dar bir alanı olan "egemenlik" kavramına yönelmiştir.

⁸⁸ Michel Foucault, *a.g.k*, 2003, s.35.

⁸⁹ Karl Marx, Friedrich Engels, *Komünist Parti Manifestosu*, Çev. Yılmaz Onay, Evrensel Yayın, İstanbul, 2007, s.46.

⁹⁰ Tülin Öngen, *a.g.k*, s.20.

⁹¹ Max Weber, *a.g.k*, 2006, s.240.

⁹² Max Weber, *Toplumsal ve Ekonomik Örgütlenme Kuramı*, Çev. Özer Ozankaya, İmge Kitapevi, İstanbul, 1995, s.92.

⁹³ *a.k*

Weberyan anlayışta egemenlik kavramı geleneksel, karizmatik ve rasyonel - hukuki olmak üzere üçe ayrılır ve bunlardan rasyonel - hukuki egemenliğin diğerlerine üstün olduğu, bunun iktidarın kaynağı olarak görüldüğü kabul edilir.⁹⁴ Weber, rasyonel - hukuki otoritenin şekil bulduğu bürokrasi ile tüm modern kurum ve işletmelerde bireylerin denetim ve gözetim altında tutulduğunu kabul eder.⁹⁵ Bu çerçevede bireyi çelik bir kafes içerisinde yaşamaya mecbur bırakılmış olarak görür.⁹⁶ Daha geniş perspektifte ise bürokrasinin “sınırları çizme” ihtiyacından dolayı doğum ve ölüm kayıtları, nüfus ve kimlik bilgileri, sicil dosyaları, ikametgah bilgileri, elektrik, su, askerlik, telefon idaresi kayıtları vs. belgelerle insanları doğumlarından ölümlerine kadar olan süreçte devamlı izlediği ve hakkında bilgi topladığı görülür.⁹⁷

Marx, Weber ve Foucault’nun iktidar tanımlamaları birbirinden farklı olsa da üçünde de ortak olan iktidar sahibi belli bir sınıfın, kişinin, grubun hangisi olursa olsun diğerleri üzerinde iktidar olmanın verdiği güç ile denetim ve gözetim faaliyetleri içerisinde bulunduğudır. Marx’ta denetim - gözetim süreci emek gücünden maksimum faydayı sağlamak için emek gücünü satanın ve üretim sürecinin denetimi iken, Weber’de bürokrasinin kurallara uygun bir şekilde devamı üzeredir. Foucault’da ise denetim ve gözetim faaliyetleri bireye dair ne varsa iktidarın bilmek istemesi, bireye hakim olmak ve onu terbiye etmek için bilgi toplaması üzeredir.⁹⁸

İktidar ontolojisinde ve denetim - gözetim faaliyetlerinde, teknolojik gelişmelerin yeri neresidir? Foucault’cu bakış açısında teknolojik gelişmeler özellikle günümüzde yani bilgi toplumu olarak ifade edilen süreçte, iktidarın elini güçlendiren, hatta onun varlığının yegane garantörü olan ve bireye ilişkin her türlü bilgiyi temin etmede kullanılan önemli araçlar olarak görülmektedir. Diğer taraftan bu teknolojik gelişmeler günümüzde bilgi toplamanın da ötesine giderek, kameralar gibi gözetim teknolojilerine dönüşmüş ve kendi varlıkları itibarıyla birer denetim aracı olmuşlardır.⁹⁹

Foucault’nun kuramında teknoloji sosyo - teknik bir anlam içerir ve bilgi gibi iktidarın aygıtıdır. Bu kapsamda tıp, kriminoloji, ordu bilimi vb. iktidarın teknolojileridir. 19. yüzyılda psikiyatri biliminin gelişimiyle akıl hastanelerinin ortaya çıkışı, hapishanelerin suçluların

⁹⁴ Kurthan Fişek, *a.g.k*, s.111.

⁹⁵ Max Weber, *a.g.k*, 2006, s.309.

⁹⁶ David Murakami Wood, *a.g.k*, s.6.

⁹⁷ Uğur Dolgun, *Şeffaf Hapishane Gözetim Toplumu*, Ötüken Yayınevi, İstanbul, 2008, s.99.

⁹⁸ Hakan Karakehya, “Gözetim ve Suçla Mücadele”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2009 C.58 S.2, s. 333 - 335.

⁹⁹ Aslıcan Kalfa, Hakan Topateş, *a.g.k*, s.440.

toplucu kapatılmaları yönünde evrilmesi teknolojinin ürünüdür. Foucault'ya göre hapishane örneğinde eskiden cellatların elinde olan denetim ve yetki, “hapishanenin karmaşık teknolojisiyle” yer değiştirmiştir.¹⁰⁰

Günümüzde özel sektörün ve devlet kuruluşlarının hepsinin bireye dönük olarak belli gözetim altyapıları ve kapasiteleri bulunmaktadır; fakat bireyler ve toplumsal gruplar kişisel bilgilerine ne olduğunu, kimler tarafından bunların kullanıldığını ve ne zaman - hangi amaç için bu bilgilerin araçsallaştırıldığını araştırmazlar ve araştırmanın da oldukça zor olduğunu düşünürler. Esasında çoğu zaman sıradan yurttaşların veya müşterilerin; yani gözetime maruz kalanların ya bunun için zamanları yoktur ya da bu detayları aramak için kendilerinde itici güç hissetmezler. Fakat yavaş yavaş bu kurumlarda biriken kişisel verileri onların yaşam imkanlarını şekillendirme ve tercihlerine rehber olma adına giderek artan oranda kendileri farkında olmadan veya rıza göstermemelerine rağmen kullanıldığı görülmektedir. Dolayısıyla günümüzde bireyin, iktidar odaklarının bilinçsel ve özselsel baskısı altında olduğu ifade edilebilir.¹⁰¹

Günümüzde iktidar odakları tarih boyunca hiç olmadığı kadar büyümüş, bukalemun gibi devamlı surette ortamın rengine göre değişebilen hal almış, sahip olduğu teknolojik çeşitlilik sınır tanımaz noktaya ulaşmıştır. Bu kapsamda iktidar, bireyin yapacağı tercihleri bireyden aldığı bilgilerle tahmin etmeye kadar bireyin bedenine inmiştir. Bundan daha vahimi birey için de iktidarın bu faaliyetleri, yani denetim - gözetim uygulamaları normalleşmiştir.

II. GÖZETİMİN DEĞİŞEN DOĞASI

Toplumu oluşturan, devletin varoluş sebebi olan “birey” günlük yaşamına hayatın olağan akışında devam ederken her şey yolunda gözükmektedir. Sokakta yürürken kameranin ekranından onu takip eden polis memurunun yürüyüşüyle alay edişini, eşkali dikkatini çektiği için kendisini takip eden istihbarat görevlisini, o esnada e-posta adresindeki mesajlaşmalarının kopyalanışını, cep telefonuna yeni yüklediği bir program tarafından koordinat bilgilerinin adım adım bir yerlere gönderilişini, kendisiyle ilgili veri ambarlarında toplanan bilgilerin hakkında “şüpheli şahıs” profili alarını verdiğini ve birilerinin kendisiyle ilgili rapor hazırladığını fark etmez. Ancak bir saatin arkaplanında çalışan çarklar gibi gözetim faaliyetleri durmaksızın, sistematik bir şekilde ve korkutucu boyutlarda hızla devam eder.

¹⁰⁰ David Rooney, “A Contextualising, Socio-Technical Definition of Technology: Learning from Ancient Greece and Foucault”, 1996, s.6., akt., Aslıcan Kalfı, Hakan Topateş, *a.g.k.*, s.441.

¹⁰¹ David Murakami Wood, *a.g.k.*, s.7 - 8.

Günümüzde bireyler, şirketler, kamu kurumları, uluslararası kuruluşlar, güvenlik birimleri, bankalar, alışveriş mağazaları gibi insanın etrafında ne kadar ilişkili olabileceği birim varsa hepsi insan hakkında bilgi toplamaya çalışmaktadır. Zira artık kişisel bilgi en az para kadar önem arz etmektedir. Günümüz kapitalist düzen çekişmesinde rekabet her türlü ilişkiyi etkilemiş ve bu çerçevede rekabet duygusu kaynaklı ortaya çıkan üstünlük kurma, hakim olma, iktidar olma arzusu bireye ait olan bilgiyi almayı ve bunu saklamayı zorunlu kılar olmuştur. Toplanan bu bilgiler bilgiyi toplayanın iştahını daha çok arttırmakta; neticede sonu gözükmeyen bir bilgi toplama furyası boy göstermektedir. Bu furyanın öncülüğünü de kamu kurumları gerçekleştirmektedir. Bireye ait olan bilgiyi toplamadaki bu istek hızla gelişen gözetim teknolojileriyle birleşince ürpertici boyutlara ulaşabilmektedir. İşte bu ürpertici durum günümüz gözetim dünyasındaki bireyin içinde bulunduğu durumun ta kendisidir.

Çalışmanın denetime bakan yönünün ortaya konulmaya çalışıldığı önceki ana başlık altında gözetimin, iktidarın kontrol mekanizması olan denetim faaliyetlerinin önemli bir parçası olduğu ifade edilmişti. Bu bölümde daha çok gözetim üzerinde durulacaktır. Öncelikle gözetim kavramının anlamı, çeşitleri ile günümüz gözetim dünyasının oluşum sürecini anlamada arkaplanını bilme açısından tarihsel süreçte ve toplumsal hayatta kendilerini gösteriş biçimleri ortaya konulmaya çalışılacaktır. Sonrasında küreselleşme ve bu paralelde ortaya çıkan bilgi ve iletişim teknolojilerinin gözetim faaliyetlerini uluslararası boyuta taşınması tartışılacak, Micheal Foucault'nun “Panoptikon” ve George Orwell’ın “Büyük Birader” metaforları dürbününde modern gözetim faaliyetleri sürecinin küresel gözetime evrilmesi incelenecektir. Ayrıca bu evrilme sürecinin neticede geldiği konumu anlama açısından ortaya çıkan yeni gözetleme sistemlerinden bahsedilecektir. Sürecin başka bir sonucu olarak ifade edilebilecek olan yurttaş - iktidar arasındaki gözetim ilişkilerinin aracı olarak e-devlet gözetime bakan yönüyle ortaya konulmaya çalışılacaktır.

1. Denetimin Temel Bileşeni Olarak Gözetimin Tarihsel Zemini

Gözetim toplumunu, günümüz gözetim teknolojilerini ve oluşturdıkları dönüşüm sürecini doğru kavrayabilmek için gözetim kavramının anlamsal çerçevesinin ortaya konulması gerekmektedir. Bu bölümde farklı bilim adamlarının görüşleri çerçevesinde gözetimin kelime anlamı, içerikleri ve çeşitleri incelenecektir.

Kökü Fransızcaya dayanan gözetim sözcüğü ilk olarak 1800’lü yılların başında kullanılmıştır.¹⁰² Gözetim, toplumsal yapının var olmasıyla hayat bulmasına karşın; kavramlaştırılması modernite, ulus devlet ve kapitalizm etkisiyle; gündelik hayatta yoğunlaşması ise bilgi ve iletişim teknolojileriyle olmuştur. Gözetim (*İng; surveillance*), Oxford sözlüğünde “şüpheli ya da suçlu şahısların izlenmesi”¹⁰³ şeklinde, Webster sözlüğünde “bir şey ya da kişinin ayrıntılı olarak takip edilmesi ve izlenmesi”¹⁰⁴ olarak, Türk Dil Kurumu sözlüğünde “gözetme, işe nezaret, himaye altına alma”¹⁰⁵ şeklinde ifade edilmektedir.

Gözetimin bilim adamları tarafından çeşitli tanımlamaları yapılmıştır. Foucault’a göre gözetim; bir veya daha çok kişinin iletişim ya da eyleminin sistematik olarak araştırılması, izlenmesi faaliyetidir.¹⁰⁶ Petersen’a göre ise birisini veya bir şeyi izlemek ve bunları kaydederek saklamaktır.¹⁰⁷ Ball ve Webster için gözetim; insanlar, süreçler ve kurumlar hakkında bilginin kategorizasyonu, gözlemi ve kayıt edilmesinden oluşur ve bilginin toplanması, depolanması, değerlendirilmesi ile aktarımını gerektiren bir süreci kapsar.¹⁰⁸

Gary T. Marx, gözetimle ilgili olarak verilen genel tanımların günümüzde kullanılan gözetim kavramını karşılamada yetersiz kaldığını düşünmektedir. Örneğin, Oxford sözlüğünde verilen gözetim tanımında özellikle vurgulanan şüpheli olma durumunun günümüz gözetim kavramıyla örtüşmediğini belirtmektedir. Ona göre bugünkü gözetim teknolojilerinin çoğu, sadece bir şüphelinin yakalanması yönelik değil toplumsal anlamda genel olarak uygulanmaktadır. Marx’a göre değişen gözetim kavramında göze çarpan diğer bir yenilik de gözetimin sadece önceden bilinen bir kişiye değil, aynı zamanda coğrafi alanlara, belirli zaman dilimlerine, şebekelere, sistemlere ve insan kategorilerine de uygulanabilir olmasıdır.¹⁰⁹

¹⁰² Gözetim kelimesinin kökeni Fransızca’dan gelmektedir. Kelimenin Fransızca’daki karşılığı “surveiller”dir. Bu kelime etimolojik olarak yukarıdan anlamına gelen “sur” ile izlemek anlamına gelen “veiller” kelimelerinin kaynaşması ile bir araya gelmiştir. İlk kullanım zamanı bilindiği kadarıyla 1802 yılıdır. Kelime Fransızca’dan İngilizce’ye “surveillance” olarak geçmiştir. Kaynak: <http://www.etymonline.com/index.php>, (Erişim Tarihi: 15.01.2013).

¹⁰³ http://oxforddictionaries.com/view/entry/m_en_gb0833040#m_en_gb0833040, (Erişim Tarihi: 15.03.2013).

¹⁰⁴ <http://www.merriam-webster.com/dictionary/surveillance>, (Erişim Tarihi: 15.03.2013).

¹⁰⁵ <http://www.tdk.gov.tr>, (Erişim Tarihi: 15.03.2013).

¹⁰⁶ Veysel Bozkurt, “Gözetim Toplumu ve İnternet”, s.3, <http://www.uludag.edu.tr>, (Erişim Tarihi: 15.01.2013).

¹⁰⁷ Julie K. Petersen, *Understanding Surveillance Technologies*, Taylor and Francis Group, New York, 2007, s.10.

¹⁰⁸ Kirstie Ball, Frank Webster, “The Intensification of Surveillance”, *The Intensification of Surveillance*, ed. Kirstie Ball, Frank Webster, Pluto Press, London, 2003, s.1.

¹⁰⁹ Gary T. Marx, “What’s New About the ‘New Surveillance’ Classifying for Change and Continuity”, s.10 - 11. <http://www.surveillance-and-society.org/journalv1i1.htm>, (Erişim Tarihi: 18.04.2012).

Gözetim kavramının içinde barındırdığı gizlilik, takibat, kişisel verilere ulaşılması gibi olumsuz anlamının yanı sıra olumlu bir anlam da içermektedir. Nitekim Martin'e göre gözetim, küçük çocukların zarar görmemeleri için büyükler tarafından yakından izlenmelerini veya hastaların sağlık durumlarının sağlık görevlilerince takip edilmesini kapsamaktadır. Ona göre insanlar, denizde yüzmek veya yüksek bir yere tırmanmak gibi riskli faaliyetlerde bulunduklarında, başkasının kendilerini takip etmesinden memnun olurlar. Bu noktada bunlar gözetimin iyi ve olumlu anlamının örnekleri olarak gösterilebilir.¹¹⁰ Lyon bu durumu "gözetimin iki yüzü" olarak açıklamaktadır. Gözetimin ikiyüzlü olması gözetimin hem kontrol, hem koruma içermesi anlamına gelmektedir.¹¹¹ Gözetimin iki yüzü ileriki başlıklarda ele alınacaktır.

Gözetimin ana unsuru "takip etme" faaliyetidir. Takip etme faaliyetinin konusunu kişinin davranışları, hareketleri, konuşmaları, ilişkileri oluşturmaktadır. Takip etme faaliyetinin temel amacı gözetleyene gözetlenen hakkında veri akışının sağlanmasıdır. Bunun yanında eğer takip edilenin gözetlendiğinin farkına varması istenirse hareketlerine dikkat etmesi yönünde bir uyarı sağlama amacı da ortaya çıkmaktadır. İşte burada toplu gözetim ve bireysel gözetim ayrımı belirmektedir. Eğer toplu gözetim yapılıyorsa gözetleyenin istemediği davranışları kitlelerin yapmamasını sağlama amacı, bireylere ait verilerin toplanması amacının önüne geçer.¹¹² Lyon bu durumu "bireylerden özellikle soyutlanmış hakikat parçacıklarını arayıp bulma faaliyeti" olarak ifade etmektedir.¹¹³ Bireysel gözetim daha çok Fransız orijinli iken toplu gözetim İngiltere ile özdeşleşmiştir.¹¹⁴

Gözetimin birbiriyle sürekli ilişki içerisinde olan iki görünümü vardır. Birincisi veri toplamaya dayalı gözetimdir. Burada gözetleyen otorite tarafından saklanabilecek kodlanmış bilgi birikimi söz konusudur. Bireyler hakkında toplanan, depolanan, şifrelenen bilgi birikimi bireylerin eylemlerini yönetme amacıyla kullanılır. İkincisi ise denetleyen gözetimdir. Herhangi bir topluluk içerisindeki bazı bireylerin eylemlerinin, bunlar üzerinde otorite kuran diğer bazı bireyler tarafından doğrudan izlenmesini içerir. Bu durum topluluk içindeki

¹¹⁰ Brian Martin, *Information Liberation Challenging the Corruptions of Information Power*, Freedom Press, London, 1998, s.64.

¹¹¹ David Lyon, *Gözetlenen Toplum*, Çev. Gözde Soykan, Kalkedon Yayınevi, İstanbul, 2006, s.17.

¹¹² Roger Clarke, "Have We Learnt To Love Big Brother", s.9.

<http://www.anu.edu.au/people/Roger.Clarke/DV/DV2005.html>, (Erişim Tarihi: 18.04.2013).

¹¹³ David Lyon, *a.g.k*, 2006, s.13.

¹¹⁴ Roger Clarke, *a.g.k*, s.9.

izlenenleri izleyenlerden daha alt bir konuma yerleştirir ve böylece izlenen bireylerin etkinlikleri rahatça koordine edilebilir.¹¹⁵

Yapılan bir etkinliğin gözetim faaliyeti olduğunu iddia etmek için bu etkinliğin gözetimin genel özelliklerini üzerinde taşıması gerekir. Gözetimin en temel özelliği, gözetleme faaliyetinin belirli bir amaca yönelik olmasıdır. Bu amaç; güvenliği sağlama, suçluları yakalama, kontrolü sağlama olabileceği gibi mevcut iktidarın diktelerinin toplum tarafından yerine getirilmesini temin etme de olabilir. İkinci olarak gözetim rutindir; yani gözetleme faaliyetleri günlük yaşantının doğal bir parçası şeklindedir.¹¹⁶

Üçüncü olarak gözetim sistematiktir. Yani gözetim, planlanmış bir şekilde belli bir mantıksal silsile dahilinde, belli bir programa göre yürütülmektedir ve rasgele değildir.¹¹⁷ Yalnız buradaki “rasgele değil” ifadesini kişiler eksenli değerlendirmemek gerekir. Zira toplu gözetim faaliyetlerinde gözetim işlemi kişi ekseninde rasgele yapılmaktadır. Ancak belli bir yerde, belli tanımlamalara göre ve belli periyotlarda yapılmaktadır. Günümüz gözetim teknolojileriyle (yüz tanıma sistemleri gibi) birlikte gözetleme faaliyetleri tanımlanmış kişiler eksenli olarak da çalışabilmektedir.

Gözetim faaliyetleri genel olarak beş kategoride değerlendirilebilir.¹¹⁸ Birinci kategoride “sahte gözetim” yer alır. Bu tür gözetimde, gözetim faaliyetleri birçok araç ve unsur tarafından yapılmış imajı verilir. Örneğin; çalışmayan kamera sistem ve mekanizmaları, boş kamera yuvaları, ilgili bölgenin izlendiğine dair duvar ilanları gibi araçlar kullanılarak gerçekte olmasa da bireylerin algısında gözetlenme düşüncesi oluşturulur. Bu tür gözetim istenmeyen davranış modellerinin oluşmasını engellemeye yönelik caydırıcılık fonksiyonu sergiler.

İkinci kategoriyi “açık gözetim” oluşturur. Açık gözetimde gözetlenenler nasıl, hangi araçlarla gözetlendiklerini bilirler ve bulundukları yerlere yerleştirilmiş olan monitörlerde de kendilerini görebilirler. Bu gözetim türü genelde alışveriş merkezlerinde ve dükkanlarda yapılmaktadır. İnsanların açık gözetim yapılan yerlerde gizli gözetim yapılan yerlere göre kendilerini daha rahat ve güvende hissettikleri iddia edilmektedir. Üçüncü kategoride “gizli gözetim” yer alır. Buna göre gizli gözetimde gözetlenen kişinin kendisinin gözetlendiğini ve gözetim araçlarının nerede olduğunu bilmemesi istenir. Bu gözetim araçlarına gizli kameralar, gizli dinleme cihazları vb. örnek gösterilebilir. Gizli gözetleme

¹¹⁵ Anthony Giddens, *Ulus, Devlet ve Şiddet*, Çev. Cumhur Atay, Devin Yayınları, İstanbul, 2005, s.24 - 25.

¹¹⁶ David Murakami Wood, *a.g.k*, 2006, s.8.

¹¹⁷ *a.k*

¹¹⁸ Julie K. Petersen, *a.g.k*, s.13 - 14.

faaliyetleri yasal değildir ve hakim kararı gerektirmektedir. Bu tür gizli gözetleme faaliyetleri istihbarat, bilgi toplama gibi amaçlar için kullanılır.

Dördüncü gözetim türü özellikle sokaklarda yaygın olan “geniş gözetim”dir. Geniş gözetim “klandestin gözetim” olarak da ifade edilmektedir. Bu gözetim türü gözetleme sisteminin varlığının gözetlenenler tarafından görülebildiği; fakat gözetleme aracının yönünün bilinemediği ve kimi gözetlediğinin anlaşılamadığı sistemleri içermektedir. *Dome* kameralar bu tür gözetleme sistemlerine güzel bir örnektir. Bu kameralar 360 dereceye kadar çevreyi gözetleyebilir, ancak gözetlenecek yöne kumanda merkezindeki görevli kişi karar verir.

Son kategoride “rıza bağlı gözetim” bulunmaktadır. Bu tür gözetlemede gözetlenen kişinin rızası dikkate alınır. Ciddi sağlık problemi olan ve anında müdahale gerektiren hastaların odalarında veya nükleer santral görevlilerinin çalışma ortamlarında yapılan gözetim gibi yaptığı işin hassasiyeti gereği anında müdahale gerektiren durumlardaki gözetim buna örnek gösterilebilir.

Gözetimin şekline göre gözetleme faaliyetleri ise üçe ayrılabilir.¹¹⁹ Birincisi daha çok belirli bir mekan veya çevredeki sesleri takip etmeye yönelik olan “akustik gözetimdir”. Petersan akustik gözetimi de işitsel teknolojiler, infrasonik ve ultrasonik teknolojiler, sonar teknolojiler olmak üzere üç gruba ayırmaktadır. İşitsel teknolojiler, insan sesi düzeyindeki sesleri dinlemeye yönelik sistemlerdir. İnfrasonik ve ultrasonik teknolojiler, insan kulağının duyamayacağı frekanstaki sesleri dinlemeye yönelik sistemlerdir. Sonar teknolojiler ise insan kulağının duyabileceği ve duyamayacağı düzeydeki sesleri dinlemeye yönelik olan ve genelde deniz altında yapılan dinlemelerde kullanılan sistemleri ifade etmektedir.

İkincisi radyo, görsel, ultraviyole, x-ray teknolojilerini içeren “elektromanyetik gözetim”dir. Buna radar, kamera, lazer gibi araçlarla yapılan dinleme, izleme faaliyetleri örnek gösterilebilir. Üçüncüsü bilimsel laboratuvarlarda gerçekleştirilebilen ve ileri teknoloji gerektiren gözetleme sistemlerini ifade eden “biyokimyasal gözetim”dir. Parmak izi, iris taraması, genetik takip bu tür gözetime örnek gösterilebilir.

Yukarıdaki tanımlamalar ve kategorizasyonlar ışığında genel olarak gözetimin; güvenlik, iş verimliliği, yönetim gibi kaygılarla çeşitli alanlarda sürekli genişleyen bir kapsam ve içerik ile kişisel verilerin elde edilmesi, depolanması, analiz edilmesi süreçlerini ifade ettiği söylenebilir.

¹¹⁹ a.k, s.15.

Tarihsel süreç içerisinde her dönemde gözetim, insan hayatında önemli bir yer tutmuş; toplumsal denetimi ve egemenlik ilişkilerini kurmanın, sürdürmenin başlıca araçlarından biri olagelmıştır. Tarihsel olarak gözetleme faaliyetleri İlkel Gözetim Dönemi, Modern (Teknik) Gözetim Dönemi, Enformatik Gözetim Dönemi olmak üzere üç ana dönemde sınıflandırılabilir.¹²⁰ İnsanlar tarih boyunca birbirlerini, toplumsal örgütlenme ve koruma amacıyla gözetlemişlerdir. Antik dönemde yönetimde bulunanlar vergi, askerlik hizmeti ve göç gibi amaçlarla halkın nüfus bilgilerini kayıt altına almıştır. İsrail'in göçebe halkında bile, M.Ö 15. yüzyılda topluluğa ilişkin ayrıntıları kaydetmek üzere birden fazla nüfus sayımı yapıldığı görülmektedir. Ancak bu dönemde gözetim faaliyetleri, sadece askerlik hizmetini düzene koymak, vergileri düzgün olarak toplamak amaçları ekseninde süregelmiştir.¹²¹

Gözetim faaliyetleri resmi olarak yazının buluşu zamanına kadar götürülebilir. Yazının buluşuyla birlikte yazı, göçebe yaşamı kontrol etmek, vergi toplamak, nüfusu kayıt altına almak, devletin kayıtları için gerekli bilgileri temin etmek gayeleriyle bir gözetim aracı olarak kullanılmıştır.¹²² Giddens'a göre yazı elektronik olmayan bir bellek aygıtıdır. Yani yazı kullanılarak hem devletin kayıtları için gerekli bilgiler hem de bireylerin özel alanlarına ilişkin her türlü malumat toplanıp depolanabilmekte ve farklı faaliyetler için kullanılabilir hale getirilebilmektedir. Bu noktada yazıyla gelen kayıtlama sistemi, devletin bireyler üzerinde bir idari denetim aracı olmasında ve gözetim faaliyetlerinin gelişmesinde başat rol oynamıştır.¹²³

Metinlerin tanımlanmasıyla birlikte yazı artık anlamlı bir içeriğe sahip olmuştur. Bunun sonucunda da sözlü gelenekteki geleneksel davranış biçimleri artık devlet tarafından ele alınıp idare edilir hale gelmiştir. Böylece yazı, nüfusun potansiyel olarak itaatsiz kesimlerinin faaliyetlerini tanımlamak ve izlemek üzere doğrudan kullanılabilmiştir. Yazıyla birlikte ayrıntılı resmi istatistiklerin tutulması, bireylerin yaka kayıtlarına ve gündelik yaşamlarına ilişkin oldukça ayrıntılı başka belgelendirme biçimleri devletlerin ve örgütlenmelerin kendine has özelliklerinden olmuştur.¹²⁴

Gözetimde edebi metinlerin gelişmesinden sonraki aşama ise matbaanın keşfi aşamasıdır. Giddens'e göre matbaa ile devlet otoritesinin mutlakiyeti pekişmiştir. Böylelikle

¹²⁰ Uğur Dolgun, *a.g.k*, 2008, s.16 - 17.

¹²¹ Gary T. Marx, "Surveillance and Society", *Encyclopedia of Social Theory*, 2005, s.1. <http://web.mit.edu/gtmarx/www/surandsoc.html>, (Erişim Tarihi 15.01.2013).

¹²² Anthony Giddens, *a.g.k*, 2005, s.66.

¹²³ David Lyon, *Elektronik Göz: Gözetim Toplumunun Yükselişi*, Çev. Dilek Hattatoğlu, Sarmal Yayınları, İstanbul, 1997, s.39 - 40.

¹²⁴ *a.k*, s.66 - 67.

de devletin gözetim faaliyetleri kabul görmüş ve ilerleyebilmiştir.¹²⁵ Matbaanın bulunuşundan sonra devlet, gözetimi özellikle kurumlar üzerinde baskı unsuru oluşturacak şekilde kullanmaya başlamıştır.¹²⁶ 15. yüzyıla gelindiğinde dini gözetim güçlü ve baskın bir gözetim şekli olmuştur. Bu gözetimin şeytan ve cadıların aranması, zina gibi günahların takibi benzeri nedenlerle yapılan gözetimi ifade ettiği söylenebilir. Bu dönemde gözetimin kaynağı dini kurumlar olmuştur. Bu kurumlar çeşitli dini temellendirmelerle kişilere ait doğum, evlilik, vaftiz ve ölüm kayıtlarını toplamış ve depolamıştır.¹²⁷

16. yüzyıla gelindiğinde, hem yeni ihtiyaçları olan hem de gelişen bilgi toplama ve kullanma kapasitesine sahip ulus devletlerin ortaya çıkmasıyla beraber siyasi gözetim dini gözetime göre daha çok önem kazanmıştır.¹²⁸ Siyasi gözetimin temel unsurları; devlet idaresi, askeri oluşumlar, bürokratik düzen, devletin her türlü tehlikeye karşı koruma güdüsü, sanayileşme ile oluşan yeni kent düzeni ve kapitalist işletme sayısındaki artışlar olarak ifade edilebilir. Bu gözetimin temel özelliğini kamusal alanda bürokrasi, üretim alanında da bilimsel yönetim ilkeleri oluşturmuştur. Bu dönemde gözetim, kapitalist üretim sürecinin ve bürokratik örgütlerin varlığının teminatı olan bir güç modülü ve sosyal normlara aykırı olanları disipline edici bir araç olmuştur.¹²⁹

19. ve 20. yüzyıllarda fabrika sisteminin, ulusal ve uluslararası ekonomilerin, bürokrasinin ve refah devletinin yükselişi ile birlikte gözetimin kapsamı da ticareti ve üretimi arttırmak, kamu sağlığını korumak, her geçen gün artan kurallara uyumu sağlamak, çocukların korunması ve çeşitli sosyal güvenlik programlarına katılımın denetlenmesi gibi alanlara doğru genişlemiştir. Bu genişlemenin bir sonucu olarak özel sektör de özellikle sigorta, banka, sağlık işlemleri ve ticari pazar uygulamaları üzerinden çalışma yaşamında gözetimi giderek artan oranda kullanmaya başlamıştır.¹³⁰

Modernleşmeyle birlikte insanlar arasında olan yüz yüze olan ilişki giderek azalmaya başlamıştır. Yüz yüze ilişkilerin azaldığı modern şehir toplumu ile ilişkilerin yüz yüze olduğu

¹²⁵ a.k, s.235.

¹²⁶ Gary T. Marx, a.g.k, 2005, s.1.

¹²⁷ a.k

¹²⁸ a.k

¹²⁹ Foucault gözetimin bireyler üzerinde yoğunlaşmasını şu şekilde anlatmaktadır: “İktidar düzenine göre gözetlemenin cezalandırmadan daha etkili ve daha verimli olduğunun fark edildiği an. Bu an, on sekizinci yüzyılda ve on dokuzuncu yüzyıl başında yeni tür iktidar işleyişinin hem hızlı hem de yavaş oluşumuna denk düşer. Siyasi rejim değiştiğinde görülen kurumsal düzenlemeleri, iktidarın bizzat devlet sisteminin başına devredilişinin değişimine tarzını, büyük altüst oluşları hepimiz biliriz. Ama ben iktidar mekanizmasını düşündüğümde, iktidarın bireylerin tohumuna kadar ulaştığı, bedenlerine eriştiği, hal ve tavırlarına, söylemlerine, öğrenimlerine, gündelik yaşamlarına sindiği kılcal var olma biçimini düşünüyorum.”

Michel Foucault, a.g.k, 2003, s.23.

¹³⁰ <http://web.mit.edu/gtmarx/www/surandsoc.html>, (Erişim Tarihi 08.01.2013).

küçük kırsal yerleşim toplumu olmak üzere bir dualist yapı oluşmuştur. Bu yapı içerisinde insanların birbirlerini tanımadıkları, dolayısıyla birbirine karşı güvensizliğin ve korkunun giderek artış gösterdiği modern şehir toplumunda gözetleme faaliyetleri daha gelişmiş gözetim teknik ve teknolojileriyle yapılmaya başlanmıştır.¹³¹

20. yüzyıl ile birlikte “geleneksel gözetim” yerini “yeni gözetime” bırakmıştır. Gary T. Marx’ın ifadesiyle yeni gözetim, teknolojik araçlar kullanılarak bireylere veya gruplara ait verileri çıkarmak ve toplamak olarak tanımlanabilir. Yeni gözetim araçlarına kameralar, bilgisayar eşleştirmeleri, veri tarama sistemleri, elektronik yer tespit sistemleri, DNA analizleri, uyuşturucu testleri, yalan tespiti için kullanılan beyin tarama sistemleri, termal kamera sistemleri vb. örnek gösterilebilir.¹³²

Yeni gözetim araçlarıyla gözetim dünyasının farklı bir boyut alışı 1949 yılında George Orwell tarafından yazılan *Bin Dokuz Yüz Seksen Dört* isimli kitapta anlatılmış ve daha sonraki gözetim faaliyetleri adına yaygın olarak kullanılacak “Büyük Birader Bizi İzliyor” metaforu ortaya çıkmıştır. Bu kitap o dönem insanların zihinlerinde oluşan gözetim distopyasını da açıkça ortaya çıkarmıştır.¹³³

Görüldüğü üzere gözetim, insanlık tarihi kadar eski bir kavramdır. Gözetimin bu erginliğinin yanı sıra günümüz toplumlarında önemi ve etkisi giderek artış göstermiştir. Zira küreselleşme, postmodernizm veya bilgi toplumu gibi kavramlar günümüzün temel toplumsal değişimlerine ışık tutmak için ortaya konurken; gözetim kavramı, bu değişimlerin ortaya çıkardığı önemli bir sonucu ifade etmektedir.¹³⁴

2. Modern Gözetimin Değişen Yüzü: Panoptikondan Büyük Biradere

Gözetim olgusu, iktidarların en önemli araçlarından birisi ve önemli bir denetim türü olarak insanlık tarihi boyunca var olagelmıştır. Modern devletlerin ortaya çıkmasıyla birlikte, gözetim pratikleri şekil değiştirmiş, gündelik hayat gelişen teknolojik cihazlarla daha kolay gözetlenir olmuştur. Gözetimin toplumsal yaşamda gerçek manada hissedilmeye başlanması teknolojinin gelişmesi ile paralellik arz etmektedir. Sanayi devrimi sonrasında bireylerin ve kurumların daha etkin bir şekilde gözetlenmesi gerektiği algısıyla günümüz bilgi ve iletişim teknolojileri alanındaki büyük gelişmeler birleşince gözetimin kapasitesi ve alanı genişlemiştir. Küreselleşme ile birlikte gözetim uluslararası bir nitelik kazanmıştır.

¹³¹ a.k

¹³² a.k

¹³³ a.k

¹³⁴ David Lyon, a.g.k, 2006, s.17.

Gözetim ve gözetim teknolojilerinin hızla gelişmesi ve bunlara verilen önemin artmasının altında yatan temel neden bilginin eski dönemlere göre daha çok önem kazanmasıdır. Zira bilginin ekonomik, sosyal, siyasal değeri artmıştır. Bu durum da bilgiye kolay ulaşım yollarından birisi olarak değerlendirilebilecek gözetim faaliyetlerini iktidar odaklarının ilgi merkezine oturtmuştur.¹³⁵ Bu yüzden günümüz toplumları gözetim toplumları olarak adlandırılarak artan gözetim faaliyetlerine dikkat çekilmeye çalışılmıştır.

Modern gözetim, kapitalizmin gelişmesiyle eş zamanlı olarak ortaya çıkmıştır. Kapitalizmin gelişim göstermesiyle birlikte üretim araçlarını elinde bulunduran yöneticiler, maksimum karla mal üretebilmek için gözetim araçlarını kullanarak işçileri fabrikalarda disiplin altında tutmaya başlamışlardır. Fabrika sisteminin işçileri kontrol altında tutmaya daha elverişli olması, işçilerin üretim araçlarının mülkiyetinden ayrı tutulmalarına neden olmuş ve sermayenin emek üzerindeki kontrolünü arttırmıştır. Kapitalizmin gelişmesiyle birlikte fabrikalarda başlayan gözetim zamanla gündelik hayata da etki etmiştir.¹³⁶

Geleneksel toplumlardan modern - kapitalist toplumlara geçişle birlikte zamanın döngüsellği de değişmiştir. Lyon'a göre, modern saatlerin icadıyla artık tarımsal günlük alışkanlıkların yaşandığı durumlar; mevsim, günışığı gibi zamanlamalarla sınırlı değildir. Modern çalışma ve yaşama saatleri zaman çizelgesine tabi olduğu için doğal etkenlerin yönettiği faaliyetlerin yerini artık saate bağlı ritimsel faaliyetler almıştır. Saatin modern yaşam içine girmesi, insan faaliyetlerinin zaman - mekan içinde örgütlenerek denetlenmesini beraberinde getirmiştir. Lyon'a göre modern gözetimin değişen doğasında artık gündelik hayat sadece saate tabi tutularak gözetlenmemekte, günümüzde gelişen bilgisayarlar saatlerin yerini alarak gözetim faaliyetini icra etmektedir.¹³⁷ Lyon bu durumu şöyle ifade eder:¹³⁸

“Saat, özellikle kapitalist fabrikada nasıl modern gözetim mekanizmasının hayati bir parçası haline geldiyse, günümüzde de bilgisayar, üretim alanının ötesindeki faaliyetler de dahil olmak üzere, zaman-mekan içindeki faaliyetleri koordine eder.”

Bu yüzden günümüz toplumlarında gözetim, zaman ve mekan kavramlarından bağımsız hareket edebilir hale gelmiştir. Modern gözetim başlarda Foucault'nun “Panoptikon” metaforu, sonrasında George Orwell'in *Bin Dokuz Yüz Seksen Dört* kitabındaki

¹³⁵ John Kenneth Galbraith bilginin önemini şöyle ifade etmektedir: “Endüstri toplumunda hız kazandıran şey paradır; fakat bilgi toplumunu hızlandıran ve güce ulaştırın bilgidir, şimdi bilgi sahibi olanlar ve olmayanlar şeklinde yeni bir sınıfsal bölünme ortaya çıktı. Bu yeni sınıf, gücünü paradan ya da sahip olunan topraklardan değil, sadece bilgiden alıyor.”

Murat Ertan, *Tarihi Sözler Antolojisi*, Afşar Matbaacılık, Ankara, 2010, s.73.

¹³⁶ Meral Tümtürk, “Gündelik Hayatın Gözetimi: Panoptikon Toplumu”, *Ethos: Felsefe ve Toplumsal Bilimlerde Diyaloglar*, Sayı 3 (2), Temmuz 2010, s.6.

<http://www.ethosfelsefe.com/ethosdiyaloglar/mydocs/Ethos-7%20Gozetim.pdf>, (Erişim Tarihi: 28.07.2013).

¹³⁷ David Lyon, *a.g.k*, 1997, s.55.

¹³⁸ *a.k*

“Büyük Birader” öngörüsü ile şekillenirken ve kendini belli ederken, günümüzde artık bunlardan da ileri seviyeye ulaşmış, bilgi ve iletişim teknolojileriyle devasa, fark edilmez, daha kapsamlı ve toplumun her kesimini kuşatan bir hal almıştır.¹³⁹

Günümüzde günlük yaşantı içerisinde gerçekleştirilen bütün faaliyetlerin izi sürülebilir olmuş, bu faaliyetler neticesinde ortaya çıkan kişisel veriler kolaylıkla toplanıp, depolanabilir hale gelmiştir. Örneğin normal günlük rutin içerisinde herhangi bir mağazadan yapılan alış -veriş neticesinde kullanılan kredi kartı veya kapalı devre kamera sistemleri sayesinde bireylerin isimleri, satın aldıkları şeyler, harcama miktarları hatta davranış biçimleri veri tabanlarına kaydedilmekte ve depolanmaktadır.¹⁴⁰ Benzer şekilde otoyolda alınan elektronik geçiş biletinden, cep telefonu ile olan görüşmelere kadar her şey kaydedilmektedir. Bu bakımdan bedenlerin gittikçe birer sanal profile dönüştüğü söylenebilir.

Modern gözetleme diğer taraftan da ulusal sınırların dışına nüfuz ederek *Echelon*, uydu takip sistemleri, internet takip sistemleriyle uluslararası gözetleme faaliyetleri haline dönüşmüştür. Foucault’nun panoptikon metaforunun sınırları dünyayı kapsar hale gelmiştir. Bütün bunlardan da önemlisi dünya yurttaşları nezdinde gözetim olağan bir şekle dönüşmüş, varlığı kabullenilmiştir. Bundan dolayı dünyanın yirmi dört saat gözetlenen açık hapishaneye dönüştüğü ifade edilebilir. Bu hapishanenin gözetleme kulesine oturmak için günümüzde gizli iktidar savaşları olduğu bilinmektedir. Nitekim buna 26 Temmuz 2010 tarihinden itibaren ABD’nin diğer ülkeler üzerinde yaptığı gözetleme faaliyetlerini açıklayan *Wikileaks*¹⁴¹ belgeleri örnek verilebilir.

Modern gözetimin bilgi ve iletişim teknolojileriyle entegre olması onu artık devamlı surette gelişmeye ve dönüşmeye mahkum hale getirmiştir. Zira bilgi ve iletişim teknolojileri doğası gereği sürekli gelişim içerisinde, bu durumda gözetleme teknikleri de değişecek, buna bağlı olarak da gözetim felsefesi devamlı olarak genişleyecektir. Nitekim modern gözetimin başlarında gözetim felsefesi işçileri ve mahkumları kontrol altında tutmak iken, giderek güvenlik adı altında tüm toplumu kontrol altında tutmaya doğru evrilmiştir.

¹³⁹ Felix Stalder, “Opinion. Privacy Is Not The Antidote to Surveillance”, *Surveillance and Society*, Vol. 1, Issue 1, 2002, s.125. <http://www.surveillanceand-society.org/articles1/opinion.pdf>, (Erişim Tarihi: 21.02.2013).

¹⁴⁰ a.k

¹⁴¹ Eski bir bilgisayar korsanı olan Avustralyalı gazeteci Julian Assange’ın liderliğinde WikiLeaks, kaynaklarının gizliliğini koruyarak hükümetlerin ve diğer organizasyonların hassas belgelerini yayınlayan, İsveç merkezli bir uluslararası organizasyondur. Kuruluşundan bir yıl sonra, organizasyonun ve *wikileaks.org*’un veritabanında 1.2 milyondan fazla doküman bulunmaktadır.

<http://www.trt.net.tr/haber/HaberDetay.aspx?HaberKodu=a6222353-8588-485a-af47-ec075d7b27de>, (Erişim Tarihi: 20.04.2013).

Modern gözetimle ilgili olarak yapılan incelemelerde bilimsel düzeyde iki temel çalışma ve görüş ortaya çıkmaktadır. Bunlardan birincisi Jeremy Bentham'ın "Panoptikon Hapishane Mimari Modeli" eksenli Foucault'nun "Panoptikon" metaforu; ikincisi ise George Orwell'in *Bin Dokuz Yüz Seksen Dört* adlı eseri ve "Büyük Birader" distopyasıdır. Jeremy Bentham'ın *Le Panoptique* adlı eseri on sekizinci yüzyıl sonunda yazılmış olan günümüz gözetim toplumuna da ışık tutan önemli bir yapıttır.¹⁴² Esasında "Panoptikon" ya da "Gözlem Evi", Jeremy Bentham'ın 1787 yılında Beyaz Rusya'dan İngiltere'deki bir arkadaşına yazdığı mektuplarda tasvir ettiği bir hapishane modelini anlatmaktadır.¹⁴³ Panoptikon, Yunancada "göz önündeki yer" anlamına gelen ve Bentham tarafından türetilen bir kavramdır.¹⁴⁴ Jeremy Bentham panoptikonu şu şekilde anlatmaktadır:¹⁴⁵

"Çevrede halka şeklinde bir bina; ortada bir kule, kulede açılmış olan geniş pencereler halkanın iç cephesine bakmaktadır. Çevre bina hücrelere ayrılmıştır, hücrelerin her biri bina boyunca derinlemesine uzanır. Bu hücrelerin iki penceresi vardır: Biri içeriye doğru açıktır, kulenin pencerelerine denk düşer; diğeri dışarıya bakarak, ışığın bir baştan bir başa hücreyi kat etmesini sağlar. Bu durumda merkezi kuleye bir gözlemci yerleştirmek ve her bir hücreye bir deli, bir hasta, bir mahkum, bir işçi ya da bir öğrenci kapatmak yeterlidir. Önden ışıklandırma sayesinde, karanlıkta kalan kuleden çevre hücrelerdeki esirlerin küçük silüetleri görülebilir. Kısacası, zindan kuralı tersine çevrilir; hücrenin apaydınlık hali ve bir gözünün bakışı, karanlıktan daha iyi yakalar ki karanlık eninde sonunda koruyucudur. Bu modele göre, daire şeklindeki bir binanın tam ortasına uzunca bir gözetleme kulesi yerleştirilmiştir. Kule, etrafını çevreleyen binadaki hücreleri görece şekilde dizayn edilmiştir. Her birine bir kişinin yerleştirildiği hücreler ise önden ve arkadan iki pencere ile aydınlatılmaktadır. Özellikle hücrenin arka tarafındaki pencereden gelen ışık, odadaki kişinin kuleden kolaylıkla görülebilmeyi sağlamaktadır. Hücredekiler, dışarıdan görülebilen ancak kendilerini izleyenleri göremeyen nesneler konumundadırlar. Kuledeki gözetimciler (ya da gardiyanlar) ise görebilen, ancak görülmeyen özne konumundadırlar."

Panoptikonda yer alan hücrelerin her biri Foucault'ya göre birer kafestir ve ne kadar kafes varsa aslında o kadar tiyatro sahnesi ve oynanan oyun bulunmaktadır. Yalnız bu oyunda herkes tek başınadır ve bireysel oyunlarını oynarlar ve sürekli olarak görünür durumdadırlar. Ona göre bu yapı, görülmeden görmeye olanak veren bir düzenlemeyi ifade etmektedir.¹⁴⁶

Bentham'ın panoptikon modeli esasında Bentham bunu dile getirmeden önce 1751 yılında Paris Askeri Okulu'nda, yatakhaneler konusunda uygulamaya konulmuştur. Bu okulda her bir öğrencinin camekanlı bir hücresi vardır ve öğrenciler diğer öğrencilerle, hatta hizmetlilerle bile hiçbir ilişkiye girmeden bütün gece gözetlenmektedirler. Nitekim Bentham da panoptikon fikrini, askeri okulu ziyaret eden kardeşinin kendisine verdiğini ifade etmiştir.

¹⁴² Michel Foucault, *a.g.k.*, 2003, s.95.

¹⁴³ Bentham'ın eserinin tam adı oldukça uzundur: Panopticon; or The Inspection-House: Containing The Idea of A New Principle of Construction Applicable to Any Sort of Establishment, In Which Persons Of Any Description Are To Be Kept Under Inspection; And In Particular To Penitentiary-Houses, Prisons, Houses Of Industry, Work-Houses, Poor-Houses, Lazarettos, Manufactories, Hospitals, Mad-Houses, And Schools: With A Plan Of Management Adapted To The Principle: In A Series Of Letters.

¹⁴⁴ David Lyon, *a.g.k.*, 1997, s.93.

¹⁴⁵ Jeremy Bentham, *The Panopticon Writings*, Verso, Londra, 1995, s.43.

¹⁴⁶ Michel Foucault, *a.g.k.*, 2006, s.295.

Bununla birlikte, panoptikon fikri Bentham'dan önce gelse de, bunu teknik ve bilimsel olarak ifade etmiş ve adını koymuş olan Bentham'ın kendisidir.¹⁴⁷

Panoptikon sözcüğü “bütünlük ilkesini” ifade etmektedir. Bu bakımdan Foucault'a göre Bentham yalnızca hapisane, okul ya da hastane gibi belirli bir sorunu çözmeye yönelik mimari bir figür hayal etmekle kalmamış gerçek bir keşifte bulunmuştur. Foucault bunu ifade etmek için “Colombus yumurtası”¹⁴⁸ tabirini kullanmıştır. Ayrıca bu keşfi gözetim sorunlarını çözmeye uygun bir iktidar teknolojisi olarak ifade etmiştir.¹⁴⁹

Panoptikon ile Bentham, hem mahkumları az sayıda personelle ve az maliyetle gözetleyerek onlar hakkında bilgi toplamayı hem de onları ıslah etmeyi amaçlamıştır. Bu nedenle az maliyetle işletilebilecek bu çok amaçlı projenin iktidarların büyük ilgisini çekeceğini düşünen Bentham, bundan iyi bir kazanç elde etmeyi ummuş; fakat hayatı boyunca bu projeyi gerçekleştirememiştir.¹⁵⁰ Buna karşın Bentham'dan sonra özellikle 19. yüzyılın ilk yarısında inşa edilen hemen tüm hapishaneler bir şekilde Bentham'ın bu projesine atfen, onun bazı uygulamalarını örnek almak suretiyle yapılmıştır.¹⁵¹ Panoptikonun bilinirliği ve gözetime ilişkin hemen her yazında kullanılması, Foucault'nun onunla ilgilenmesi ve 1975 yılında yayımladığı “Hapishanenin Doğuşu” adlı kitabında ona geniş yer vermesiyle olmuştur.¹⁵²

Görülmeden gözetlemeye olanak veren panoptikon düzenlemesi, sürekli görmeye ve hemen tanımaya olanak veren mekansal birimler oluşturmaktadır.¹⁵³ Gözetim, mahkumların görünmeyen gözler tarafından gözetlenmesi esasına dayanmaktadır. Mahkum için saklanacak ve özel alan olarak ifade edilebilecek hiçbir yer yoktur. İzlenip izlenmediğini, kulenin içerisini göremediği için bilemeyen ama orada izlemek için birilerinin var olduğunu varsaymak durumunda olan mahkum açısından tek makul seçenek itaat etmektir. Bu hapisane modelinde kolay gözetleme olanağı ve mahkum üzerinde oluşturduğu “sürekli gözetleniyorum” hissi nedeniyle, çok az gardiyanla işler yürütülebilmektedir.¹⁵⁴

Panoptikon her ne kadar bir hapisane şeklinde dizayn edilse de ondaki temel felsefe, akıl hastanelerinden askeri kışlalara, okullardan fabrikalara gözetilmek istenen her yerde

¹⁴⁷ Michel Foucault, *a.g.k.*, 2003, s.87 - 88.

¹⁴⁸ Colombus Yumurtası (İng; *Columbus' egg*); harika bir fikir veya keşfi ifade etmek için kullanılan bir deyimdir. http://en.wikipedia.org/wiki/Egg_of_Columbus, (Erişim Tarihi: 04.06.2013).

¹⁴⁹ Michel Foucault, *a.g.k.*, 2003, s.87 - 88.

¹⁵⁰ <http://www.felsefeekibi.com/site/default.asp?PG=1270>, (Erişim Tarihi: 09.02.2013).

¹⁵¹ Michel Foucault, *a.g.k.*, 2003, s.86.

¹⁵² David Lyon, *a.g.k.*, 1997, s.92.

¹⁵³ Michel Foucault, *a.g.k.*, 2006, s.295.

¹⁵⁴ *a.k.*, s.297.

uygulanabilecek türdendir. Dolayısıyla panoptikon Foucault'nun deyimiyle sadece bir hapishane değil, bir iktidar teknolojisi, bir gözetim projesidir.¹⁵⁵ Panoptikon, düşünce tarihinde geliştirilen bir dizi ideal toplum modelinden biridir. Nitekim Bauman'a göre panoptikon, tüm toplumun tanımlayıcı bir modeli olarak görülebilir. Ona göre panoptikon tek bir dairesel binayla sınırlı bir minyatür modeldir; ancak en önemli tarafı kusursuz bir toplumun idealize modeli olmasıdır.¹⁵⁶

Panoptikon hapishane modelinin en büyük etkisi tutukluda veya işçide, yani gözetime maruz kalan kişide iktidar tarafından sürekli bir görülebilirlik hissini oluşturmaktır. Gerçekte gözetleme süreci çok kısa olabilir veya hiç gözetleme de yapılmayabilir. Fakat gözetleme yapanın görülmediği ve gözetleme faaliyetinin her an yapılabilir olması hali gözetlenende sürekli gözetime maruz kaldığı düşüncesini oluşturur. Bu nedenden ötürü Bentham, “iktidarın görünür ve varlığının kanıtlanamaz ilkesini” ortaya koymuştur. Görünür olma ilkesi; tutuklu veya işçinin, sürekli olarak göz önünde ve gözlenebilir olmasını ifade etmektedir.¹⁵⁷

Varlığının kanıtlanamaz olması ilkesi; tutuklunun ya da işçinin o anda kendine bakılıp bakılmadığını asla bilmemesi, fakat bunun her an olabileceğinden hiçbir kuşkusunun da bulunmamasını ifade etmektedir. Bu duygunun yaşanabilmesi için, sürekli olarak gözetlendiği duygusunun kişi tarafından içselleştirilmesi gereklidir. Görünür olma ve varlığının kanıtlanamaz olması ilkelerinin aynı zamanda iktidarın varlığının sürekliliğini sağlayan birer garantör olduğu ifade edilebilir.¹⁵⁸

Günümüzdeki gözetim faaliyetleri açısından değerlendirildiğinde gözetim teknolojileri panoptikon modelindeki kule ve mimariyle, yaşadığımız dünya da hapishane metaforu ile ifade edilebilir. Nitekim bu benzeşmeyi Mark Poster “süperpanoptikon” kavramıyla tanımlamaktadır.¹⁵⁹ Ona göre süperpanoptikon, veri imajları ile çevrelenmiş sanal dünyayı ifade eder. Yani bireyler siber uzay içinde kendilerini takip eden gözler gerçekliğinin farkında bile olmadan duvarsız, penceresiz, gözetleme kulesiz bir gözetim çevresinin içine mahkum olmuştur.¹⁶⁰

¹⁵⁵ Michel Foucault, *a.g.k.*, 2003, s.87.

¹⁵⁶ Zygmunt Bauman, *Özgürlük*, Çev. V. Erenus, Sarmal Yayınevi, İstanbul, 1997, s.31.

¹⁵⁷ Yüksel Akaya, “İş Yasası Mı, Panoptikon Hapishane Talimatnamesi Mi?”

<http://www.hukuki.net/hukuk/index.php?article=445>, (Erişim Tarihi: 19.04.2013).

¹⁵⁸ *a.k.*

¹⁵⁹ Colin J Bennett, “Privacy in the Political Systems: Perspectives from Political Science and Economics”, 1995, s. 11. <http://web.uvic.ca/polisci/bennett/pdf/westinbook.pdf>, (Erişim Tarihi: 19.04.2013).

¹⁶⁰ Mark Poster, “Databases as Discourse; or Electronic Interpellations”, *In Computers, Surveillance, and Privacy*, Ed. David Lyon, Elia Zureik, University of Minnesota Press, Minneapolis, 2001, s.175 - 192.

Süperpanoptikondaki sanal dünyada bedenler şebekelere, veritabanlarına, elektronik bilgi koridorlarına tespih tanesi gibi dizilmektedir. Böylece bedenler Poster'in deyimiyle ipe geçirilmektedir. Tüm bu bilgi depolayan sistemler sayesinde artık gözetlenmekten kaçabilecek ya da etrafında direniş oluşturabilecek bir alan kalmamıştır. Zira bireyin yapacağı her elektronik işlem veya atacağı her adım süperpanoptikonu oluşturmaktadır.¹⁶¹

Günümüzde panoptikon modelinde olduğu gibi gözetleme artık tek bir merkezden yapılmamaktadır. Zira bugün gözetimin temel dayanağı olan gözetim teknolojileri o kadar çok yaygınlaşmış ve kolay elde edilir olmuştur ki artık daha çok kurum ve kişi (örneğin, polis, sigorta şirketi, alışveriş şirketleri, bankalar, istihbarat birimleri vb.) tarafından yapılabilmektedir.¹⁶² Bu durumda artık gözetleme kulesinin yeri de bilinmemektedir. Bu açıdan panoptikonda temel olan görünmezlik günümüzde gerçek anlamını bulmuştur.

Foucault tarafından gerçekte herhangi bir kullanımdan bağımsız olarak düşünülmesi gereken bir siyasal teknoloji figürü olarak ifade edilen panoptikon, mimari bir yapılanma olmanın ötesinde politik ve toplumsal bir yapılanmayı da simgelemektedir.¹⁶³ Panoptikonda hücredekilerin sürekli gözlerinin önünde duran ve bütün binaya hakim durumdaki kule, iktidarın simgesidir. Buradaki gözetleyici “her şeye kadir” yarı - tanrısal bir görüntüyle, beşeri “gerçek varlık” görüntüsünü kendi üzerinde birleştiren kişidir.¹⁶⁴

İktidardaki güç, toplanan bilgilere dayanarak toplumsal yapılarda, kurumlarda ve sistemlerde niceliksel ve niteliksel değişimler ve biçimlendirmeler yapmaktadır. Ancak bu bilgi toplama sürecinde toplumdaki bireyler ayırım yapılmaksızın gözetlendiği, fişlendiği, denetim altına alındığı için bu gözetim sisteminin yaşamın her alanına sızdığını ve bu süreçte iktidarın görünmez hale geldiğini söylemek mümkündür.¹⁶⁵

Modern gözetimle ilgili olarak ilk ortaya çıkan önemli çalışmalardan birisi de George Orwell'in *Bin Dokuz Yüz Seksen Dört* distopyası ve ortaya koyduğu birçok bilimsel kaynağa ilham veren “Büyük Birader” metaforudur. *Bin Dokuz Yüz Seksen Dört*¹⁶⁶, George Orwell

¹⁶¹ a.k, s.281 - 294.

¹⁶² Kirstie Ball, a.g.k, s.5 - 6.

¹⁶³ Michael Foucault, *Discipline and Punish: The Birth of the Prison*, Penguin Books, Harmondsworth, 1977, s.203 - 205.

¹⁶⁴ Jeremy Bentham, a.g.k, 1995, s. 45.

¹⁶⁵ Jeremy Bentham, Catherine P. Watkin, Simon Werret, *Panoptikon: Gözün İktidarı*, Çev. Barış Çoban, Zeynep Özarslan, Su Yayınları, İstanbul, 2008, s.120 - 121.

¹⁶⁶ Roman, *Avrupa'daki Son Adam (The Last Man in Europe)* ismiyle yazılmıştır. Fakat ABD ve Birleşik Krallık'taki yayımcısı ki roman bu iki ülkede aynı anda satışa sunulmuştur, pazarlama meseleleri nedeniyle romanın adını Bin Dokuz Yüz Seksen Dört'e (Nineteen Eighty-Four) çevirmiştir. Aldous Huxley'in *Cesur Yeni Dünya* isimli romanıyla birlikte, *Bin Dokuz Yüz Seksen Dört* İngiliz edebiyatının ilk ve en ünlü anti-ütöpik edebi

tarafından 8 Haziran 1949 tarihinde kaleme alınmış alegorik bir politik romandır. Hikayesi distopik bir dünyada geçmekte ve gözetim faaliyetlerinin aşırıya ulaştığı baskıcı rejime dönüşmüş bir dünyayı gözler önüne sermektedir.¹⁶⁷

Romanın ortaya koyduğu distopik dünyada totaliter bir tek partinin yönetiminde bireyler yoğun korku, propaganda ve beyin yıkama faaliyetleriyle harmanlanmış yatak odalarına kadar giren bir gözetim etkinliğinin merkezinde yer almaktadır. Romanla günümüzde de gözetleme etkinliklerini ifade ederken birer metafor olarak kullanılan "Büyük Birader" ve "Düşünce Polisi" gibi kavramlar literatüre girmiştir.¹⁶⁸ Bu kitapta esasen devletin her şeyi denetim altında tuttuğu, en küçük bir aykırılığa ve bireyselliğe izin vermediği, resmi ideolojinin bütün tarihi ve dili kendine göre kurguladığı bir toplum distopyası ortaya konulmuştur.¹⁶⁹

Orwell'in eserinde çizdiği karanlık senaryo, yurttaşların düşüncelerinin dahi denetlendiği, totaliter bir topluma doğru gidildiği şeklindedir ve devletin bireyin hayatına el koymasını anlatılır. Orwell, "Büyük Birader" adını verdiği dev bir bürokratik organizasyon tarafından, yurttaşların tele-ekranlar aracılığı ile yirmidört saat gözetim altında tutulduğu bir toplumu çarpıcı biçimde anlatmaktadır. Ekran tarafından kuşatılan kişileri yönlendirmek, günlük yaşantılarına müdahale etmek, davranış ve zihinlerine yön vermek oldukça kolaydır. Kişileri istediklerine inandırmak için geçmiş sürekli güncellenerek değiştirilir. Kimlik sahibi olma hakkı bireyin elinden alınmış, toplum tekdüze bireyler haline dönüştürülmüştür. Tekdüze olmayı reddedenler "Düşünce Polisi" tarafından tutuklanarak infaz edilmektedir.¹⁷⁰

Büyük Birader olarak ifade edilen totaliter otorite, bireyleri herkesin evinde yirmidört saat açık tutulması zorunluluğu olan tele-ekranlar, her yerde olan kameralar, muhbirler ve

Bin Dokuz Yüz Seksen Dört ve içerdiği terminoloji Can Yayınları tarafından Türkçe olarak basılmaktadır. Kitap birçok farklı dile çevrilmiştir. Türkiye'de bu roman aynı zamanda 1984 yılında beyaz perdeye de uyarlanmıştır.

¹⁶⁷ http://en.wikipedia.org/wiki/Nineteen_Eighty-Four, (Erişim Tarihi: 17.09.2012).

¹⁶⁸ a.k

¹⁶⁹ Devletin bir resmî ideolojisi vardır: İngsos. Bütün yurttaşların İngsos'un ilkelerine bağlı olması zorunludur. Vatandaşların resmî ideolojiye bağlılıkları sürekli kontrol ve test edilir. Rejimin iç ve dış düşmanları vardır. Bütün vatandaşlar bu iç ve dış düşmanlara karşı sürekli uyanık olmak zorundadırlar. Goldstein, rejim düşmanı hain, her kötülüğün arasındaki isimdir. Rejimin en önemli hedefi "Goldsteinciliğin kesin ve tümden yok edilmesidir"... Her gün rejim düşmanlarını lanetlemek için "iki dakikalık nefret" uygulaması yapılır... Ayrıca "Nefret Haftası" denen yılın bir haftasında rejim düşmanları daha yoğun olarak lanetlenir. Bu kutlamalarda sık sık bir marş söylenir: Duyguların yoğunlaştığı anlarda sık sık söylenen bir nakarattır bu. Büyük Birader'in bilgeliğine ve görkemine adanan bir ilahîdir, ama daha çok, halkın kendi kendisini hipnoz etmesi, bilinçlerin ritmik bir ses yardımıyla, istemli olarak bastırılmasına yarar.

<http://yayim.meb.gov.tr/dergiler/sayi45/akcadag.htm>, (Erişim Tarihi: 21.09.2012).

¹⁷⁰ <http://www.izleniyoruz.net>, (Erişim Tarihi: 17.06.2013).

bireyin olağan dışı aktivitelere girme niyetinde olup olmadığını değerlendirmek için kullanılan uzaktan kalp atışlarını algılayan sensörler aracılığıyla sürekli takip etmektedir.¹⁷¹

Romanda Büyük Birader hayatın her alanında denetleme yapmaktadır. Bu noktada Büyük Biraderin en büyük dayanağı, insan doğasının da buna başkaldırmayacağıdır. Çünkü insan doğası, onlara göre uysaldır.¹⁷² Romanın sonunda da ana karakter Winston bu uysallığı kazanmakta ve direnmekten vazgeçmektedir. Zira Büyük Biradere direnmek boşunadır. En sonunda Büyük Birader bütün dünyayı ele geçirecektir. İnsan kendisiyle savaşmayı bırakacak ve onu sevmeyi öğrenecektir.¹⁷³

Günümüz perspektifinde de bu durum yeni gözetim araçlarıyla yaşadığımız ilişkiyi anımsatmaktadır. Yeni gözetim araçlarına karşı direniş eksikliği, bu gözetim araçlarını kullananların da tıpkı Orwell'in romanındaki gibi, insanların direniş eksikliğini ve uysallığını bilmelerinden kaynaklanmaktadır. Oluşan sistem, insan doğasının uysallığından yola çıkarak onun oluşan tele ekranın gönüllü olarak bir parçası olmayı kabul edeceği varsayımı üzerine kuruludur.¹⁷⁴

“Büyük Birader İzliyor” (*Ing; Big Brother is watching you*), George Orwell'in *Bin Dokuz Yüz Seksen Dört* isimli kitabında geçen, “Orwellian korku”nun ismi haline gelmiş olan bir metafordur. Orwellian korku, herhangi birisinin herhangi bir yerde her an kameralar tarafından izlenebildiği ve kaydedilebildiği anlamına gelen bir korkudur. Bu korkunun asıl sebebi bu yolla bazılarının insanların özgürlük ve özel yaşamlarını ihlal ederek sistemi kötüye kullanabileceği ihtimalidir.¹⁷⁵ İnsanlar herhangi bir illegal faaliyet veya suç işleme durumunda değilse bile evlerindeki veya işyerlerindeki bilgisayarlarda kendilerini devamlı surette izleyen, dosyalarını okuyan, ailevi video ve fotoğraflarına erişebilen casus yazılımlarla baş başa kalabilmekte; günlük fiziksel hareketlerini takip eden gözetleme kameralarına takılabilmektedir. Bütün bunlar kişinin isteği ve bilgisi dışında gerçekleşmektedir.¹⁷⁶

Teknoloji mevcut hızıyla ilerlemeye devam ettiği takdirde Orwell'in kitabında bahsettiği Büyük Birader metaforundan kastedilenden daha büyük etki oluşturacak bir yapıya doğru gidileceği öngörülebilir. Fakat Büyük Birader artık, devletin tekelinde değil devlet dışı organizasyonlar ve kişilere dağılarak merkezilikten, çok merkezliliğe doğru bir süreç içerisinde ilerlemektedir. Nitekim posta kutusu büyüklüğünde hatta çok daha küçük ebatlarda

¹⁷¹ George Orwell, *Bin Dokuz Yüz Seksen Dört*, Çev. Nuran Akgören, Can Yayınları, İstanbul, 2008, s.22 - 23.

¹⁷² a.k, s.218.

¹⁷³ a.k, s.238 - 239.

¹⁷⁴ Veysel Bozkurt, a.g.k, s.1.

¹⁷⁵ Anthony C. Caputo, *Digital Video Surveillance and Security*, Elsevier Inc, Burlington, 2010, s.7.

¹⁷⁶ a.k

bireysel kameraların yurttaşlar tarafından kullanılmaya başlandığı, kameralı telefonların yaygınlaştığı, sıradan insanların bunlara rahatlıkla ulaştığı çağımızda durum daha tehlikeli gözükmektedir.

Özellikle internet, Büyük Biraderin genelleşmesine ve yaygınlaşmasına önemli katkıda bulunmaktadır. Nitekim insanların komşusunun televizyonuna veya meslektaşının bilgisayarına truva atı koymak suretiyle onu takip edebildiği bir ortamla karşı karşıyayız. Gazeteciler bir politikacının telefon faturasını ve telefonla görüştüklerinin listesini görebiliyorsa, artık gözetimin devletin tek elinden çıktığını söylemek isabetli olacaktır. Nitekim 2005 yılında İsrail’de yaşanan gözetim skandalı bunu açıkça ortaya koymaktadır. Bu olayda içinde medya patronu, telefon şirketi sahibi ve bir araba ihracatçısının da bulunduğu birçok işadamı iş rakiplerini truva atı casus programı sayesinde günlerce takip etmiştir.¹⁷⁷

Günümüzde Büyük Biraderler hayatımızın her alanında yer almaktadır; telefon konuşmalarımızı, e-posta yazışmalarımızı, internette ziyaret ettiğimiz siteleri ve kredi kartıyla yaptığımız alışverişleri sürekli olarak izleyebilmekte, sokağa çıktığımızda kameralarla donatılmış caddelerde yaptığımız her hareketi izleyerek kayıt altına alabilmekte, çıkarılan yasalarla tüm internet trafiğini izlemeleri mümkün olmaktadır.¹⁷⁸

¹⁷⁷ Nigel Gilbert, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, The Royal Academy of Engineering, London, 2007, s.18 - 19.

¹⁷⁸ Can Dündar’ın 26.08.2006 tarihinde Milliyet Gazetesinde yazdığı “Büyük birader bize bakıyor” isimli köşe yazısı: “Havaalanı... Uçuş kartı için sıradayım. Bir yer hostesi yaklaşıyor: "Artık sıra beklemenize gerek yok. Uçuş kartınızı makineden kendiniz alabilirsiniz" diyor. Zaten rezervasyon uzun süredir internetten yapıyordum. Şimdi ayırttığınız koltuğun kartını almak için de birkaç tuşa basmanız yeterli. Böylece tek bir kula muhtaç olmadan uçağa binebiliyor, hostesler yerine bilgisayar animasyonlarının yaptığı uyarı anonslarını dinleyebiliyorsunuz. Otel... Almanya’da küçük bir madenci şehri... Gece... Otelin kapısı kilitli... Zili çalınca mekanik bir ses kod numaranızı girmenizi söylüyor. Girişteki panele numaramızı tuşluyoruz, kapı açılıyor. İçeride resepsiyon memuru yok, herhangi başka bir görevli de... Otel boş; bomboş. Her şey kod numaralarına ve güvenlik kameralarına emanet... Girişi geçtikten sonra susadıysanız içecek makinesine para atıp suyun kod numarasını yazıyor ve suyunuzu alıyorsunuz. Acıktıysanız yine soğutucunun camkanında görünen sandviçlerden birinin numarasını tuşluyor, karnınızı doyuruyorsunuz. Sonra yukarı çıkıp bu kez odanızın kod numarasını yazıp kapıyı açıyorsunuz. İşte yine tek bir Allah’ın kulunu görmeden odanızdasınız. Şifreyi girerseniz paralı TV’de yeni filmler var. Ödeme yapmadan kaçmaya kalkışmayın; otelin her bir yanına yerleştirilmiş kameralarda kaydınız var. 21. yüzyıl insanının sindirilmişliğinin, kıştırılmışlığının, yalnızlığının simge mekanı burası... Ürkütücü bir yeniçağın son sığınağı... Sokak... Metrolar kondüktörsüz... Yol kenarında paralı büyük kutular tuvalet... Peçeteci, kolonyacı yok; büyük küçük ayrımı da... Banka hizmetleri, bilet gişeleri, sigara büfeleri, gazete bayileri, çamaşır makineleri hepsi parayla çalışan kutulardan ibaret... Ancak bir kişinin sığabileceği tek kişilik "sinema salonları", attığınız para kadar film izlemenize izin veriyor. Polis yok sokaklarda; kameralar var. Otoparklar kart ya da parayla; değnekçi, gişe görevlisi yok. Hizmet sektörü tam insansızlığa gidiyor, koşar adım. Kort... Avrupa tenis turnuvası... Maçta top tam çizgiye düşüyor. Hakem "Dışarıda" kararı veriyor. Topu atan oyuncu "İçeride" diye itiraz ediyor; kameralara bakılmasını talep ediyor. Marttan beri uygulanan kurallara göre bu hakkı var. Maç duruyor. Gözler korttaki dev ekrana çevriliyor. Az sonra son atılan topun elektronik izlekte kayıtlı hareketi geliyor ekrana... Top içeride; hakem haksız. Karar düzeltiliyor. Elektronik hakemler, insanların yerini almaya hazırlanıyor. Bunlar kısa bir geziden izlenimler... Otomasyon salgınına dair daha yüzlerce örnek var. Bir kısmı gündelik hayatımızı kolaylaştıran, insanlara boş vakit yaratacak türden teknolojik yenilikler... Bir kısmı ise korkutucu işaretler: Sadece dev bir işsizler ordusu yaratmasıyla değil, aynı zamanda

Günümüzde özellikle bilgi ve iletişim teknolojileriyle birlikte bir “gözetim kültürü”nden söz edilmeye başlanmıştır. Bu kültürün Orwell’ın distopyasından en önemli farkı, artık gözetimin sadece “Büyük Birader” olarak nitelendirilen iktidar ve iktidar organları tarafından yapılmamasıdır. Staples’a göre artık bu yeni gözetimde sadece Büyük Birader yoktur. Günümüz gözetimi doğrudan veya dolaylı olarak artık “Küçük Biraderler” tarafından gerçekleştirilmektedir.¹⁷⁹ Staples’in bu görüşünü Mitchel de destekler. O da bir tane “Küçük Birader” yerine “Küçük Biraderler Sürüsü” ile karşı karşıya kaldığımızdan bahseder. Mithcell, “Küçük Birader ” ya da onun tanımıyla küçük diktatör durumunu şu şekilde ifade etmektedir:¹⁸⁰

“İki taraflı elektronik iletişim cihazları çoğaldıkça ve çeşitlendikçe, hayatlarımız siber uzayda daha bütünlüklü ve ayrıntılı izler bırakmaya başladı. Geniş çaplı kullanıma ulaşan bu türdeki ilk cihaz telefon olmuştur. Çok kısa sürede, görüşmelerin ne zaman, nerede, kim tarafından yapıldığını gösteren fatura bilgilerine ulaşılmıştır. Sonra ATM, para çekme makineleri ve perakende satış mağazalarındaki satış noktalarında yapılan işlemlerin kayıtları tutulmaya başlanmıştır. Kişisel bilgisayarlar ticari çevrimiçi ağlarına bağlanmaya başlayınca, onlar da elektronik izler bırakmaya başladılar. Artık anahtarlı video ağları alışveriş, banka işlemleri, film secimi, sosyal iletişim, siyasi toplantılar gibi günlük amaçlar için kullanıldıkça, önceden elde edebildiklerinden çok daha ayrıntılı özel yaşam görüntülerimize sahip olmaya başlamıştır.”

3. Bilgi ve İletişim Teknolojilerinden Gözetim Teknolojilerine

Günümüzde dijital iletişim sistemleri modern toplumun can damarı haline gelmiştir. İnsanlar internet üzerinden çevrimiçi bağlantılarla buluşmakta, günde onlarca kez düşüncelerini ve faaliyetlerini twit atmakta, çeşitli sosyal medya programları üzerinden diğer insanlarla etkileşim kurmakta, alış-verişlerini sokağa adımını bile atmadan internet üzerinden yapmaktadırlar. Kamusal işlemlerini e-devlet portalları üzerinden yürütmekte, araba alım-satım işlemlerini internet üzerinden gerçekleştirmektedirler. Bunun gibi dijital sistemlerin bireyin hayatını kapsayışını anlatabilecek çok sayıda örnek bulunmakta ve her geçen gün de giderek bu örnekler çoğalmaktadır.

Bilgi ve iletişim teknolojileri insanların hayatını her yönüyle çevrelemiştir. Bilgi ve iletişim sistemleri üzerinden kurulan ilişkiler ve etkileşimler farklı yazılımlar yoluyla rahatlıkla takip edilebilmektedir. Günümüzde yaygın olarak kullanılan sosyal medya

insanın insanla iletişimine son vermesiyle, insanoğlunu derin bir yalnızlığa itmesiyle ve tüm hayatı makinelerin emrine vermesiyle de ürkütücü bir yarının habercisi... Barkodunuzu iyi ezberleyin: Yakında onu tuşlayıp ya da kırıp sicilinize ulaşacaklar; hesap defterlerinize, e-posta adreslerinize, genetik özelliklerinize, gezdiğiniz internet sitelerine, yediğiniz sandviçlere, seyrettiğiniz filmlere... Kamera kayıtlarınıza, cep mesajlarınıza, kütüphaneden aldığınız kitaplara, çekip sakladığınız fotoğraflara, sağlık raporlarınıza... Barkodunuz demir parmaklığınız olacak. Şifrenize kelepçeleneceksiniz...”

¹⁷⁹ William G. Staples, *The Culture of Surveillance: Discipline and Social Control in the United States*, St. Martin's Press, New York, 1997, s.129.

¹⁸⁰ William J. Mitchell, *City of Bits*, MIT Press, Cambridge, 1996, s.156 - 159.

araçlarından *Twitterı* kullananları takip etmek için aynı programın sahipleri tarafından *TopsyPro* isimli bir program oluşturulmuş ve yüksek meblağlar karşılığında satışa sunulmuştur.¹⁸¹ İnternet üzerinden alacağınız kullanıcı adı ve şifresiyle bu program üzerinden insanların *Twitter* hesaplarını takip edebilir, farklı analizler yapabilirsiniz.

Yukarıda belirtilen *Twitter* örneğinde olduğu gibi günümüz bilgi sistemlerini üretenler, aynı sistemler üzerinden geçen bilgileri toplayacak, analiz edecek gözetim sistemlerini de geliştirmektedirler. Bu bakımdan bilgi ve iletişim teknolojileri ile gözetim teknolojileri birbirine eklemlenmiş, hatta birbirinin yerine kullanılan terimler haline gelmiştir. Bu durumun diğer bir temellendirmesi de bilgi ve iletişim teknolojilerinin gelişiminde yer alan teknoloji bilgisinin gözetim teknolojilerini geliştirmek için de kullanılabilir olmasıdır. Elektronik izlerin takip edilmesi gerekliliği ve modern elektronik araçlarla bu izlerin takip edilmesinin kolay olmasından dolayı bilgi ve iletişim teknolojileri gözetim teknolojilerine evrilmiştir. Bu bölümde bilgi ve iletişim teknolojilerinin gözetim teknolojileri üzerindeki etkisine ve gözetim sektörüne olan katkısına vurgu yapılacaktır.

Gözetleme, geçmişte somutlaşmış, insanların göz ile diğerleri tarafından izlendiği bir işlem olarak varlığını sürdürmüştür. Her ne kadar günümüzde son derece gelişmiş gözetim teknolojileriyle gözetimin şekli değişmiş olsa da tarih boyunca önemini yitirmemiş olan birçok temel ve insan bazlı gözetim faaliyetleri de unutulmamalıdır. Zira gelişmiş gözetim teknolojilerine rağmen esasen bu temel gözetim faaliyetleri halen varlıklarını devam ettirmektedir.

Yukarıda ifade edilen temel gözetim faaliyetleri, basit gözlem, bire bir izleme, kulakla dinleme, ajan kullanma, muhbirler, yüz yüze yapılan mülakat ve görüşmeler, kişilerle ilgili tutulan bilgi notları vs. şeklinde örneklendirilebilir. Tarih boyunca birçok otoriter gözetim rejimleri toplumda; istilaya uğrama, bölünme, yabancı devlet ajanlarının varolması gibi halk ve yöneticiler üzerinde şekillendirdikleri korkularla güvensizlik ortamları oluşturmuştur. Bu sayede de belirtilen temel gözetim faaliyetleri toplumsal hayatta yoğun olarak kullanılmıştır.¹⁸² Buna örnek olarak İkinci Paylaşım Savaşı öncesindeki Japonya, eski Doğu Bloğu ülkeleri, özellikle nüfusun altıda birini muhbir olarak işe aldığı iddia edilen Alman Demokratik Cumhuriyeti gösterilebilir.¹⁸³

¹⁸¹ <https://pro.topsy.com/>, (Erişim Tarihi: 13.12.2013).

¹⁸² David Murakami Wood, *a.g.k*, s.16 - 17 - 18.

¹⁸³ Bu konuyla ilgili olarak 2006 Alman yapımı “Das Leben Der Anderen” filminde anlatılan gözetleme faaliyetleri örnek gösterilebilir.

Günümüzde bilgi ve iletişim teknolojilerindeki ilerlemeler kişisel verilerin çok uzak mesafeler arasında daha hızlı akmasına olanak sağlamış ve gözetlemeyi küresel bir aşamaya getirmiştir.¹⁸⁴ Gözetlemenin bu aşamaya gelmesinde bilgi ve iletişim teknolojilerinin gözetimle ilgili dört teknolojik alanda sağladığı etki önemlidir. Bunlar; telekomünikasyon teknolojileri, işitsel - görsel kayıt teknolojileri, dijital bilgisayar teknolojileri ve takip - tarassut teknolojileridir.¹⁸⁵

Gözetim teknolojilerinin gözetimin doğasında bir takım değişimlere neden olduğu bir gerçektir. Bu kapsamda gözetim teknolojisi hakkında birkaç tane genel tespit yapılabilir. Birincisi, bu teknolojilerde kalıcı bir “iyilik” veya “kötülük” yoktur. Örneğin; devlet tarafından yurttaşları için tutulan veri tabanları, genel sağlık politikaları oluşturulurken toplumdaki sağlık sorunlarının tespitinde ve bu sorunların bölgesel analizinde önemli bir kaynak olabilirken; diğer taraftan aynı veri tabanları toplumu sınıflara ayırıp, bireyleri farklı muamelelere maruz kalmaya itebilecek araca da dönüşebilir. Bu noktada ileride açıklanacak olan gözetimin ikiyüzlülüğü kavramı ortaya çıkmaktadır.

Gözetim teknolojileri sonuçları itibariyle değişkenlik gösterebilecekleri gibi ortaya çıkış nedenleri ve kullanımları açısından da farklılık gösterebilmektedirler. Bütün teknolojiler genelde somut belli hedefler için ve belli kurumlar için geliştirilirler. Teknolojiyi kullanım ve geliştirme açısından süreç içerisinde bu hedefler ve kurumlar değişebilirler. Örneğin cep telefonları başlangıçta ses iletişimi amacıyla ortaya çıkmışken artık bu amacı dışında mesaj gönderme, kamera, internet, GPS gibi özelliklerle amaç değişikliğine uğramıştır.¹⁸⁶ Başlangıçta insanlar arasındaki iletişim sorunlarını gidermek amacıyla ortaya çıkarılan bilgi ve iletişim teknoloji ürünleri, daha sonra tamamen veya kısmen gözetim faaliyetlerinde kullanılır hale gelmiş; hatta iktidarlar tarafından toplumun daha iyi gözetlenebilmesi için kullanımının yaygınlaştırılması desteklenen gözetim teknoloji ürünlerine dönüşmüşlerdir.

Gözetim teknolojilerinde başat rol oynayan telekomünikasyon teknolojilerinde gözetim; bireylerin, kurumların ve tüzel kişilerin başkasına ait telekomünikasyonun içeriği, gerçekleşme şartları (zaman, yer vs.) hakkında bilgi toplama, toplanan bilgileri kategorize etme ve canlı olarak telekomünikasyonu izleme şeklinde gerçekleşmektedir. Telekomünikasyon; iletişim teknolojilerinin altyapısını, telekomünikasyonun gerçekleştiği sistem ve cihazları, mesaj - veri veya bilgi iletişimini kapsamaktadır. Dolayısıyla

¹⁸⁴ David Lyon, *a.g.k*, 2006, s.89 - 90.

¹⁸⁵ David Murakami Wood, *a.g.k*, s.16 - 17 - 18.

¹⁸⁶ *a.k*

telekomünikasyonun içerisinde hem analog hem de dijital sistemler varlığını sürdürmektedir. Bu kapsamda cep telefonu teknolojisi, faks cihazları, sabit telefon teknolojisi, GPRS - internet gibi bilgisayar iletişim teknolojilerini bünyesinde barındırmaktadır.¹⁸⁷ Telekomünikasyon teknolojilerinde gözetim de bu teknolojilerin hepsinde yapılan gözetim faaliyetlerini ifade etmektedir.

Telekomünikasyon sistemlerinin gelişmesinde üç önemli faktör bulunmaktadır. Bunlar; telekomünikasyon teknolojilerinin yaygınlaşması ve sistemsal gelişimi, bilgi depolama ve işleme kapasitesindeki gelişmeler, telekomünikasyon pazarlarının devlet tekelinden çıkıp çeşitlenmesi olarak ifade edilebilir. Son yirmi yıllık süreç içerisinde teknolojik gelişmeler ve değişimler telekomünikasyon sistemlerince çok çeşitli teknolojilerin kullanılmasına neden olmuştur. Radyo frekanslı cihazlar (cep telefonlarının ortaya çıkışındaki en önemli gelişme), hızlı internet ve veri paylaşımını sağlayan optikal fiber kabloların ortaya çıkışı, kablosuz internet sistemleri, ses iletişiminin yanı sıra fotoğraf - video paylaşımını sağlayan ve konum belirleyici sistemlerle akıllı cep telefonları örnek gösterilebilir. Günümüzde bu farklı teknolojilerdeki her bir gelişim gözetimin kullanım mekanizması haline dönüşmektedir.¹⁸⁸

Elektronik gözetleme teknolojileri dünyada özellikle 1990'ların başından itibaren yaygınlaşmaya ve etkin hale gelmeye başlamıştır. Bunun altında yatan temel nedenler beş ana başlık altında toplanabilir.¹⁸⁹ Birincisi, sivil ve devlet faaliyetleri (arama - kurtarma faaliyetleri, iş güvenliği, yasalara uyma takibi, ulusal güvenlik vs.) yürütülürken elektronik gözetim araçlarının kullanılmaya başlanmasıdır.

İkincisi, toplumda “Büyük Birader”, “Biri Bizi Gözetliyor” söylemlerinin yaygınlaşması ve toplumlar tarafından *Echelon* gerçeğinin algılanmaya başlanmasıdır. Üçüncüsü, bilgisayar teknolojisinin halk arasında yaygınlaşması, internetin geliştirilip halk tarafından benimsenmesidir. Dördüncüsü, yönetim dünyasında teknolojik ilerlemelere paralel hareket etme gayretinin ve endişesinin ortaya çıkmasıdır. Beşincisi, halkın istihbarat örgütlerinin gözetleme araçlarını kötüye kullanabileceği kaygısını taşımaya başlaması ve bu kapsamda takip edilemediğini düşündüğü yeni teknolojik araçlar aramasıdır.

Ayrıca araba alarmlarının arabalara monteli satılmaya başlaması, büro veya bina güvenliği için kapalı devre kamera sistemlerinin yaygınlaşması, gelişmiş hırsız alarm

¹⁸⁷ a.k

¹⁸⁸ a.k

¹⁸⁹ Julie K. Petersen, a.g.k, s.50 - 51.

sistemlerinin kurulması, kreşlere kamera kayıt sistemlerinin kurulması gibi gelişmelerle toplumda gözetim teknolojilerine karşı oluşan gereklilik algısı geri dönüşü olmayan bir gözetim sektörü kurulmasına neden olmuştur.¹⁹⁰

Diğer taraftan teknik olarak gözetim faaliyetlerinde analog sistemlerden dijital sistemlere geçilmesinin teknoloji üretiminde hız ve kolaylık sağlaması açısından gözetim teknolojilerinin gelişimine sağladığı katkı da yadsınamaz. Zira dijital video gözetleme sistemleri ile birlikte gözetleme daha kolay ve ucuza yapılmaya başlanmıştır ki bu da gözetimin topluma yayılmasında etkili olmuştur.¹⁹¹

Görüldüğü üzere bilgi ve iletişim teknolojileri alanındaki gelişmeler, gözetim teknolojilerini etkilemekte ve gözetim teknolojilerindeki gelişmeler de gözetimin topluma yayılmasına yol açmaktadır. Artık, gözetim teknolojilerinin son derece geliştiği ve giderek yeni teknolojilerin ortaya çıktığı günümüzde sıradan bilgisayar ve elektronik ürünler satan her hangi bir mağazada veya internet satış mağazalarında gözetim teknoloji ürünlerini ve gözetim kataloglarını incelemek ve ucuza satın alabilmek oldukça kolay hale gelmiştir.¹⁹²

Günümüzde bireyler bir haftalık maaşları ile komple bir gözetleme sistemini evlerine kurabilecek durumdayken, 1990'ların başlarında bunun için bir servet ödemeleri gerekirdi. Gözetim araçlarına kolay ulaşılabilirliği ortaya koymak için fiyatlarından örnekler verilebilir. Bugün internet satış mağazalarından kalem kameralar 59 TL'ye, uzaktan dinleme cihazı 480 TL'ye, araç takip cihazı 500 TL'ye, telefon dinleme programları 1000 TL'ye, facebook takip programı 50 TL'ye, duvar saati gizli kamera sistemi 300 TL'ye rahatlıkla satın alınabilir.¹⁹³ Diğer taraftan uydu görüntülerini internette ücretsiz veya makul ücrete canlı olarak sağlayan internet siteleri de mevcuttur; hatta Türkiye, İngiltere ve Amerika'da bazı belediyeler internet sitelerinde belediye bölgelerini 24 saat canlı görüntüyle herkese ücretsiz sunmaktadırlar.¹⁹⁴

Gözetim teknolojisindeki gelişimi sağlayan bilgi ve iletişim teknolojik gelişmeleri tarihsel olarak şu şekilde sıralanabilir. Bilgisayarların icat edilmesi ve yazılı kaynakların dijital ortama geçmesi, “*mainframe*”lerin¹⁹⁵ icat edilmesi ve bilginin paylaşımının kolaylaşması, telekomünikasyondaki hızlı gelişme ve reform hareketleri, verinin telekomünikasyon şebekeleri üzerinden taşınmaya başlanması, masaüstü kişisel

¹⁹⁰ a.k

¹⁹¹ a.k

¹⁹² a.k, s.4.

¹⁹³ www.casuskamerafiyat.com, (Erişim Tarihi: 16.03.2013).

¹⁹⁴ Julie K. Petersen, a.g.k, s.4.

¹⁹⁵ *Mainframe*; ana bilgisayar veya ölçüleri ve kapasitesi itibarı ile büyük bir bilgisayarı ifade eder. www.bilisimterimleri.com/?arananterim=frame&dil=eng, (Erişim Tarihi: 16.03.2013).

bilgisayarların icadı, modemın icadı (evlere kadar gitmiş olan telefon şebekeleri üzerinden veri iletişimine izin vermiştir), yazılım ve donanım alanında görülen olağanüstü gelişmeler, mikrodevre (*İng; chip*) boyutlarının milyonlarca kat küçülmesi ve fiyatlarının ucuzlaması, buna bağlı olarak bilgisayar ve iletişim teknolojisinin ucuzlaması, işletim sistemlerinin görselleşmesi ve kullanımının olağanüstü kolaylaşması olarak ifade edilebilir.¹⁹⁶

Bütün bu gelişmelerin yanında gözetleme teknolojisinde başat rol oynayan, günümüzde en önemli gözetleme aracı haline gelmiş ve toplanan verinin saklanmasına, eşlenmesine, geri getirilmesine, işlenmesine, pazarlanmasına ve dolaştırılmasına olanak sağlayan “bilgisayarlar ve bilgisayar teknolojileri”dir. Veriler, numaraların ve isimlerin ötesinde DNA kodları veya fotoğraf görüntülerine kadar uzansa da, gözetlemenin gerçekleşmesini sağlayan teknolojiler bilgisayar gücü içermektedir. Bilgi ve iletişim teknolojilerini de gözetlemenin merkezine koyan şey bilgisayar uygulama alanları ve bunların teknik açıdan muazzam büyümesidir.¹⁹⁷

İnternet teknolojilerinin gelişmesi ve ortaya koyduğu etki alanı gözetleme faaliyetlerinin çok daha kolay yapılmasını sağlamıştır. Ayrıca *Facebook*, *Twitter*, *Msn*, *Linkedn*, *Flickr* gibi sosyal paylaşım siteleri vasıtasıyla insanların en gizli bilgileri dijital ortama kolay ve güncel olarak aktarılır hale gelmiştir. Diğer taraftan kişinin internete girdiği bilgisayarın IP adresi numarası¹⁹⁸ ile hangi sitelerde dolaştığına, internet üzerinde ne gibi işlemler yaptığına uzman ekiplerce rahatlıkla ulaşılabilir ve elde edilen bu verilerle yapılan analizler neticesinde bireyin iç dünyasına kadar profil çalışmaları gerçekleştirilebilir olmuştur.

Günümüzde internet; alışveriş, ticaret, bilimsel faaliyetler, toplumsal örgütlenme, siyasi propaganda, eğlence gibi birçok alanda kullanılmaktadır. İnternetin bu kadar çeşitlilik arz eden alanlara yansması ve sağladığı hız, bürokrasinin olmaması gibi kolaylıklarla birlikte günlük hayat içindeki birçok faaliyetin internet üzerinden yapılmasına teşvik etmektedir.¹⁹⁹ İnsanların faaliyetlerini internet ortamına taşımasıyla birlikte, ekonomik kayıtlardan sağlık

¹⁹⁶ Hakan Yıldırım, *a.g.k*, s.23.

¹⁹⁷ David Lyon. *a.g.k*, 2006, s.13.

¹⁹⁸ IP adresi (İnternet Protokol adresi), TCP/IP (İletim Kontrol Protokolü/İnternet Protokolü) standardını kullanan bir ağdaki cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve veri alışverişinde bulunmak için kullandıkları benzersiz bir numaradır. İnternet bağlantısı bulunan her cihazın bu cihaza tahsis edilen bir adresi olması gerekir. Bu adres ya da numara, iletilen bilginin doğru adrese gönderilmesini, ya da verinin doğru adresten alınmasını sağlar. IP adresi ya da numarası, bugün suçluların takibinden online satış ve pazarlamaya kadar çok çeşitli alanlarda yaygın olarak kullanılan bir veridir. IP numarasına bakarak kullanıcının bulunduğu ülkeyi, kenti, enlem ve boylamı ve İSS'yi (İnternet Servis Sağlayıcısı) belirlemek mümkündür.

<http://www.ip-numaram.com/ipadres.html>, (Erişim Tarihi: 16.03.2013).

¹⁹⁹ Necati Alkan, “Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler”, *Çağın Polisi Dergisi*, Ağustos 2003, Sayı 20, s.41 - 42.

kayıtlarına kadar uzanan geniş yelpazedeki kişisel bilgilerin internet üzerinde depolanmasının yolu açılmıştır. İnternet üzerinde yapılan bu işlemler, bir yandan bireyin hayatını kolaylaştırırken diğer taraftan da geniş veri ambarları oluşmasına yol açmıştır. Bu veri ambarları, bilgi toplumundan gözetim toplumuna doğru evrilen dünyamızda önemli araçlardandır.

İnternet her geçen gün geliştirilen altyapısı ile daha çok verinin toplanmasına, depolanmasına, sınıflandırılıp herkesin ulaşımına açılmasına olanak sağlamaktadır. Böylelikle internet her zaman her şekilde kullanıcılarının istedikleri bilgilere ulaşımına ve onların bilgi paylaşımına izin vermektedir. Bu bilgiye kolay ve hızlı ulaşım açısından olumlu karşılanabileceken, elektronik gözetimin yaygınlaşmasında ve güçlenmesinde bir araca dönüşmesi bakımından tehlikeli gözükmemektedir.²⁰⁰ Örneğin Ankara Üniversitesi'nde öğrenci olan Özgür Günaydın isimli şahıs ile ilgili, bu kişi bilgi ve iletişim teknolojilerini hiç kullanmasa bile, hakkında internette arama motorlarında yapılacak birkaç aramayla bilgi sahibi olunabilmektedir. Üstelik bu kişinin *Facebook*, *Twitter* gibi sosyal paylaşım sitelerinde hesabı varsa onun ve çevresi hakkında birçok bilgiyi toplamak da mümkündür. Elektronik posta kullanıyorsa casus yazılımlarla elektronik postasının içeriğine ulaşarak kimlerle nasıl bir irtibatı olduğu çözümlenebilir. Bunlar internet üzerinden yapılabilecek gözetleme faaliyetlerine sadece birkaç örnektir. Bu bakımdan gözetim toplumu sürecinde internetin etkisinin yadsınamayacağı ifade edilebilir.

Bilgi ve iletişim teknolojilerindeki gelişmelerle gözetim, kişilerin bedenlerinin takibinin yanı sıra elektronik izlerinin sürülmesine de yoğunlaşır olmuştur. Bu gözetim araçlarıyla bireyler birer dijital kodun parçası haline gelmeye başlamıştır. Bilgi ve iletişim teknolojilerinin artan kullanım oranı gözetimi sıradan insanların da hayatına sokmuştur. Bu noktada artık herkesin gözetime maruz kaldığı ya da maruz kalma ihtimali olduğu ifade edilebilir. Sonuç olarak bilgi ve iletişim teknolojilerinin her geçen gün artan gücünün gözetimin gücü ile paralellik arz ettiği iddia edilebilir. Geleneksel gözetim metotları ile kıyaslandığında gözetleme sistemlerinin gittikçe daha az belirgin, ancak giderek daha sistematik ve zekice olduğu söylenebilir.²⁰¹

Bu bölümde, hızla gözetim toplumuna evrilen günümüz dünyasında bilgi ve iletişim teknolojilerinin gelişim seyri, bu paralelde sosyal alanda oluşan etkileşim kültüründen bahsedilecektir. Gözetim teknolojilerinin bilgi ve iletişim teknolojileri ile olan ilişkiselliği

²⁰⁰ a.k

²⁰¹ David Lyon. *a.g.k*, 2006, s.12.

anlatılacak ve sonunda da bu teknolojilerin kamusal yansıması olan e-devlet düzeni tartışılacaktır.

3.1. Gözetim Teknolojileri ve Dijital Kültür

Bilgi ve iletişim teknolojileri²⁰² bilginin toplanmasını, işlenmesini, saklanmasını ve gerektiğinde herhangi bir yere iletilmesini ya da herhangi bir yerden bu bilgiye erişilmesini sağlayan teknolojiler, uygulamalar ve hizmetlerin bütünü olarak tanımlanabilir.²⁰³ Bu teknolojiler başka bir tanımda, “bilginin gerektiğinde herhangi bir yere iletilmesini ya da herhangi bir yerden bu bilgiye erişilmesini, elektronik, optik ve benzeri tekniklerle otomatik olarak sağlayan teknolojiler” olarak açıklanmaktadır.²⁰⁴ Küreselleşmeyle bağlantılı olarak başka bir tanımlama da “bireyler, organizasyonlar ve ülkelerarası etkileşimi hızlandıran, küreselleşme sürecine katkıda bulunan bilgi tabanlı teknolojik gelişmeler” şeklindedir.²⁰⁵

Bu tanımlamalardan daha geniş olarak Webster’a göre bilgi ve iletişim teknolojileri, bilginin toplanmasında, işlenmesinde, depolanmasında, ağlar aracılığıyla bir yerden başka bir yere iletilmesinde ve kullanıcıların hizmetine sunulmasında yararlanan, iletişim ve bilgisayar teknolojilerini de kapsayan bütün teknolojilerdir.²⁰⁶ Bu çalışmada bilgi ve iletişim teknolojileri, toplumsal faaliyetleri ve toplumsal unsurları dijitalize eden, gün geçtikçe gelişen ve değişen, gözetleme faaliyetlerine doğrudan hizmet eden ve bunların altyapısını oluşturan tüm bilgi tabanlı sistemler anlamında kullanılacaktır.

Günümüzde bilgi ve iletişim teknolojileri sayı ve çeşit açısından oldukça geniş bir yelpazeye yayılmış durumdadır. Buna yüksek bilgisayar teknolojileri, uydu ağları, televizyon, video, dijital radyo, internet, kablosuz iletişim araçları (mobil telefon, harici bellek, Cd-Rom ve dijital/sesli posta, vb.), 3G - 4G mobil teknolojileri gibi teknolojik gelişmeler örnek gösterilebilir. Bu teknolojilerin dijital bilgi ağı bağlamında bilginin sınır ötesi akışını, sınırsız

²⁰² Günümüz bilişim teknolojilerini ifade etmede “Information Technologies – enformasyon teknolojileri”, “Information and Communication Technologies – Bilgi ve İletişim Teknolojileri” ve “Informatics – Bilişim” kavramları kullanılabilir. Bu kavramların Türkçe karşılıklarının tam olarak konumlandırılmaması ve birbiri yerine kullanılabilir olması bu alanı sorunlu hale getirmektedir. “Information and Communication Technologies” kavramının Türkçe karşılığı olarak “enformasyon ve iletişim teknolojileri”, “bilgi ve iletişim teknolojileri” ya da “bilişim teknolojileri” kullanılmaktadır. Bu çalışmada son dönem teknolojik gelişmeler ve yarattığı olanaklar için “bilgi ve iletişim teknolojileri” kavramı kullanılacaktır.

Gamze Yücesan Özdemir, *Emek ve Teknoloji*, Tan Yayınları, Ankara, 2009, s.15.

²⁰³ Hakan Yıldırım vd., *a.g.k.*, s.181.

²⁰⁴ Ceyhan Yurdakul, H.Ufuk Çağlayan, *Bilgi teknolojileri Türkiye İçin Nasıl Bir Gelecek Hazırlamakta*, Kültür Yayınları, Ankara, 1997, s.14.

²⁰⁵ Adem Ögüt, *a.g.k.*, s.176.

²⁰⁶ Frank Webster, “The Information Society: Conceptions and Critique”, *Encyclopedia of Library and Information Science*, ed. Allen Kent, New York, 1996, Vol. 58, Supp. 21, s.78. akt., Devlet Planlama Teşkilatı, *Sekizinci Beş Yıllık Kalkınma Planı: Bilişim Teknolojileri ve Politikaları Özel İhtisas Komisyonu Raporu*, Ankara, 2001, s.3.

depolanabilmesini, bilgiye hızlı ulaşımı da kapsadığından yeni bir dünya düzeni doğrultusunda bir değişimi doğurduğu söylenebilir.

Bilgi ve iletişim teknolojilerinin üç temel ayırt edici özelliği bulunduğu değerlendirilmektedir. Bunlar minyatürizasyon, kapasiteyi genişletme ve maliyeti düşürmek olarak ifade edilebilir.²⁰⁷ Minyatürizasyon, bilgi ve iletişim teknolojilerinin boyut olarak giderek küçülmesine rağmen işlevsel olarak oldukça geniş kapasitelere ulaşabilmesidir. Kapasiteyi genişletme ise kullanım açısından giderek yaygınlaşmasını ve kendini vazgeçilmez hale getirmesini ifade etmektedir. Maliyet açısından da talebin fazlalığı ve seri üretimin de giderek artış göstermesiyle bu teknolojilerin maliyetinde ciddi düşüşler olmuştur.²⁰⁸

İletişim ve bilgisayar teknolojisindeki gelişmeler mikroelektronik teknolojilerdeki gelişmelere bağlı olarak sürekli artmaktadır. Teknolojik gelişmelerin hangi alanda olursa olsun birbirini etkilemeleri kaçınılmaz olduğu için mikroelektronik teknolojiler de bilgi ve iletişim teknolojilerinin yenilenmesini sağlamıştır. Bu kapsamda bilgi ve iletişim teknolojilerindeki bilgi miktarındaki artış, bilgilerin saklanması ve dağıtılmasıyla ilgili kanalların geliştirilmesini de hızlandırmıştır.²⁰⁹

Bilgi ve iletişim teknolojilerinin tarihsel süreç içerisindeki gelişimi ve dönüşümü incelendiğinde kapsam ve gelişimi daha net olarak ortaya konulabilecektir. 19. yüzyılın sonlarından itibaren tarım toplumundan sanayi toplumuna doğru bir geçiş olduğu kabul edilmektedir. Bu dönüşümde teknolojik gelişmelerin etkisi yadsınamaz. 20. yüzyılın ikinci yarısından itibaren başta bilgi ve iletişim teknolojileri olmak üzere teknolojik gelişmelerin çok hızlı gerçekleşmesiyle ve bunların insan hayatına entegre olmasıyla birlikte sanayi toplumundan bilgi toplumuna geçiş gerçekleştiği kabul edilmektedir. Burada dikkat edilmesi gereken husus, tarıma dayalı geleneksel toplum yapısından sanayi toplumuna geçişin uzun yıllar sürmesine rağmen, sanayi toplumu yapısından bilgi toplumuna geçişin oldukça hızlı olmasıdır. Bu hızlı dönüşümün temel nedeni, bilgi ve iletişim teknolojilerindeki gelişmelerin oldukça hızlı olması ve insanların da bu gelişmelere ayak uydurma ihtiyacı hissetmeleridir.²¹⁰

Sanayi toplumunda artı değer maddi değer iken, bilgi toplumunda artı değer bilgi olmuştur.²¹¹ Bilginin giderek değerli hale gelmesi de onun üretim, iletim ve saklama

²⁰⁷ Haluk Geray, “1980 Sonrası Yeni Teknolojiler ve İkitelli Medyası”, *Medya Gücü ve Demokratik Kurumlar*, Afa Yayıncılık, İstanbul, 1999, s.107.

²⁰⁸ a.k, s.108.

²⁰⁹ a.k

²¹⁰ Mehmet Özçağlayan, *Yeni İletişim Teknolojileri ve Değişim*, Alfa Basım Yayım Dağıtım, İstanbul, 1998, s.16-22.

²¹¹ Adem Ögüt, a.g.k, s.25 - 31.

araçlarının giderek gelişmesine yol açmıştır. Bu açıdan hızla gelişen bilgi ve iletişim teknolojileri karşısında insanlar trenin son vagonunu yakalama telaşı içerisine girmişler ve doğal olarak bu değişimden doğan dönüşümün aktörü haline gelerek bilgi toplumu sürecinin genişlemesine neden olmuşlardır.

Bilgi ve iletişim teknolojilerindeki radikal hızlanma ve dönüşüm özellikle son 15 - 20 yıldan beri süregelmektedir. Bu süreçte özellikle iletişim teknolojisi ile bilgisayar teknolojisinin bir araya gelerek “telematik”²¹² kavramının ortaya çıkması sanayi sonrası toplumun en önemli kaynağının bilgi, en önemli altyapısının ise iletişim altyapısı olmasına yol açmıştır.²¹³ Bilgi ve iletişim teknolojilerinin gelişmesinde başat rolü bilgisayarın keşfi ve geliştirilmesi faaliyetleri almaktadır. Bilgisayarın çıkış noktası 1840’larda Charles Babbage’in geliştirdiği analitik makineye dayanmaktadır. Bu gelişmenin tetiklemesiyle 1940 yılında Mancelly ve Eckert ilk bilgisayar olarak bilinen “*ENIAC*”ı bulmuşlardır. Bu bilgisayar askeri gaye ve çalışmalarla bulunmuş ve bu amaçla kullanılmıştır.²¹⁴

İkinci paylaşım savaşının başlaması ile yönetimler bilgisayarların potansiyel stratejik önemi nedeniyle bilgisayar araştırmalarını iyice arttırmışlardır. Bilgisayar teknolojisindeki hızlı gelişme, hacim olarak oldukça büyük olan bilgisayarların küçülmesini ve ucuzlamasını sağlarken; sınırlı kullanımından, kişisel bilgisayar kullanımına kadar uzanan imkanlar doğurmuştur. Nitekim günümüzde 100 gram ağırlığındaki bir mikro işlemcinin bu dev aygıttan on kez daha güçlü bir makine olduğunu düşününce teknolojideki inanılmaz ilerlemenin farkına varabiliriz.²¹⁵

Bilgisayarlar kullanım amaçlarına göre tarihsel olarak üç döneme ayrılabilir. Masuda’ya göre birinci dönem, 1945 - 1955 yılları arasındaki “bilgi dönemi”dir. Bu dönemde bilgisayarlar genelde ulusal projelerin hazırlanmasında ve oldukça sınırlı seviyede kullanılmıştır. İkinci dönem 1955 - 1975 yılları arasında olan “yönetim dönemi”dir. Bu dönemde bilgisayarlar devletin tekeline çıkarak, işletmelerin yönetim faaliyetlerinde de kullanılmaya başlanmıştır. Masuda’nın “toplum aşaması” diye adlandırdığı üçüncü dönem ise bilgisayarların daha yoğunluklu olarak eğitim ve sağlık gibi toplumsal hizmet alanlarında kullanılmasıdır. 1975 yılından beri devam eden bu aşamayla birlikte bilgisayarlar artık, kişisel

²¹² Telematik; bilgisayar entegrasyonu anlamına gelir, geniş ağlar üzerinden veri almak, depolamak ve göndermek için kablolu iletişim ve küresel konumlandırma sistemini ifade eder.
http://bilgi.didikle.com/Telematik_nedir.html, (Erişim Tarihi: 15.01.2013).

²¹³ Haluk Şahin, *Yeni İletişim Ortamı, Demokrasi ve Basın Özgürlüğü*, Anadolu Matbaası, İstanbul, 1991, s.17.

²¹⁴ Adem Ögüt, *a.g.k.*, s.35.

²¹⁵ Hasan Çoban, *Bilgi Toplumu Planlı Geçiş*, İnkılap Yayınevi, Ankara, 1997, s.13.

bilgisayar (*İng; personel computer; PC*) olarak adlandırılmaktadır. Nihayetinde bilgisayarlar devletin ve özel sektörün tekelinden çıkarak halka yayılmıştır.²¹⁶

Bilgisayar teknolojisinin gelişme sürecinde ilk ticari bilgisayar geliştirilene kadar yöneticilerin karar vermesinde kullanılan verilerin elle işlenerek bilgiye dönüştürüldüğü bilinmektedir. Elle işlenen veri miktarındaki artıştan kaynaklanan zorluklar ve yetersizliklerden dolayı veri toplama ve işlemede bilgisayar kullanılmaya başlanmıştır. 1960'larda mevcut bilgisayarlar da yeterli görülmemeye başlanmış ve yeni çalışmalarla bilgisayarların hızı ve gücü arttırılmıştır. Böylece daha çok verinin işlenmesi sağlanmıştır. 1970'li yılların sonlarında bilgisayarları sadece veri aracı olarak değerlendirmek eksiklik olarak görülmeye başlanmış ve bilgisayarlar ile diğer iletişim araçlarının birleşmesiyle ve desteklenmesiyle bilgi ve iletişim teknolojileri ortaya çıkmıştır.²¹⁷

Günümüzde bilgi ve iletişim teknolojileri genelinde gerçekleşen gelişmeler yeterli görülmemekte, sürekli daha gelişmiş istenmektedir. Bu durum insanoğlunun doyumsuzluğunun ve kapitalizmin artı değerini arttırma psikolojisinin bir göstergesi olarak ifade edilebilir. Bilgisayar teknolojisindeki gelişmelerin yanı sıra internet sistemlerinin geliştirilmesi ve bu alandaki hızlı gelişim ve dönüşüm bilgi ve iletişim teknolojilerinin teknolojik çeşitlilik, kullanımın yaygınlaşması ve etkililik özellerinde yüksek performans sağlamasına yol açmıştır. Nitekim internet; veri paylaşımı ve iletişim bağlamında dünya genelinde milyonlarca bilgisayarın fiber - optik kablolar, telekomünikasyon uyduları ve sıradan telefon hatları vasıtasıyla birbiriyle haberleşmesini sağlayan bilgisayar ağından oluşmaktadır.²¹⁸

Günümüzde internetin ekonomiden siyasete, eğitimden sağlığa, toplumsal yaşamın tüm alanlarında kullanılabilir boyutlara ulaşması bilgiyi üretme, paylaşma, saklama ve bilgiye ulaşma konularında onu önemli bir aktör haline getirmiştir. Bilgi ve iletişim teknolojilerinin hızlı gelişim ve dönüşümünde etkili konulardan birisi de bu teknolojilerin birbirinden farklı teknolojileri, yöntemleri ve sistemleri birbirine ekleme imkanı sunarak yeni iletişim biçimlerinin denenmesine olanak sağlamasıdır. Buna bilişim terminolojisinde “*convergence*”²¹⁹ denilmektedir.²²⁰

²¹⁶ Yoneji Masuda, “Managing in the Information Society: Relasing Synergy Japanese Style”, s.114., akt., Cihan Dura, Hayriye Atik , *Bilgi Toplumu, Bilgi Ekonomisi ve Türkiye*, Literatür Yayıncılık, İstanbul. 2002, s.51.

²¹⁷ a.k, s.62.

²¹⁸ Hakan Kara, “İnternet, Gazetecilik ve Yeni Olanaklar”, *Siyahbeyaz*, Der. Serhan Yedig, Haşim Akman, Metis Yayınları, İstanbul, 2002, s.37-42.

²¹⁹ İletişim teknolojilerinin birbirine yaklaşması ve birbiri içine girmesi durumunu ifade eden teknik bir terimdir.

Bilgi ve iletişim teknolojilerinin birbirine eklenenebilir hale gelmesini ifade eden “convergence” kavramı 1990’lı yılların sonlarında ortaya çıkmıştır. Bu kavram GSM (İng; *Global System for Mobile - Küresel Cep Telefonu Sistemi*) teknolojisi dünyasında kendini SMS (İng; *Short Message Service - Kısa Mesaj Servisi*) olarak göstermiştir. Zira SMS ile birlikte sadece ses iletimi değil ses ile birlikte yazı iletimi de sağlanır hale gelmiştir. Yani bilgisayar teknolojisiyle GSM teknolojisi entegre olmuştur. Diğer taraftan internet teknolojisi ile GSM teknolojinin buluşması demek olan WAP (İng; *Wireless Application Protocol - Kablosuz Uygulama Protokolü*) teknolojisi de başka bir örnektir. Özellikle bankacıların ve ekonominin diğer bazı sektörlerinin de WAP teknolojilerine ilgi duyması bu alanda yeni gelişmelerin önünü açmış ve daha hızlı veri transferi için GPRS (İng; *General Packet Radio Service-Paket Anahtarlama Radyo Hizmetleri*) gibi teknolojiler geliştirilmiştir. Bugün artık ses, veri ve görüntü iletişiminin aynı anda yapılması çok kolay ve hızlıdır.²²¹

Günümüzde internet teknolojileri ve GSM teknolojilerinin birbirine eklenmiş olması ve dijital sistemlerin de gelişmesiyle birlikte bilgilerin toplanma ve depolanma yerleri farklı formatlarda birbirine dönüşebilir veya birbirinin yerine kullanılabilir hale gelmiştir. Bu durum gözetim teknolojilerinin de yelpazesini genişletmiş ve işini kolaylaştırmıştır. Nitekim casus cep telefonu dinleme programları sayesinde cep telefonunda geçen konuşmaların istenilen e-posta adresine gönderilebilmesi bunun en somut örneğidir.

Bilgi ve iletişim teknolojilerinin “convergence” özelliğinin yanı sıra “multimedya” özelliğinin geliştirilmesi de bu süreçte ifade edilmesi gereken önemli bir adımdır. Multimedya; yazılı metin, çizgi grafikler, fotoğraf, film ve ses gibi bilgilerin bir araya getirilerek numaralanması ve hacminin küçültülerek kullanıma sunulması işlemidir. Kullanıcının, bir bilgiden diğerine istediği şekilde gitme imkanına sahip olması ile aynı belge üzerinde, sesler, yazılar, resim, animasyon veya videolar ve bilişim programlarının bir arada bulunabilmesi multimedyanın temel özelliklerini oluşturmaktadır.²²²

Bilişim teknolojisi alanındaki hızlı ve etkili gelişmeler doğrudan toplumsal hayatı etkilemektedir. Günümüz toplumsal hayatında giderek bağımlılık haline gelen "bilgi ve iletişim teknolojileri" ekonomide, toplumsal hayatımızda ve kültürümüzde kalıcı ve köklü değişimler meydana getirmiştir. Bilgi ve iletişim teknolojilerinde meydana gelen gelişmelerin ülkelerarası coğrafi sınırları ortadan kaldırarak, dünyayı küresel ticaretin yapılabildiği ortak

²²⁰ Hakan Yıldırım, *a.g.k.*, s.32.

²²¹ *a.k*

²²² Frederic Vasseur, *Geleceğin Medyaları*, Çev. Galip Üstün, İletişim Yayınları, İstanbul, 1993, s.18 - 19.

bir pazar haline dönüştürmesi ile ulusların öz varlık ve öz değerlerinde aşınmalar ortaya çıkmıştır.²²³ Bu bakımdan toplumların değerlerindeki değişimler kültürel varlıklarını da etkileyerek yeni kültürel formların oluşmasına zemin hazırlamıştır.

Bilgi ve iletişim teknolojilerinin varlığının giderek artması ve toplumlarda geniş kitlelere yayılması bu teknolojilerin kendi kültürünü oluşturmaya yol açmıştır. Bu oluşan kültüre dijital kültür denilmektedir. Dijital hayat veya kültür kavramlarının temelinde yer alan “dijital” terimi ses veya görüntüyü; yani datayı bir sayısal dizi formatında kodlayıp, saklayarak iletilmesini sağlayan elektronik sistemler için kullanılmaktadır.²²⁴ Dijital sistemler sahip oldukları özellikleri ifade etmenin yanı sıra sosyal hayatımızı tanımlamak için de kullanılmaya başlanmıştır. Bu durumun altında yatan temel neden bilginin analogdan dijitale dönüşmesi ve fiziki varlıkların sanallaşmasıdır.²²⁵ Bu bakımdan sanal dünya olarak adeta yeni bir yaşam biçimi ortaya çıkmıştır.

Kültürel yaşam toplumsal, ekonomik ve siyasal boyutları olan karmaşık bir yapıdır. Dijital kültür toplumsal ilişkilerin boyutunu farklılaştırmakta ve yönlendirmektedir. Nitekim teknolojik gelişim açısından geline düzeyin, toplumsal ilişkiler açısından da önemli etkileri bulunmaktadır. Bilgi ve iletişim teknolojilerinin yaygınlaşmasıyla insanlar, toplumlar ve kültürler arasındaki yakınlaşma ve tanışıklık artış göstermiştir. Ancak bu yakınlık ve tanışıklık içerisinde gayri samimi ve soğuk bir havayı içermektedir. Zira çok boyutlu olan kültürel ilişkiler sanallaştırılarak basitleştirilmiş, kültür insanların zihninde yer tutan dijital bir veri artığına dönüştürülmüştür.²²⁶

Dijital kültürün oluşma sürecinde bilgi ve iletişim teknolojilerindeki çok hızlı gelişmeler bilgi akışının oldukça hızlanmasına yol açmıştır. Bu bilgi paylaşım sürecinde bireysel olarak her geçen gün birikimler artarken, bütün insanlık da kendini adeta bir bilgi denizinin içinde bulmuştur. Bu bakımdan bilgi birikiminin artması ve anında piyasaya sürülmesinden kaynaklanan yoğunluk nedeniyle bilgi kirliliği olmuş ve doğru bilgiye ulaşma imkanları eskisine göre azalmıştır.

Kültürel yaşamın bir parçası olarak ekonomi de dijitalleşmiş, ekonomiyle ilgili olan her şey internet üzerinden yapılabilir, takip edilebilir hale gelmiştir. Bu da ekonomide sanallaşmayı ifade eden dijital ekonomi, internet ekonomisi veya yeni ekonomi gibi

²²³ Oktay Öksüzler, *a.g.k*, s.389.

²²⁴ <http://www.ekodialog.com>, (Erişim Tarihi: 05.05.2013).

²²⁵ www.elektrotekno.com/about25604.html, (Erişim Tarihi: 18.01.2013).

²²⁶ Mehmet Özçağlayan, *a.g.k*, s.16 - 22.

kavramları, çevreleri ortaya çıkarmıştır.²²⁷ Yeni ekonomi kapsamında bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte özellikle internet teknolojileri ekonomi alanının bütün bölümlerinde kullanılmakta ve giderek toplumun geniş kesimlerine yayılmaktadır. Alım - satım işlemlerinden para aktarmaya, ortak ürün geliştirmeden planlamaya, ihaleden sözleşmeye, ekonomide ne kadar işlem varsa dijital ortamda gerçekleştirmek mümkün hale gelmiştir.²²⁸

Esasında yeni ekonominin kapitalizmin kendisine yeni kapılar açma gayretinin doğal bir sonucu olduğu ifade edilebilir. Artık uluslararası şirketler yerlerini devasa geliri olan internet sitelerine bırakmaya başlamıştır. Yeni ekonomi ile insanlar dünyanın bir ucundaki ülkede bulunan ürünü internet üzerinden sipariş verebilmekte ve çok kısa zamanda kimsenin yüzünü görmeden, kimseyle konuşmadan ürüne sahip olabilmektedir.

Dijital kültürün başka bir etkisi de toplumların köklü alışkanlıklarını değiştirmesidir. Örneğin; elektronik bilgi ve haber kaynakları hayatımıza e-kitap, e-dergi, e-gazete anlayışını sokmuştur.²²⁹ Gazeteler modern toplumun vazgeçilmez sembollerinden birisi olarak şekil değiştirmiştir. Toplumlarda uzun yıllar sonrası oluşan “gazete kültürü” değişim geçirmekte, gazeteleri sanal ortamda okuma alışkanlığı yaygınlaşmaktadır. Bu kapsamda gazete aboneliği yerini sanal gazete aboneliğine bırakmaktadır.

Bilgi ve iletişim teknolojilerindeki gelişim süreci o kadar hızlı ilerlemektedir ki daha insanlar “e-gazete” kültürünü kazanamadan “m-gazete”(mobil gazete) ortaya çıkmıştır. Benzeri durumlar dijitalleşme sürecinin doğal bir parçası olma özelliği taşımaktadır. Bu hızlı değişim süreci bir kültür oluşturacak kadar uzun sürmemektedir. Esasında dijital kültürün, bilgi ve iletişim teknolojilerinin toplumsal kültürü yok ettiği, bireyleri kültürsüzleştirdiği veya bütün ulusları ortak bir kültürel forma mahkum ettiği ifade edilebilir. Nitekim dijitalleşmenin insanların kimliklerini, şahsiyetlerini ve varlıklarını kaybetmesine neden olduğu da aşıkardır. Artık, zamandan ve mekandan bağımsız kimliksiz sanal ilişkiler artmış, insanlar kendilerini bu ortamda bir bilgisayar oyununun figürü olarak görmeye başlamışlardır.

3.2. Yeni Gözetim Sistemleri

Basit gözetleme teknikleri kullanılarak işçilerin gözetimi alanında kendini gösteren modern gözetim günümüzde bilgi ve iletişim teknolojileri ile sosyal çevrede yaşanan gelişim

²²⁷ Hasan Aykın, "Yeni Ekonomide Devletin Yönü: E-Devlet" www.mmd.org.tr/eserler/yeniekonomidedevletin.pdf, (Erişim Tarihi: 18.03.2013).

²²⁸ Adem Ögüt, *a.g.k.*, s.6.

²²⁹ www.epaperflip.com/, (Erişim Tarihi: 18.03.2013).

ve deęişimlerle farklı boyutlar kazanmıştır. Bu dönüşüm süreci gözetim faaliyetlerinin teknik altyapısını deęiştirdiđi gibi gözetimin yaygınlaşmasını ve topluma yayılmasını da sağlamıştır.

Modern gözetim faaliyetlerinde yaşanan dönüşüm esasında insanların yaşam biçimlerinde yaşanan deęişim ile paralellik arz etmektedir. Modernite ile insanlar yaşam çevresi olarak kentleri tercih etmeye başlamış, bu yüzden kent nüfusunda hızlı ve kontrolsüz artışlar meydana gelmiştir. Bu noktada kontrol edilemeyen nüfus hareketliliđi neticesinde suç artışı, gettolaşma gibi birçok farklı sorun ortaya çıkmıştır. Bu sorunlarla mücadele etmek ve kontrolü eline almak isteyen iktidar güçleri çareyi gözetim araçlarında bulmuştur.²³⁰

Gözetim araçlarının kullanılmasıyla bireye ve topluma ait bilgi iktidar güçlerinin eline çok hızlı ve kolay bir şekilde akmaya başlamış, zamanla başkasına ait bilgiye sahip olma arzusu gözetim araçlarını kent yaşamında vazgeçilmez hale getirmiştir. Kentsel yaşamın getirdiđi sorunlar da gözetim faaliyetlerini ve bunlardaki artışı halk ve iktidar güçleri nezdinde meşrulaştırıcı bir zemine oturtmuştur. Sonuçta günümüz kentlerinin her yanı elektronik ağlarla çevrili gözetim evlerine dönüştüđü söylenebilir.

Manuel Castells, *Enformasyon Çađı* isimli eserinde günümüz kentini “enformasyon kenti” olarak ifade etmektedir. Castells’e göre bu kent yaklaşımı bir yer olduđu kadar aynı zamanda bir süreç halini de ifade etmektedir. İnsanlar her ne kadar halen mekanlarda yaşamlarını sürdürseler de işlev ve gücün organize edildiđi yerler akışların alanıdır. Ona göre bu akışlar; elektronik uyarıcılar ve devrelerce mümkün kılınır ve kapital, bilgi, teknoloji, imge ve sembollerden oluşur.²³¹

Akışlar olarak ifade edilen kavrama örnek olarak günümüz sanayi süreci örnek gösterilebilir. Günümüzde üretim çok geniş ve farklı yerlerde gerçekleştirilir hale gelmiştir. Şirketin merkezi Amerika’da iken teknoloji üretimi Çin’de, tasarım merkezi Fransa’da, dağıtım yeri Polonya’da olabilmektedir. Bu durum sanayi sürecinin birbirinden bağlantısız ve rasgele olduđu anlamına gelmemektedir. Aksine telekomünikasyon bağları ve teknoloji sayesinde bu süreç tek merkezden başarılı bir şekilde yürütülebilmekte ve cođrafi yakınlıktan ziyade enformasyon akışlarını kullanarak sağlam bir şekilde bütünleşmiş ve koordine edilebilen bir süreç haline getirilebilmektedir.²³² Benzer bir şekilde tele-bankacılık, tele-alışveriş ve uzaktan eğitim uygulamaları gibi bilgi ve iletişim uygulamaları da eski yer ve

²³⁰ David Lyon, *a.g.k*, 2006, s.101.

²³¹ Manuell Castells, *a.g.k*, 2008, s.286.

²³² *a.k*

zaman biçimlerine olan bağımlılığı azaltmaktadır. Esneklik, hareketlilik ve iletişimin hızı şehrin nasıl düzenlendiği üzerinde büyük bir etkiye sahiptir.

Şehrin doğasında oluşturduğu önemli etki de düşünüldüğünde enformasyon şehirlerinin aynı zamanda gözetleme şehirleri haline geldiği ifade edilse yanlış olmaz. Zira bilgi ve iletişim teknolojileri gözetim faaliyetleriyle iç içe girmiş, birbirine eklemlenmiştir. Şehirdeki akışlar kişilerin yaptıklarının izlenmesini ve takip edilmesini mümkün kılan veri ve bilgileri taşımaktadırlar.

Gözetimin, gerçek hayatta henüz gerçekleşmemiş olaylar ve süreçler üzerine ön veri oluşturmak için kendi kendinin önüne geçtiği söylenebilir.²³³ George Orwell'ın *Bin Dokuz Yüz Seksen Dört* isimli eserinden uyarlanan 1984 tarihinde yayımlanan *Bin Dokuz Yüz Seksen Dört* filminin girişinde ifade edildiği gibi “geçmiş kontrol eden geleceği de kontrol eder; şuanı kontrol eden geçmiş de kontrol eder.”²³⁴ Bu bakımdan iktidarlar tarafından geleceği, şimdiki zamanı ve hatta geçmiş kontrol edilebilme hevesi gözetlemenin değişen konumunu da ortaya koymaktadır. Nitekim bir zamanlar şehirde gözetleme demek, sokak ışıkları ve fiziksel mimari aracılığıyla kontrolü sağlamak ve çarpıklıkları önlemek demek iken, şu anda bunun çok daha ötesinde kamera görüntüleri ve diğer teknolojik gözetleme araçları kullanılarak bütün toplum unsurları hakkında elektronik etiketler tutulabilmesi olmuştur.²³⁵

Bilgi ve iletişim teknolojilerindeki hızla gerçekleşen gelişmeler, gözetim teknik ve teknolojilerinde de birçok yenilik oluşturmuştur. Bu yeniliklerin arka planında yatan iki temel neden vardır. Birincisi, kamu ve özel iktidarların yurttaşlarla ilgili daha çok bilgiyi elde edip onları daha çok kontrol altına alma hırsı iken; ikincisi gözetim teknolojilerinin bir sektör haline dönüşmesidir. Nitekim günümüz itibarıyla gözetim sektörünün dünya çapında yaklaşık 1 trilyon dolarlık bir sektör halini alması da bunu açık bir şekilde açıklamaktadır.²³⁶ Günümüz gözetim dünyasını daha iyi anlamak için bu teknolojileri incelemek gerekmektedir. Bu açıdan bazı yeni gözetim teknik ve teknolojilerinden örnekler verilecektir.

Gözetim faaliyetlerinin dinleme, ilişki çevresi ve yer tespiti ayaklarını oluşturan toplumda yaygın olarak kullanılan, mütemadiyen farklı teknolojik özelliklerle geliştirilen cep telefonları için günümüz gözetim dünyasının asli unsuru denilse yanlış olmaz. Zira

²³³ David Lyon, *a.g.k.*, 2006, s.113 - 114.

²³⁴ Michael Radford, *Bin Dokuz Yüz Seksen Dört*, Film, İngiltere, 10 Ekim 1984.

²³⁵ David Lyon, *a.g.k.*, 2006, s.113 - 114.

²³⁶ Mete Yıldız, R.Erdem Erkul, “*Elektronik Göz ve Türkiye’de Kameralı Hayat*”, www.inet-tr.org.tr, (Erişim Tarihi 15.09.2012).

günümüzde istihbarat birimleri tarafından bir şahısla ilgili yapılacak profillemeye veya risk analizi çalışmalarında ilk bakılan şahsın cep telefonu ve bununla yaptığı görüşmelerdir.

Bir kimsenin cep telefonu açık olduğu müddetçe 150 - 400 metre yanıyla noktasal olarak kişinin nerede olduğunu tespit etmek mümkündür. Bunun kayıp kimselerin veya suçluların izlerini bulma veya şirketlerin motorize personelinin yerlerini tespiti gibi faydalı olarak değerlendirilebilecek uygulama alanları vardır. Ancak bu gibi faydalı kullanımlarının yanı sıra bu teknoloji büyük bir tehlike de oluşturmaktadır.

Cep telefonu ile yer tespiti teknolojisi günümüzde sadece devlet elinde değil, telekomünikasyon şirketleri, hatta sıradan yurttaşın bile ulaşabileceği durumdadır. Nitekim kişinin haberi olmadan telefona yüklenecek izleme programları ile kişinin saat kaçta nerede olduğunu tespit etmek mümkündür.²³⁷ Bu durumda cep telefonu adeta bir takip cihazına dönüşmektedir. Bunların dışında hiçbir cihaza gerek duymadan casus cep telefonu dinleme programları sayesinde telefonu dinlenilmek istenen kişinin yaptığı bütün konuşmalar kaydedilip istenilen elektronik posta adresine gönderilebilmesi de mümkündür.²³⁸

Yeni gözetim teknolojilerine başka bir örnek “*smartcard* sistemleridir”. 1997’de İngiliz Havayolları ve Londra’nın merkezindeki *Victoria* Tren İstasyonu’nda her yolcunun her an nerede olduğunu belirleyen bir *smartcard* sistemi test edilmiş ve takip eden yıllarda bu sistem bütün metro, tren istasyonları ve havaalanlarında kullanılmaya başlanmıştır. Bu sistemde yolcular ücret ödemek yerine sahip oldukları bu kartları *smartcard* okuyucu sistemlerine tanıtmaktadırlar. Böylece yolcular ücretlerini ödemenin yanı sıra günlük hareketlilikleri de veritabanına kaydedilmektedir.²³⁹

Dijital çerezler (*İng; cookies*) de son zamanlarda özellikle internet teknolojilerinde yaygın kullanılan bir gözetim teknolojisidir. Çerezler; bir web sitesi ziyaret edildiğinde, kullanıcının harddiskine gönderilen bilgisayar kodlarıdır. Bir kere harddiske yüklendiği zaman, web site operatörünün siteye nasıl ve ne zaman giriş yapıldığını görmesine izin vermektedir.²⁴⁰ Dijital çerezler, internet sitesi sahiplerinin (büyük oranda ticari firmalar) insanların internette hangi siteleri ziyaret ettiğine dair verileri kaydedebilmesini sağlayan programcıklardır. Bunlar firmaların, reklam amacıyla, kişisel bilgisayarlardan veri toplayarak, kullanıcı hedeflerini belirlemelerine yöneliktir.²⁴¹ Hemen hemen bütün ticari internet site

²³⁷ Nigel Gilbert, *a.g.k*, 2007, s.34.

²³⁸ <http://www.telefondinleme.org/>, (Erişim Tarihi 02.07.2013).

²³⁹ <http://www.economist.com/node/1280806>, (Erişim Tarihi 08.01.2013).

²⁴⁰ David Lyon, *a.g.k*, 2006, s.111.

²⁴¹ *a.k*, s.88.

sahiplerinin bu tür çerezleri rahatlıkla kullanabildikleri göz önünde bulundurulursa, gelişmiş istihbarat teknolojilerine sahip yapılanmaların kişilerin internet hareketlerine yönelik neler yapabileceği tahmin bile edilememektedir.

Gözetim teknolojileri denince akla ilkgelenlerden birisi olan kameralar ve kamera teknolojileri de gözetimin günümüzdeki en gözle görülür yüzüdür. Günümüzde İngiltere başta olmak üzere dünyadaki birçok ülkede alışveriş merkezlerinde, ulaşım araçlarında, asansörlerde, bankalarda, resmi kuruluşlarda, sokaklarda gözetleme amaçlı kameralar her geçen gün artış göstermektedir. Artık kameraların varlığı kanıksanmıştır. Hatta Stephen Graham’a göre ileride bunlar su, gaz, elektrik ve telefon gibi “beşinci bir kamu hizmeti” haline gelecektir.²⁴² Kameralar günümüz gözetiminin simgesi haline gelmiştir. Bu nedenle ayrıntılı olarak tez çalışmasının ikinci bölümünde ele alınacaktır.

Özel hayatın merkezine tam nüfuz edebilme noktasında yeni gözetleme teknolojilerinin en tehlikelileri arasında yer alan ortam dinleme cihazları (böcekler) da giderek yaygın bir şekilde kullanılmaktadır. Bu cihazların küçük olmaları, ses kaliteleri, mekanın tamamındaki sesleri alabilmeleri gibi özellikleri bulunmaktadır. Çalışma mekanizmaları farklı olmakla birlikte genel olarak ortam dinleme cihazları, radyo frekansı üzerinden sinyal göndererek belirli bir mesafeye sesi iletme sistemi üzerine kuruludurlar. Ancak yeni çıkan sistemlerle telefona yüklenen bir program sayesinde GSM hattı üzerinden ortamdaki sesleri sınırsız mesafelere gönderebilmek de mümkün hale gelmiştir. Dolayısıyla GSM hattının çektiği her yerde böceklerle ortam dinlemesi yapılabilmektedir.²⁴³ Günümüzde bu cihazlara internet üzerinden sipariş vererek bile ulaşmak mümkün hale gelmiştir.

Gözetim teknolojilerine adeta yeni bir soluk veren, bireyleri uzaktan kumanda ve takip edilebilir kılan Radyo Frekanslı Tanıma Teknolojisi (*İng; Radio Frequency Identification*) günümüzde yaygın olarak kullanılmaktadır. Bu teknolojinin en önemli özelliği canlı veya cansız her türlü şeyin fiziksel temas olmadan radyo frekanslı çipler vasıtasıyla uzaktan takip edilmesini mümkün kılmasıdır. Örneğin, sahte paraya karşı önlem alınması perdesinde devletler milli paraların üzerine bu çipleri yerleştirmektedirler. Bu çipler kullanılarak kimin üstünde ne kadar para olduğu ve kişinin o anda nerede bulunduğu gibi bilgilerin anında güvenlik birimleri tarafından izlenmesi sağlanabilmektedir.²⁴⁴

²⁴² a.k, s.123.

²⁴³ <http://dinlemecihazlari.com/dinleme-cihazlari/mini-bocek-dinleme-cihazlar.html>, (Erişim Tarihi 08.01.2013).

²⁴⁴ <http://www.medyaplaza.net/03.html>, (Erişim Tarihi 12.01.2013).

Gözetim teknoloji ve tekniklerinin günümüzde akıl almaz boyuta ulaşmasındaki en büyük neden ve kaynak internettir. Gözetim teknolojilerinin mevcut potansiyelini anlamak için interneti incelemekte fayda vardır. Bu nedenle burada öncelikle internetin kavramsal ve teknik boyutu incelenip gözetim teknolojilerine olan etkisi tartışılacaktır. Günümüzde “süper bilgi otobanı”²⁴⁵ olarak görülen internet, kavramsal olarak dünya genelindeki bilgisayar ağlarını ve kurumsal bilgisayar sistemlerini birbirine bağlayan elektronik iletişim ağı olarak ifade edilmektedir.²⁴⁶

İnternetin ortaya çıkışı 1969 yılında çeşitli bilgisayar ve askeri araştırma projelerini desteklemek ve ABD Savunma Bakanlığı’nın *ARPANET* adında paket anahtarlama bir ağ tasarlamasıyla başlamıştır. Böyle bir zeminde başlayan internet, Amerika’da üniversitelerdeki akademisyenlerin çalışmalarıyla giderek gelişmiştir.²⁴⁷ Günümüzde yaygın olarak herkesin kullandığı bir teknoloji ve her gün yenilenen bir bilgi kaynağı haline gelmiştir.

İnternetin sahip olduğu geniş özellikler ve geliştirilebilir - dönüştürülebilir olması, toplumda yaygın olarak kullanılması nedenleriyle gözetim teknolojilerine olan etkisi yadsınamaz derecede büyüktür. İnternet teknolojisiyle birlikte verilerin kolayca toplanması, saklanması, eşlenmesi, pazarlanması ve dolaşımı sağlanmıştır. Gözetim hedefinde toplanan veriler, numaraların ve isimlerin ötesinde DNA kodları veya fotoğraf görüntülerine kadar uzansa da, gözetimin gerçekleşmesini sağlayan esasen internet teknolojisinin gücüdür. Bilgi ve iletişim teknolojilerini gözetimin merkezine yerleştiren etmenlerin başında internet uygulama alanlarındaki gelişmelerin olduğu söylenebilir.²⁴⁸

İnternet tabanlı gözetim, farklı organizasyonlardaki klasik kağıtdokümanlarla yapılan gözetimden çok daha iyi bir şekilde ve kapsamlı, sistematik olarak yapılabilmektedir.²⁴⁹ Uzmanlaşmış kurumlar, rutin olarak kişisel veri toplayan geliştirilmiş araçları daha çok kullanır hale gelmişlerdir. Lyon’un da belirttiği üzere hastaneye gitmek, kütüphaneden kitap almak gibi modern toplum yaşamına katılmak ve bu yaşama ait enstrümanları kullanmak, her yerde iz bırakmak ve interneti kullanmak anlamına gelmektedir.²⁵⁰

²⁴⁵ Gamze Yücesan Özdemir, *İletişim Emek ve Kalkınma: Ekonomi Politik Yaklaşım*, Gazi Üniversitesi İletişim Fakültesi Basımevi, Ankara, 2008, s.15.

²⁴⁶ Merriam Webster's Dictionary and Thesaurus, 2008.

²⁴⁷ Hakan Yıldırım, *a.g.k.*, s.21.

²⁴⁸ David Lyon, *a.g.k.*, 2006, s.13.

²⁴⁹ David Lyon, Christian Holler, “Surveillance Systems Towards an Electronic Panoptical Society?”, 1997. <http://www.heise.de/tp/r4/artikel/8/8026/1.html>, (Erişim Tarihi 08.10.2012).

²⁵⁰ David Lyon, *a.g.k.*, 1997, s.154.

İnternetin gözetim teknolojileri içerisinde başat rolü oynaması, bu teknolojinin diğer gözetim teknolojileri ile uyumlu olabilmesinden kaynaklanmaktadır. Nitekim bir cep telefonuna internet yoluyla kullanıcı farketmeden yüklenen casus yazılım ile yine internet kullanılarak casus dinleme yapılabilmesi, internet kullanılarak güvenlik kamera sistemlerinin kontrol edilebilmesi bunun açık örnekleridir.²⁵¹ Esasında bu durum interneti gözetim araçlarının kapasitesini arttırması açısından büyük bir tehdit unsuru olarak da ortaya koymaktadır.

İnternet, internet teknolojisi tabanlı gözetim sistemlerini oluşturduğu kadar kendisi de başlı başına bir gözetim aracı haline gelmiştir. Örneğin, güncelde kullanılan bir gözetleme aracı olarak “Spypig” adında elektronik posta takip sistemiyle gönderilen elektronik postaların takibi mümkündür. Bu sistem internetten ücretsiz olarak temin edilebilmektedir ve kullanımı için gereken tek şey gönderen ile okuyan tarafların *HTML* desteleyen bir elektronik posta programı kullanmasıdır.²⁵² Elektronik posta takip programları ve yöntemlerinin çok sayıda olması, bunlara ulaşmanın kolay olması ve elektronik posta kullanımının toplumda her geçen gün artış göstermesi²⁵³ elektronik posta üzerindeki gözetim tehlikesini gözler önüne sermektedir.

İnternet, günümüzde kişi veya kurumlarca ulaşılabilir nitelikte insanların özel yaşamlarına ilişkin bilgilerin yer aldığı bir veri deposu haline dönüşmüştür. Nitekim *Facebook*, *Twitter*, *Linkedin*, *Flickr* gibi sosyal paylaşım sitelerine insanlar özel hayatlarına ilişkin adres, kimlik, özgeçmiş, kişisel fotoğraf-video gibi bilgileri yüklemektedirler. Bu durum kişilerle ilgili banka bilgilerine ulaşılmasını kolaylaştırmak suretiyle banka hırsızlığı gibi bireye zarar verici durumların oluşmasına neden olabilmektedir. Diğer taraftan iş başvurusu gibi durumlarda işveren, kişi görüşmeye gelmeden onunla ilgili olarak boş zamanlarını nasıl geçirdiğine, nasıl bir karaktere sahip olduğuna, arkadaş profiline yönelik bilgilere ulaşabilmektedir.²⁵⁴ *Facebook* şirketince 2013 yılının Mart ayında yapılan

²⁵¹ <http://inet-tr.org.tr>, (Erişim Tarihi 12.01.2013).

²⁵² Sistem bir kaç basit adımda kullanılabilir. SpyPig'in size geri dönmesini istediğiniz e-posta adresinizi ve geri dönüş mesajınızı giriyorsunuz. Daha sonra bir SpyPig resmi seçip casus resminizi oluşturuyorsunuz. Bu resmi de kopyalayıp e-posta mesajınıza yapıştırdığınız zaman iletiniz gönderilmeye hazır olmaktadır. <http://www.spypig.com/>, (Erişim Tarihi 08.10.2012).

²⁵³ 2010 yılı Nisan ayı içerisinde Türkiye’de gerçekleştirilen Hanehalkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre internet en çok e-posta amacıyla kullanılmaktadır. Son üç ay içerisinde İnternet kullanan bireylerin %72,8’i e-posta göndermek veya almak, %64,2’i sohbet odalarına, haber gruplarına veya çevrimiçi tartışma forumlarına mesaj göndermek, anlık ileti göndermek, %58,8’i haber, gazete ya da dergi okumak, haber indirmek, %55,7’si mal ve hizmetler hakkında bilgi aramak, %51,2’si oyun, müzik, film, görüntü indirmek ya da oynatmak için interneti kullanmıştır. TUIK, *2010 Yılı Hanehalkı Bilişim Teknolojileri Kullanım Araştırması Sonuçları*, Nisan 2010. www.tuik.gov.tr, (Erişim Tarihi 01.03.2013).

²⁵⁴ Nigel Gilbert, *a.g.k.*, s.24.

açıklamaya göre üye sayısının dünyada 1,11 milyar civarı, *Twitter* şirketince 2013 yılının Temmuz ayında yapılan açıklamaya göre üye sayısının dünyada 554,75 milyon civarı olduğu düşünülürse sosyal medyanın toplumun dijital olarak fişlenmesi için muazzam bir kaynak olduğu görülebilir.²⁵⁵

Yukarıda belirtilen sosyal paylaşım ağlarına ek olarak “*gradfinder.com*” kişinin lise ve bütün yüksekokul mezunlarına ulaşmasına olanak sağlamakta; “*whowhere.com*” da soy arama imkanı tanımaktadır. Hatta evlatlıkların biyolojik ebeveynlerini bulmalarına ya da insanların ünlüleri aramalarına olanak sağlayan siteler de bulunmaktadır. Örneğin; “*www.usa-people-search.com*” internet sitesi incelendiğinde normal bir internet kullanıcısının internet üzerinden arama imkanlarının genişliği anlaşılabılır. Basit dizin taramalarına ek olarak bu site kullanıcılarına aradıkları kişinin sicil geçmişi ve davaları hakkında bilgi vermeden, çalışanların video kamerayla gözlenmesi, hatta emlak bilgilerine ulaşma gibi şeyleri yapabilmelerine kadar olanak sağlamaktadır. Bu ve benzeri dizin taramalarla, şimdiki ve geçmişteki adres bilgileri, kullanılan veya kullanılmış telefon numaraları, akrabalar, ev arkadaşları, aynı adresi paylaşmış olanlar, olası komşular, dava kayıtları, vergi kayıtları ve menkul kıymetlerin yaklaşık değerleri gibi birçok veri türüne ulaşılabilir.²⁵⁶

İnternet gözetiminin yer aldığı başka bir alan da kişilere ait telefon numaralarıyla onlara ait bilgilere internet üzerinden ulaşılabilmesidir. Nitekim casusluk internet siteleri üzerinden veya GSM şirketlerinin internet üzerinde bulunan veri depolarına erişerek kişilere ait telefon numaralarından isimlerine ve adreslerine veya isimlerinden telefon numaralarına ulaşmak mümkün hale gelmiştir. Hatta pazarlamacılar yalnızca sokak adı girerek orada oturan kişilerin isim ve telefon numaraları listesine erişebilmektedir.²⁵⁷

İnternetin gözetim aracı olarak kullanılmasının yanında “internetin gözetimi” de yapılabilmektedir. Nitekim kişilerin ev ve işyeri bilgisayarları için bilgisayar gözetim yazılımı satan birçok şirket bulunmaktadır. “*Spector*” adındaki bir ürün buna örnek olarak gösterilebilir. Üretici firma olan *Spectrosoft*, başlangıç olarak bu programı ebeveynlerin, çocukların pornografik içerikli veya tehlikeli internet sitelerine girmelerini denetlemek için ev versiyonlarını geliştirmiştir. Ancak, daha sonraları hedef kitlesini genişletip, evde çocukların, işyerinde çalışanların, istihbarat birimlerinde hedef kitlenin, suç örgütlerinde çıkar elde etmek için mağdurlarının bilgisayarlarında kullanılabilecek şekilde geliştirilmiştir. *Spector* yazılımı

²⁵⁵ www.statisticbrain.com, (Erişim Tarihi 10.12.2013).

²⁵⁶ Colin J. Bennett, “Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web”, *Ethics and Informaion Technology*, Vol. 3, Issue 3, 2001, s.197 - 205.

²⁵⁷ Brian Martin, *a.g.k*, 1998, s.60.

çevrimiçi çalışabildiği için gözetlenecek kişinin bilgisayarına kaydedilmek zorunda değildir.²⁵⁸

Spector internet programı kişilerin bilgisayarlarındaki her klavye hareketini, ekrandaki bütün görüntüleri düzenli olarak kaydederek programı kullanan kişiye düzenli olarak veri aktarabilmektedir. Bu program kullanılarak birisinin elektronik posta hareketleri, internette girdiği siteler, yaptığı internet yazışmaları, internet bankacılığı bilgileri gibi her türlü bilgiye ulaşarak kişi hakkında bilgi toplanabilmektedir.²⁵⁹

İnternet ve bilgisayar teknolojisi, sadece iktidar ve iktidar organlarının değil, artıkbireylerin de kolay yoldan gözetleme yapabilmelerine olanak sağlamaktadır.²⁶⁰ Bu kapsamda internet teknolojisini kullanan devlet, örgütler ve bireyler, artık insanların gündelik hayatlarına ilişkin verileri çok kolay bir şekilde elde edebilmektedirler. Bu veriler kişilerin özel hayatlarına veya iş faaliyetlerine yönelik olabilmektedir.

3.3. Gözetim Sistemlerinin E-Kapısı: E-Devlet

Bilgi ve iletişim teknolojileri; çalışma, ticaret, ekonomi, üretim faaliyetleri, eğlence, yönetim gibi alanlar başta olmak üzere toplumsal yaşamın her alanında köklü değişim ve dönüşümlere yol açmaktadır. Bu değişim ve dönüşüm süreci devlet unsurlarında ve faaliyetlerinde de yankı bulmuştur. Devlet hizmetlerinde meydana gelen bilgi ve iletişim teknolojileri eksenli değişimi ifade etmek üzere “elektronik devlet” yani “e-devlet” kavramı kullanılmaktadır.²⁶¹ Türkiye Bilişim Derneği’nin 2002 yılında yayımladığı E - Devlet Çalışma Raporu’nda e-devlet kavramı şu şekilde tanımlanmaktadır:²⁶²

“...devletin yurttaşlara karşı yerine getirmekle yükümlü olduğu görev ve hizmetler ile yurttaşların devlete karşı olan görev ve hizmetlerinin karşılıklı olarak elektronik iletişim ve işlem ortamlarında kesintisiz ve güvenli olarak yürütülmesi...”

2003 yılında OECD’nin yayımladığı rapora göre e-devlet, dar anlamda devletin internet tabanlı hizmetlerinin, geniş anlamda da kamu hizmetlerinde bilgi ve iletişim teknolojilerinin kullanılmasını ifade etmektedir.²⁶³ Baştan’a göre e-devlet, kamu hizmetlerinin bilişim teknolojileri temelinde yeniden biçimlendirilmesini ifade eder. Ona göre bu şekilde

²⁵⁸ Colin J. Bennett, *a.g.k.*, 2001, s.197 - 206.

²⁵⁹ *a.k*

²⁶⁰ David Lyon, *a.g.k.*, 1997, s.120 - 121.

²⁶¹ Burak Aydın, “E-Devlet Kapsamında Emniyet ve Diğer Kamu Kurumlarının Bütünleşmesi”, *1.Polis Bilişim Sempozyumu*, EGM Bilgi İşlem Dairesi Başkanlığı Yayınları, Ankara, 2003, s.27.

²⁶² Türkiye Bilişim Derneği, *Türkiye Bilişim Şurası E-Devlet Çalışma Raporu*, 2002.

<http://bilisimsurasi.org.tr/cg/rapor/rapor.zip>, (Erişim Tarihi: 09.02.2013).

²⁶³ OECD, “The E-Government Imperative - Internet”, *Flagship Report*, 2003, s.23.

<http://www1.oecd.org/publications/e-book/4203071E.PDF>, (Erişim Tarihi: 09.02.2013).

bürokratik süreçlerin otomasyona geçişi sağlanarak; yurttaşlar, özel sektör ve devlet organları arasında iletişim becerileri ve faaliyetleri arttırılmaktadır.²⁶⁴

Yıldırım'a göre e-devlet; devletin kamu hizmetlerini daha hızlı ve verimli bir şekilde sunmasını sağlayan teknolojik, elektronik ve telekomünikasyon imkanlarının ve faaliyetlerinin bütünüdür.²⁶⁵ Brown ve Brudney e-devleti, herkes tarafından kamusal bilgi ve hizmetlere kolay ulaşımın sağlanması için etkin bir yapının kurulması amacıyla internet başta olmak üzere bilgi ve iletişim teknolojilerinin kullanımı olarak ifade etmektedirler. Bu çerçevede e-devlet uygulamalarını devletten yurttaşa, devletten devlete ve devletten özel sektöre olmak üzere üçe ayırırlar.²⁶⁶

E-devlet ile oluşturulmak istenen şeyin yeni bir kamu yönetim sistemi olduğu ileri sürülmektedir.²⁶⁷ Bu sistemde devletten yurttaşa, devletten devlete ve devletten özel sektöre olan iletişimin elektronik tabanlı sistemler üzerine kurulması amacı güdülmektedir. Bu durumda kimse devletin gerçek yüzünü göremeyecek, herkes devletin elektronik yüzüne mahkum olacaktır. Her ne kadar başlangıçta e-devletin, iletişim teknolojilerinin sunduğu olanakların kamu hizmetlerinin daha kolay ve basit bir şekilde yerine getirilmesini sağlayacağı varsayımına dayandığı iddia edilse de esasında bilgi ve iletişim teknolojilerini içeren yalın bir kavram olmaktan öte, sosyal ve kurumsal özellikleri olan çok boyutlu bir dönüşüm sürecini ifade ettiği söylenebilir.²⁶⁸

E-devlet kavramı kamu hizmetlerinin bilgi ve iletişim teknolojileri temelinde yeniden şekillendirilmesi ve böylelikle yurttaşlar, ticari kuruluşlar ve kamu kurumları arasındaki iletişim yeteneklerinin geliştirilmesi ile bürokrasinin azaltılarak, elektronik ortama geçişi ifade etmektedir.²⁶⁹ E-devlette esasen “devlet” kavramı işlevsel olarak geleneksel “devlet” kavramıyla aynıdır. Dolayısıyla e-devlet kavramının tamamen de yeni bir devlet kavramına karşılık geldiği söylenemez. Farklı olan şey devletin işlevlerini yerine getirdiği araçlar ve yöntemlerdir. E-devlette işler büyük oranda mikro planda internet, makro planda da bilgi ve

²⁶⁴ Serhat Baştan, Ramazan Gökbunar, “Kamu Hizmetlerinin Sunumunda E-devletle İlgili Yeni Gelişmeler: Tümüleşik E-devlet Sistemlerine Doğru”, *D.E.Ü.İ.B.F.Dergisi*, Cilt 19, Sayı 1, 2004, s.72.

²⁶⁵ Hakan Yıldırım, *a.g.k.*, s.103.

²⁶⁶ Mary M. Brown, Jeffrey L. Brudney, “Achieving Advanced Electronic Government Services: An Examination of Obstacles and Implications from an International Perspective”, 2001, s.1 <http://www.spea.indiana.edu/NPMRC6/Brown&Brudney.doc>, (Erişim Tarihi: 09.08.2013).

²⁶⁷ Nurcan Törenli, “E-Devlet’in Ekonomi-Politigine Giriş”, *Ankara Üniversitesi SBF Dergisi*, Sayı 60-1, s.192.

²⁶⁸ *a.k.*, s.192 - 193.

²⁶⁹ Buğra Gültekin, *Türkiye’de E-Devlet Uygulamaları ve Toplumsal Açılımları*, Gazi Üniversitesi, Ankara, 2007, s.32.

iletiřim teknolojileri araçları ile gerekleřtirilmektedir. Dolayısıyla kamusal hizmetlerin sunuluşunda bir řekil ve yöntem deęiřiklięi söz konusudur.²⁷⁰

E-devlet uygulamalarının avantajları; mevcut kamu hizmetlerinin sunumunun etkinlięinin geliřtirilmesi ve dolayısıyla para, zaman kazancının olması, yurttařların kamusal bilgilere eriřiminin kolay olması ve bu sayede kamu kurumlarının řeffaflıęının artması, kırtasiyecilięin azalması olarak ifade edilebilir.²⁷¹ Burada belirtildięi üzere elbette kamu hizmetlerinin elektronik ortamda sunulmasının saęlamıř olduęu bazı avantajlar vardır. Ancak burada unutulmaması gereken řudur ki elektronik ortama geiřle kamu hizmetlerinin ierięinde deęil, sadece veriliř biiminde deęiřim olmaktadır.²⁷² Bu perspektifte genel hatlarıyla e-devlet uygulamalarının dezavantajları řöyle sıralanabilir. Birincisi, elektronik devlet uygulamalarının temelinde yurttařla ilgili bilgilerin elektronik sistemler üzerinde toplanması, depolanması ve herkesin ulařabileceęi řekilde yayımlanması ihtimali yatmaktadır. Bu durumda yurttařların kiřisel verilerine herkesin ulařabilmesi tehlikesi ortaya çıkmaktadır.²⁷³

İkincisi, e-devlet uygulamalarıyla özel sektör, devlet yakınlařmasının giderek artması ve devletin, yurttařlar hakkında topladıęı bilgileri özel sektörle paylařması tehlikesi bulunmaktadır. Böylece sermaye sahipleri ile devlet, yani bütün iktidar odakları yurttařa ait ne varsa elektronik ortamda bunları toplayarak yurttařa, toplumun her kesimine karřı güç birlięi yapabilecektir.²⁷⁴ Üüncüsü, kamu hizmetlerinin insan gücü yerine bilgisayar teknolojileri tarafından gerekleřmesinin kamuda alıřan sayısını azaltacaęı gereęidir. Bununla birlikte kamu hizmetlerinin internet üzerinden verilmeye bařlanması üzerine yüz yüze hizmet anlayıřı azalacak²⁷⁵ ve bu paralelde uzun vadede yurttař - devlet arasında sanal yakınlařma olacak, gerek hayatta bir yabancılařma söz konusu olacaktır. Her ne kadar bařlangıta yurttařların kamusal bilgilere hızlı ulařmasından dolayı devlet - yurttař yakınlařması olacaęı düşünülse de sokaęa inmeden yurttařları anladıęını söyleyen siyasetiler

²⁷⁰ a.k

²⁷¹ Nurcan Törenli, *a.g.k.*, s.193.

²⁷² a.k

²⁷³ Örneęin; TC kimlik numarası ile kiřinin Baę-Kur Genel Müdürlüęünün web sayfasından Baę-Kur'lu olup olmadıęını da öğrenmek mümkündür. Baę-Kur'lu ise mesleęe kabul tarihi, emekli olup olmadıęı, Baę-Kur'a olan borcu, kaç gün hizmet verdięi, Baę-Kur aylıęını hangi bankanın hangi řubesinden aldıęı, en son maařını hangi tarihte aldıęı, mesleęini hangi ilde icra ettięi, vergi numarası, Baę-Kur saęlık hizmetinden yararlanıp yararlanmadıęı, saęlık priminin kesilip kesilmedięi de ortaya çıkıyor. Elde edilen bilgilerle Gelir İdaresi Başkanlıęının internet sitesinden söz konusu kiřinin evinin bulunduęu cadde, sokak, kapı numarası gibi açık adresine ulařılabilir. Buradaki adres bilgileri kullanılarak ise Türk Telekom'un internet sitesinden kiřinin telefon numarası varsa mail adresi, fatura borcu ve faturanın son ödeme tarihi öğrenilebilir. http://www.cyber-warrior.org/Forum/e-devletin-zararlari_315613,0.cwx, (Eriřim Tarihi: 09.02.2013).

²⁷⁴ Nurcan Törenli, *a.g.k.*, s.201.

²⁷⁵ http://www.teknolojide.com/e-egitim_1087.aspx, (Eriřim Tarihi: 18.09.2012).

gibi zamanla devlet de yurttaşlarını tanımayacak, anlayamayacak hale gelecek, sanal istatistiklerle onları algılamaya çalışacaktır.

Dördüncüsü, kamu hizmetlerinin sunumunu tamamen internet ve elektronik tabanlı sistemler üzerine kuran devletin, siber saldırılar veya sistemsal arızalar nedeniyle veri tabanlarını kaybedebilmesi ve hizmet sunumunda ciddi aksaklıkların meydana gelmesi ihtimali ile devamlı surette karşı karşıya kalabileceği düşünülmektedir.²⁷⁶ Beşincisi; elektronik ortamda sunulacak olan kamu hizmetlerinin toplumda kamu hizmetlerine ulaşma noktasında eşitsizliğe yol açmasıdır. Nitekim ülkede insanlar arasındaki dijital uçurum²⁷⁷ ve internet okuryazarlığının eşitsiz gelişimi nedeniyle herkes internete veya bilgi ve iletişim teknolojilerine rahatlıkla ulaşamamaktadır. Bu durumda toplumun bir kesimi bu hizmetlerden faydalanabilirken diğer başka kesimleri yararlanamayacaktır.²⁷⁸

Sayılan bu dezavantajların yanı sıra e-devlet uygulamaları ile devletin, yurttaşlarının tüm bilgilerini dijital ortamlarda toplaması ve bu sakladığı bilgileri nasıl kullandığı ve başkalarıyla paylaşıp paylaşmadığı konuları muallaktır. Günümüze kadar telefon, faks gibi iletişim araçlarıyla yapılan haberleşmeler de kişisel gizlilik açısından suistimallere uğramış ve bireyler mağdur edilmiştir. Ancak, internet ve bağlı teknolojiler üzerinde toplanan verilerin kapsamı ve işlenmesinin kolaylığı bunlarla kıyaslanamayacak kadar büyüktür.²⁷⁹ Bu noktada bireyin adeta bir veri öznesine dönüştüğü ifade edilebilir. Yurttaşların kendileriyle ilgili verilerin her an devlet görevlileri tarafından suistimal edilerek başkalarına verilebilmesi korkusu içinde yaşaması korku toplumu göstergelerindendir.

²⁷⁶ 21 Ekim 2010 tarihinde, İlaç takibi amacıyla geliştirilen Medula Eczane Sisteminin çökmesi nedeniyle tüm Türkiye çapında ortaya çıkan mağduriyetle ilgili olarak sıradan bir eczacı olan Nurten Saydan'ın şu ifadeleri e-devlet hizmetlerinin ortaya çıkarabileceği zararı açıkça anlatmaktadır: "*Eczacıların mesleğimizi yapabilme hakkı ve vatandaşın ilaca ulaşma hakkı, teknik eksikliklerden ve kurumlar arası anlaşmazlıklardan dolayı engellenmemeli. Sosyal Güvenlik Kurumu'nun uygulamaya başladığından bu yana randımanlı çalışmayan ve buna rağmen, her yeni uygulamada üzerine yeni yazılımların eklenmesiyle daha da ağırlaşan eczane provizyon sistemi üç gündür çalışmayarak, eczanelerimizde büyük bir kaosu yaşanmasına sebep olmuştur. Sistemin neden çalışmadığını sorduğumuzda ise iki kurum da SGK ve İEGM sorunun kaynağı olarak diğerini göstermekte. Sistem arızasının kendilerinden kaynaklanmadığını söylemektedirler. Ancak ortada bir gerçek var ki vatandaş üç gündür ilacına ulaşamıyor.*" <http://sondakika.com/haber-eczane-provizyon-sistemi-nedeniyle-hasta-ve-2331077/>, (Erişim Tarihi: 09.09.2012).

²⁷⁷ Dijital uçurum ise, farklı sosyo-ekonomik düzeydeki bireylerin, firmaların veya ülkelerin bilgi iletişim teknolojilerine erişiminde ve kullanımında yaşadığı eşitsizlik olarak tanımlanmaktadır. "Sayısal Uçurum", "Sayısal Bölünme", "Sayısal Ayrım" ve "Sayısal Kopma" gibi kelimeler bu terimin karşılığı olarak kullanılabilir. Lütfü Öztürk, "Türkiye'de Dijital Eşitsizlik: Tübitak-Bilten Anketleri Üzerine Bir Değerlendirme" *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, Sayı 24, 2005, s.111 - 131. <http://iibf.erciyes.edu.tr/dergi/sayi24/lozturk.pdf>, (Erişim Tarihi: 18.09.2012).

²⁷⁸ <http://msg-itlg.blogspot.com/2008/01/advantagesdisadvantages-of-electronic.html>, (Erişim Tarihi: 18.09.2012)

²⁷⁹ Ersanel Nedret, *Siber İstihbarat*, Asam Yayınları, Ankara, 2001, s.40.

E-devlet beraberinde e-şehir, e-trafik, e-sağlık, e-eğitim, e-tarım, e-demokrasi, e-sosyal güvenlik, e-imza gibi yeni kavramları getirmiştir. Bu kavramlardan özetle bahsedilecektir. E-şehir, şehirle ilgili bilgilerin ve hizmetlerin “şehir internet portalı” kurularak, aktarılması ve yurttaşların su - gaz dağıtım işlemleri, evlendirme işlemleri, ulaşım araçları - saatleri, ölüm işlemleri, fatura ödemeleri, itfaiye hizmetleri, kurs imkanları gibi kamu hizmetlerinden internet üzerinden faydalanmasıdır.²⁸⁰

E-sağlık; kişilerin sağlık öykülerinin, hastalık tedavilerinin, verilen ilaçlarının takibinin ve diğer sağlık işlemlerinin bilgisayar sistemleri üzerinden yapıldığı elektronik sağlık hizmetleri faaliyetlerini ifade etmektedir. E-sosyal güvenlik; internet üzerinden emekli maaşı ve tazminat hesaplama, prim ödeme, işsizlik sigortası işlemleri, sigorta hizmetleri (sağlık, hayat, kaza, deprem, yolculuk vs.), iş ve işçi bulma kurumları hakkında bilgi ve takibat yapabilme gibi sosyal güvenlik işlemlerinin gerçekleştirilebilmesidir.²⁸¹

E-eğitim; eğitimci istediği bir lokasyonda ders verirken öğrencilerin internet ve yüksek teknolojinin sağladığı imkanlardan faydalanarak evlerinden, iş yerlerinden hatta farklı şehirlerden ya da ülkelerden e-eğitime katılarak eğitim kamu hizmetinden faydalanmasıdır.²⁸² Günümüzde e-eğitim ile yüksek lisans dahi yapılabilmektedir. E-imza; elektronik ortamda bulunan bir belgeye eklenerek imzalayanın kim olduğunu belirlemeye yarayan veridir.²⁸³ E-demokrasi, dar anlamda oy verme işlemlerinin internet sistemleri üzerinden gerçekleşmesi iken, geniş anlamda devlet organlarının her türlü konuda internet sistemleri üzerinde kurulacak anket, form, oylamalarla halkın görüşlerini alarak kararlar alması ve uygulamasıdır.²⁸⁴

E-devlet uygulamaları ilk çıkışında yurttaşın kamu hizmetini hızlı ve kolay bir şekilde sunma, bürokratik işlemleri azaltma hedefli olarak gözüksede günümüzde geldiği boyutta artık bir veri toplama aracına dönüşmüştür. Zira yurttaşın bilgilerini toplamak, sınıflandırmak ve depolamak iktidar için oldukça kolay hale gelmiştir. E-devlet hizmetlerinin tek bir mekanizma üzerinden sunulması da birey ile ilgili tüm verilerin tek bir veritabanında toplanabilmesini sağlamıştır. Dolayısıyla iktidar güçleri bu veritabanında yurttaşın kimlik bilgilerini girince onunla ilgili tapu kayıtları, yurtdışı vize başvuruları, dernek - vakıf

²⁸⁰ Hakan Yıldırım, *a.g.k*, s.60 - 62.

²⁸¹ *a.k*

²⁸² http://www.teknolojide.com/e-egitim_1087.aspx, (Erişim Tarihi: 18.07.2013).

²⁸³ Türkiye’de 17.01.2004 tarih ve 5070 sayılı Elektronik İmza Kanunu uyarınca e-imza, ıslak imza ile eşdeğerdedir. E-imza sertifikası dağıtmaya yetkilendirilmiş kuruluşlar tarafından dağıtılan sertifikalar kullanılarak imzalama işlemi yapılabilir.

²⁸⁴ <http://www.e-demokrasi.org/index.php?option=com>, (Erişim Tarihi: 21.07.2013).

faaliyetleri, vergi ödemeleri, noter işlemleri, araç - trafik ceza bilgileri gibi onun devletle ilgili tüm işlemlerini aynı anda tek bir ekranda görebilecektir. Böylece yurttaşın devlet ile olan ilişkisi, faaliyet çevresi, ekonomik gücü çok kısa bir süre içinde ölçülebilecek, sınıflandırılabilir. Bu kapsamda e-devlet yoluyla yurttaşın kendi kendini devletin gözetleme kollarına bıraktığı söylenebilir.

İKİNCİ BÖLÜM

GÖZETİM TOPLUMU VE GÜVENLİK: OLASILIKLAR VE SINIRLILIKLAR

Son yıllarda artan gözetim faaliyetleri “acaba George Orwell’in işaret ettiği gözetim toplumunu mu yaşıyoruz?” sorusunu gündeme getirmiştir. Bu bölümde özellikle bu sorunun yanıtı aranmaya çalışılacak, gözetim toplumu endekslerinin varlığı sorgulanacaktır. ABD’nin gelişmiş gözetim teknolojilerini kullanarak 35 ülkenin liderinin telefonlarını dinleyebilmiş olması²⁸⁵, bir aylık sürede ABD ulusal istihbarat birimi olan NSA tarafından dünyada 124,8 milyar telefonun takip edilmiş olması²⁸⁶, uydular aracılığı ile “Google Streetview” gibi çeşitli programlarla 7 gün 24 saat insanların takip edilebilir olması gözetim toplumu olduğumuz gerçeğini açık ve net olarak ispatlamaktadır.

İktidar güçlerinin gözetim faaliyetlerinden ve bunlardan dolayı giderek özel hayatın alanının daralmasından bireyler belkide bazen gözetleyenler bile rahatsız olmaktadır. Ancak ne zaman böyle bir rahatsızlık olsa akabinde metro istasyonunda patlayan bomba, masum kadınların çantalarını çalan kapkaç failleri, adam öldürme - hırsızlık - cinsel taciz gibi olaylar hatırlanmakta ve sessiz kalınmaktadır. İşte bu noktada gözetleyen ve gözetlenenler nezdinde güvenliğin ortadan kalkması; yani suçun meydana gelmesi ihtimali gözetleme faaliyetlerini meşrulaştırmaktadır. Bu durum da artık gözetim toplumundan geri dönüşün olmayışı ya da suç olduğu müddetçe gözetim toplumunun var olacağı anlamına gelmektedir.

Bireyler can ve mal güvenliklerinin sağlanabilmesi için gözetlenmeye razı olmaktadır. Zira kişi, her yerde her yeri gözetleyen kameralar olursa güvenli bir ortamda yaşayacağını düşünebilmektedir. Bu durum adeta hiçbir mikrop bulaşmaması için kendisini ömür boyu steril bir odada yaşamaya mahkum eden insanın durumuna benzemektedir; yani ömür boyu güvende ama ömür boyu esaret altında olmak. Halbuki bu durum insanın temel özelliklerine terstir. Zira insanoğlu özgür olmak, karşısındakinin esareti altında olmamak için yıllarca savaşmıştır. Özgürlüğü için ölmeyi göze alan varlıkların, bugün özgürlüklerini ölmek ihtimaline karşın feda edebilmesi dikkat çekicidir. İnsanoğlunun yapısı gereği özgürlüğüne

²⁸⁵ <http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>, (Erişim Tarihi: 10.06.2013).

²⁸⁶ Eric Preiffer, “Watchdog”, *Yahoo News*, 23.10.2013. <http://news.yahoo.com/nsa-spied-on-124-8-billion-phone-calls-in-just-one-month-watchdog-group-claims-213633988.html>, (Erişim Tarihi: 28.11.2013).

düşkün olmasının eninde sonunda onun kemikleşen gözetim faaliyetlerine karşı harekete geçeceğinin bir göstergesi olduğu değerlendirilmektedir.

Güvenliğin sağlanması özgürlük alanlarının sınırlandırılmasında hep meşru bir kaynak olagelmıştır. İktidarlar tarih boyunca güvenliği sağlamak için sokağa çıkma yasağı uygulamışlar, insanların evlerinde, arabalarında keyfi aramalar yapmışlar, günlerce insanları gözaltında tutmuşlar, telefonlarını dinlemişlerdir... İşte güvenlik söz konusu olunca hep özgürlük alanına girilmiştir. Dolayısıyla güvenlik ile özgürlük arasında bir çekişme, zıtlık bulunmaktadır. “Güvenlik mi? Özgürlük mü?” sorusu altında birey ezilmiş ve tercihi genelde güvenlik alanında olmuştur. Bu bölümde tercihini güvenlik tarafında yapan bireyin içinde bulunduğu tehlikeli duruma ve gözetim teknolojilerinin özgürlük alanına karşı olan acımasız duruşuna ve gelişimine dikkat çekilmeye çalışılacaktır.

Bu bölümde öncelikle çağımızın bir fenomeni olarak gözetim toplumunun kavramsal boyutu ve bilgi toplumuyla ilişkisi, oluşum süreci ele alınacaktır. Sonrasında gözetim toplumuna evrilmemizde gözetimi meşrulaştıran en temel araç olarak “Güvenlik” olgusu gözetim teknolojisine bakan yönüyle tartışılacaktır. Ayrıca özellikle 11 Eylül 2001 terör saldırılarından sonra değişen güvenlik paradigması paralelinde değişen gözetim paradigmasına açıklık getirilmeye çalışılacaktır. Gary T. Marx’ın ifade ettiği “yüksek güvenli toplumdaki” gözetim toplumundan bir sonraki toplumsal aşama olabileceği tehlikesine dikkat çekilecektir.

Sonrasında güvenlik temelli gözetim denildiğinde ilk akla gelen kameralı gözetim faaliyetleri, bunların güvenlik boyutuyla sağladığı faydalar ile bireyde ve toplumda bıraktığı negatif etkiler çeşitli boyutlarıyla tartışılacaktır. Sonraki kısımlarda Gary T. Marx’ın “yüksek güvenli toplum” distopyasını anlamlılaştıracak değerlendirilen, gözetimin bedenlerin içine inmiş hali olan biometrik gözetime dikkat çekilecektir. Son kısımda da bireylerin gelişen bilgi ve iletişim teknolojilerini kullanmaları neticesinde dijitalleşen kişisel verilerinin güvenliğini sağlamaları; güvenliğini sağlama amaçlı yapılan gözetleme faaliyetleri sonucunda elde edilen kişisel verilerin üçüncü şahıslar tarafından yine gözetim araçları kullanılarak gözetleyenlerin elinden alınması gibi farklı boyutları olan bilişim suçları incelenecektir. Ayrıca bu noktada dijitalleşen kişisel verilerin gizlilik açısından ne kadar büyük bir tehlike altında olduğuna dikkat çekilmeye çalışılacaktır. Gözetim toplumuna dair farklı yönleriyle eleştirel bir analiz yapılacaktır.

I. GÖZETİM TOPLUMU

Bilgi ve iletişim teknolojilerindeki akıl almaz gelişmelerle birlikte topyekun bir değişim, toplumsal dönüşüm süreci içerisine girilmiştir. Bu yeni toplumsal yapıyı Daniel Bell “endüstri sonrası toplum”, Peter F.Drucker “bilgi toplumu”, Zbigniew Brzezinski “teknokratik çağ”, John Naisbitt ve Patrico Aburdane “büyük yönelimler çağı” ve Yonerji Masuda ise “enformasyon toplumu” olarak nitelendirmişlerdir.²⁸⁷ Bunlara ek olarak “bilgi çağı”, “bilişim çağı” ve “küresel köy” gibi tanımlamaların da kullanıldığı bilinmektedir.

“Bilgi toplumu” ve “gözetim toplumu” ilişkisinde, birbirini tamamlayan veya birbirinin yerine de kullanılabilen iç içe geçmiş bir ilişkisellik söz konusudur. Bu sürecin ortak özelliği yeni bir toplumsal yapı, hatta dünya düzeni oluşturulmasıdır. Bu kapsamda bütün bilgi toplumları aynı zamanda gözetim toplumları olmalarına rağmen, bunların gelişim süreci yerel kültürlere, teknolojik gelişimin derecesine, politik önceliklere ve hukuksal düzenlemelere göre değişebilmektedir.²⁸⁸

Gözetim toplumunun bilgi toplumuyla bütünleşmiş bir süreç olması ve bilgi toplumunun altyapısını oluşturan bilgi ve iletişim teknolojilerinin gözetim toplumunun da oluşmasında ve yayılmasında etkili olması nedeniyle “gözetim toplumu”nu incelemeden önce “bilgi toplumu” süreci ele alınacaktır. Bilgi toplumunu arkaplanıyla doğru anlamak için evrildiği sanayi toplumu ile olan ilişkisine bakmak gerekir. Bell’e göre sanayi toplumuyla bilgi toplumunu ifade için kullandığı “sanayi sonrası toplumunun” arasındaki fark kullanılan ve benimsenen teknoloji şeklidir. Sanayi toplumunda temel teknolojik form mekanik teknoloji iken sanayi sonrası toplumda entelektüel teknoloji olmuştur. Entelektüel teknoloji başta bilgisayar olmak üzere bilgi ve iletişim teknolojilerini ifade etmektedir.²⁸⁹

Sanayi toplumunda sermaye ve emek temel öge iken sanayi sonrası toplumda temel öge bilgi olmuştur. Bu bakımdan sanayi sonrası toplumda sınıf yapısı teorik bilgi sahipliğine dayanırken siyasal iktidar da bilginin denetimine bağlı olmuştur. Neticede bilgi ve iletişim teknolojilerine sahip olan, takip eden ve yönetenler bilgiye hakim olanlar olmuştur. Bu sahip oldukları bilgi genişliği de bir anlamda sınıfsal üstünlük aracına dönüşmüştür.²⁹⁰

²⁸⁷ Bahadır Akın, *Yeni Ekonomi: Strateji, Rekabet ve Teknoloji Yönetimi*, Çizgi Kitabevi, Konya, 2001, s.20.

²⁸⁸ David Lyon, *a.g.k*, 2006, s.61 - 63.

²⁸⁹ Daniel Bell, *The Coming of Post-Industrial Society: A venture in Social Forecasting*, Basic Boks, New York, 1973, s.xiii.

²⁹⁰ *a.k*

Bilgi toplumunun temel karakteristiği, sanayi toplumundaki gibi standartlaşmaya ve çalışma hayatındaki belirli rutinlere dayanmamasıdır.²⁹¹ Sanayi sonrası toplum, hizmet sektörü üzerine kuruludur. Artık önemli olan çıplak kas gücüne dayalı enerji değil, bilgidir. Merkezdeki insan, sanayi sonrası toplumun isteklerine cevap verecek şekilde donanımlı, profesyonel insandır. Sanayi toplumu, tüketilen malların miktarıyla ölçülen bir yaşam standardına sahipken, sanayi sonrası toplumda bu, hizmet sektörünün (sağlık, eğitim, sanat vb. gibi) sağladığı olanaklarla ölçülür hale gelmiştir. Sanayi öncesi toplumun doğaya karşı bir oyun olmasına karşılık sanayi toplumu, üretilmiş doğaya karşı bir oyun, sanayi sonrası toplum ise kişiler arasında bir oyundur. Sanayi sonrası toplumda sanayi toplumundaki gibi hiyerarşi ve eşgüdümünden çok, işbirliği ve karşılıklılık esastır.²⁹²

“Bilgi Toplumu” kavramının ilk defa Jonerji Masuda tarafından 1971 yılında yayımlanan *Plan for an Information Society: A National Goal Toward Year 2000* adlı raporda kullanıldığı kabul edilmektedir.²⁹³ Masuda analizlerini Japon milleti üzerinde yapmış ve bilgi toplumunu ifade etmek için *computer* (bilgisayar) ve *utopia* (ütopya) kelimelerinden türetilen “*Computopia*” terimini kullanmıştır.²⁹⁴ Ona göre bilgi ve iletişim teknolojilerinin kullanımı ile ilgili sanayi toplumu sürecinde ortaya çıkan iki sonuç bulunmaktadır. Bunlardan birincisi; bilgi ve iletişim teknolojilerinin devletin birey ve örgütler üzerinde birer kontrol aracı olması; ikincisi ise bilgi toplumuna dönüşümdür.²⁹⁵

Bilgi toplumu, sanayi toplumunda olduğu gibi maddi değerler üzerine değil bilgi değerleri üzerine kuruludur ve ekonomik faaliyetlerde de bilgi önemli bir unsurdur. Sanayi toplumunda maddi refah önemli iken, bilgi toplumunda bireysel bilişsellik ön plana çıkar. Ona göre sanayi toplumunda en yüksek aşama yüksek kitle tüketimi toplumuyken, bilgi toplumunda en yüksek aşama küresel toplumdur.²⁹⁶

Bilgi toplumu ile ilgili yaklaşım sahiplerinden birisi de Manuel Castells’tir. Castells sanayi sonrası süreçte oluşan yeni toplumu “ağ toplumu” olarak kavramsallaştırmaktadır. Ona göre 21. yüzyılda dünyada bir bilgi ve iletişim teknolojisi devrimi olmuştur. Bu devrim “enformasyonizm”dir. Bunun toplumsal yapıdaki karşılığı da “ağ toplumu”dur. Dolayısıyla

²⁹¹ a.k, s.318.

²⁹² a.k, s.127 - 128.

²⁹³ Haluk Geray, “Enformasyon Toplumu ve Türkiye: Erişim Açısından Bir Değerlendirme”, *Yeni Türkiye Dergisi*, Yıl 4, Sayı 20, 1998, s.1416.

²⁹⁴ a.k, s.1416 - 1417.

²⁹⁵ a.k

²⁹⁶ a.k

Castells bu devrimden sonra toplumun bilgi ağlarından oluşmuş sosyal bir yapıya dönüştüğünü iddia etmektedir.²⁹⁷

Yirmi birinci yüzyılda başta batı ülkeleri olmak üzere birçok ülke sanayi toplumundan bilgi toplumuna geçişi bir gaye olarak benimsemiş ve bu kapsamda çeşitli eylem planları hazırlamıştır. Örneğin Avrupa Birliği üyesi ülkeler kapsamında bilgi toplumuna geçiş ile ilgili e-Avrupa eylem planları hazırlanarak yürürlüğe konulmuştur. Bu kapsamda internet kullanımı ve internete erişiminin yaygınlaştırılması, ticari işlemlerin e-ticaret başlığı altında internet ortamına kaydırılması, e-iş, e-sağlık, e-devlet gibi birçok yeni alanların açılarak bunların geliştirilmesi ve bu alanlara katılımın sağlanması, bilgi toplumu müktesebatı oluşturulması gibi adımlar atılmıştır.²⁹⁸

Bilgi toplumu sahip olduğu arka plan, temel dinamikler, araçlar ve sonuçlar bakımından gözetim toplumunun teknolojik altyapısını hazırlamıştır. Bu noktada kavramsal olarak gözetim toplumu kişi veya grupların faaliyetlerinin yönetim birimleri tarafından bilgi ve iletişim teknolojileri ve gözetim teknikleri kullanılarak izlenildiği, kaydedildiği topluma verilen addır.²⁹⁹

İlk defa “gözetim toplumu” ifadesi 1949 yılında George Orwell’ın *Bin Dokuz Yüz Seksen Dört* kitabında tasvir edilmiş ve 1985 yılında Gary T. Marx tarafından kavramsal olarak kullanılmıştır.³⁰⁰ Gary T. Marx’a göre gözetim toplumu, bilgisayar teknolojisiyle, bütünsel denetimin önündeki engellerin yıkıldığı bir durumu ifade etmektedir. Yeni teknolojiler, gözetim potansiyelini sürekli artırmaktadır. Ona göre içinde yaşadığımız gözetim toplumunda artık herkesin gizliliği tehdit altındadır.³⁰¹

Gözetim toplumu; gözetim temelli teknikler kullanarak örgütlenen toplum olduğu için gözetim altında olmak da kişinin hareketlerinin ve faaliyetlerinin toplumu oluşturan örgütler ve yönetim birimleri adına teknoloji kullanarak kayıt edilmesi demektir. Gözetim faaliyetlerinin doğasında kayıt altına alınan bu veriler incelenerek kategorilere ayrılır ve bireylerin yaşamlarını etkileyecek birçok kararın alınmasında kullanılır.³⁰²

²⁹⁷ Manuel Castells, *a.g.k*, 2008, s.114.

²⁹⁸ Avrupa Birliği, *2003 E-Avrupa Eylem Planı*, Haziran 2001, s.3.

http://www.bilgitoplu.gov.tr/Documents/3/Diger/010600_eAvrupa+EylemPlani.pdf, (Erişim Tarihi 15.09.2012).

²⁹⁹ www.inet-tr.org.tr/inetconf11/bildiri/97.pdf, (Erişim Tarihi 08.05.2013).

³⁰⁰ David Murakami Wood, *a.g.k*, s.5.

³⁰¹ Veysel Bozkurt, *a.g.k*, s.3.

³⁰² www.inet-tr.org.tr/inetconf11/bildiri/97.pdf, (Erişim Tarihi 08.05.2013).

David Lyon gözetim toplumunu oldukça geniş yorumlayarak yönetilme ve kontrol işlevleri için iletişim ve bilgilendirme teknolojilerine bağımlı olan bütün toplumları gözetim toplumları olarak ifade etmiştir.³⁰³ Lyon'un bu tanımına göre günümüzde bütün toplumların gözetim toplumu olduğu söylenebilir.

Toplumsal hayatta kişisel verilerin depolandığı kamusal ve özel geniş veri tabanlarının oluşturulması ve veri toplama araçlarının; yani gözetim araçlarının artış göstermesi gözetim toplumunun en önemli göstergelerindendir. Gündelik yaşam sürecinde bireylerin telefon görüşmeleri, e-posta trafikleri, internet kullanım bilgileri düzenli olarak kamu veya özel şirketler tarafından toplanıyorsa; DNA, parmak izi, avuç izi gibi bireyin öz vücuduna dair biometrik tanımlayıcı veriler sistematik olarak depolanabiliyorsa; bazı özel şirketler tüm ülkede yaşayan bireylerin kimlik ve adres bilgilerini belli bir ücret karşılığında satabiliyorsa; bireyler kafasını yukarı doğru kaldırdığında mutlaka kameralar ile karşılaşlıyorsa, “Google Streetview” gibi özel sektör girişimleri gözetim olanaklarını herkese sunabiliyorsa bu toplum gözetim toplumu kavramı haricinde ancak belki “süper gözetim toplumu” olarak ifade edilebilir.³⁰⁴

Gözetim toplumunun oluşumu ve yayılması bu sayılan ve benzeri birçok dönüşüm odaklı gelişmelerin varlığıyla birlikte insanoğlunun varlığından beri olan tekniklerin yeni yöntemlerle genişletilmesine ve geliştirilmesine dayanmaktadır. Gözetim toplumunun oluşmasıyla ilgili olarak sayısal bir sınır belirginliği yoktur. Yani güncelde ulus toplumların gözetim toplumu olmasıyla ilgili olarak net bir ayırım yapılamaz.³⁰⁵ Zira artık gözetleme karmaşıklaşmış ve bulanık hale gelmiş, küresel nitelik kazanmıştır. Dolayısıyla belki de günümüzde gözetim toplumu evren değiştirerek “gözetim dünyası” haline gelmiştir. Fakat ister gözetim toplumu ister gözetim dünyası olarak nitelendirilsin fark etmez, günümüzde bedenlerin gözden kaybolması süreci gözetim toplumu veya dünyasının bir sonucu ve aynı zamanda da bir sebebidir. Bu noktada Lyon, bedenlerin kaybolması durumunu şöyle açıklamaktadır:³⁰⁶

“...hayatların sürat ve hareket tarafından domine edildiği bir dünyada yaşandıkça daha göze çarpar bir hal alır. Hızlı bir dünya, uygunluk ve katılım haklarının gösterilmesi için güven işaretlerinin gittikçe artan sayıda yöntemlerle sunulduğu bir dünyadır. Sürekli büyüyen görünmez bir yapı (enformasyon altyapısı) her yeni gözetleme işlevinin başlayabileceği bir platform oluşturmaktadır; ancak bu aynı zamanda bir zamanlar birbirinden daha ayrı olan sektörler arasında daha serbest bir veri akışının da

³⁰³ David Lyon, *a.g.k.*, 2006, s.11.

³⁰⁴ Timothy Pitt Payne, “The Surveillance Society In And Out of The Workplace”, June 2009, s.1. www.11kbw.com/articles/docs/SurveillancesocietyTPP.pdf, (Erişim Tarihi: 11.06.2013).

³⁰⁵ David Lyon, *a.g.k.*, 2006, s.98.

³⁰⁶ *a.k*

aracıdır. Hızlanan akışlar, risk hesaplanmasını ve buna bağlı, bizim davranışlarımızın değerlendirilmesinde kullanılan kategorilerin artan güçlerini yansıtmaktadır.”

Bedenlerin kaybolarak enformasyonel birer veri niteliği kazandığı dünyamızda Lyon, gözetim toplumunu “Disneyland”, gözetlemeyi de “Disneyleştirme” olarak ifade etmiştir.³⁰⁷ Disneyland, oyun ve eğlence köyüdür, mekansal sınırları belirlidir ve insanlar bu sınırlar içerisinde çılgınca eğlenirler. Bu esnada güvenlik gerekçesi ile sürekli olarak tanımadıkları gözler tarafından gözetlenmektedirler. Gözetlendiklerini bilirler; fakat eğlenceye daldıklarından bunun farkında değildirler, bu duruma tepki göstermezler.³⁰⁸

Günümüz toplumunun da bu şekilde bir Disneyland haline dönüştüğü iddia edilebilir. Yalnız burada küçük bir köy değil, küresel bir köy vardır. Küreselleşmenin giderek yayıldığı günümüzde dünya uydular, gelişmiş bilgi ve iletişim teknolojileri vasıtasıyla sürekli kontrol altında tutulmaktadır. Ülkeler arasında gözetleme çevresi ve teknikleri ile kapasite açısından bir takım farklılıklar olsa da her an her yerde bir takım bilinmedik gözlerle bireylerin hareketlerinin izlendiği de bir gerçektir.³⁰⁹ Artık gözetleme aralıksız olarak tecrübe edilmektedir. Sabahki ilk telefon aramasından, kafanızın üzerinde sokakta duran kameraya, bankamatikteki retina tarayıcısına, bilgisayardaki iz sürme çerezine, ofis anahtarındaki barkoda, otomatikleştirilmiş otoban ücretine, cep telefonu bağlantılarına, dükkandaki kameraya, metro istasyonuna ve gecenin sonu olan bara kadar...

Bilgi toplumunun dünyada yayılması ve bununla birlikte bilgi ve iletişim teknolojilerinin kullanım genişliği gözetim toplumunun oluşmasına ve dünyaya yayılmasına ivme kazandırmış, gözetim toplumunun küreselleşmesi sürecini oluşturmuştur. Nitekim kamera sistemleri, şifreleme teknikleri ve biometrik gözetleme tekniklerindeki gelişmelerin yaygınlaşması gözetlemenin küreselleşmesine kuvvetle işaret etmektedir. Bilgi altyapıları ve veri tabanlı ekonomilerin kurulduğu her yerde gözetleme uygulamaları hızla artan bir oranda büyümektedir.³¹⁰

Günümüz teknolojik gelişmeleri çerçevesinde gözetim toplumunun boyutlarını net olarak kestirmek mümkün gözükmemektedir. Ancak gözetim toplumu olma sürecinde dünyada başat rol oynayan İngiltere’deki güncel aktiviteler ve gelişmeler incelenirse bu sürecin nasıl yol aldığı noktasında çıkarımlarda bulunulabilir. İngiltere’de gözetim her geçen gün giderek artış göstermektedir. Bugün bu ülkede her on dört kişiye bir kamera düşmektedir. Alışveriş merkezlerindeki müşterilerin hareket profilleri gelişmiş kameraları ile analiz

³⁰⁷ a.k, s.38 - 41.

³⁰⁸ a.k

³⁰⁹ a.k

³¹⁰ a.k, s.17 - 18.

edilmekte, ebeveynler okul veya kreşteki çocuklarının tüm faaliyetlerini internetten takip etmekte, işe alım işlemlerinde yapılan biyolojik gözetleme faaliyetleri kapsamında işe başvuran kişinin hastalık yatkınlığı, çalışkanlığı gibi değerlendirmeler yapılmakta, her yerde olan kameralarla bireylerin günlük faaliyetlerinin fişlendiği bilinmektedir. Yakın zamanda da İngiltere’de yaşayan her yabancıya konum belirleyici çipler takılacağına yönelik de haberler bulunmaktadır.³¹¹ İngiltere’deki bu gözetim faaliyetlerinin ve teknolojilerinin diğer gelişmiş ülkelerce de örnek alınması gözetim toplumunun uluslararası niteliğe kavuştuğunun bir göstergesi olduğu söylenebilir.

“Gözetim Çalışmaları Grubu” olarak adlandırılan bir grup akademisyenden oluşan Londra Bilgi Komisyonu Ofisi tarafından düzenlenen 28. Uluslararası Veri Koruma Komisyonları Konferansı’nda sunulan gözetim toplumu raporunda İngiltere’nin diğer Batı ülkeleri içinde en çok gözetimin yapıldığı ülke olduğu; kapalı devre kamera sistemlerinin giderek artış gösterirken veri güvenliği ve özel alanla ilgili olarak gerekli adımların atılmadığı tespitlerinde bulunulmuştur.³¹² İngiltere örneğinde olduğu üzere gözetim toplumlarının önemli bir özelliği de iktidarların ellerindeki gözetim gücünü kaybetmemek veya zedeletmemek için gözetimin aleyhine fakat yurttaşların lehine olan konuların sorunsallaştırılmaması, kanunlar çıkarılırken gözetleyenler tarafının hep kazanmasıdır.

Gözetim ve bilgi teknolojilerinin ortaya çıkış çevresinin kapitalist tabanlı olduğu göz önünde bulundurulursa gözetleme faaliyetlerinin gözetim toplumuna evrilmesi sürecini çalışma yaşamındaki gözetleme ve denetleme faaliyetlerinin yaygınlaşmasının tetiklediği iddia edilebilir. Bu açıdan burada, gözetim toplumu için önemli olduğu düşünülen “çalışma yaşamında gözetimi” tartışmak isabetli olacaktır.

Çalışma yaşamında uygulanan gözetim, toplumun diğer alanlarından daha fazla ve belkide daha görünür kılınarak yapılmıştır. Gandy’e göre, çalışma yaşamındaki gözetim, toplumun diğer sektörlerindeki gözetimden en az üç sebepten dolayı daha yaygındır. Birincisi, bilgi toplumunda, bilgi teknolojileri mevcut ekonomik sistem tarafından zirveye çıkarılmıştır ve işyerleri, gözetim potansiyeli olan bilgi ve iletişim teknolojileri için hazır durumdadır. Bu nedenle de gözetim teknolojileri işyerlerinde daha hızlı yayılma imkanı bulmuştur. İkincisi, gözetim maliyetleri açısından işyerleri diğer toplumsal konumlara göre daha uygun ve hesaplıdır. Üçüncüsü, işverenlerin çalışanları için çalışma şartlarını belirleme ve bu şartlara uyum sağlamayanları işten atabilme gibi hareket serbestileri bulunmaktadır. Bu çalışma

³¹¹ http://news.bbc.co.uk/2/hi/uk_news/6108496.stm, (Erişim Tarihi: 08.08.2013).

³¹² a.k

şartları serbestisi işverenlerin gözetim faaliyetlerinde bulunmaları için yasal serbestlik ve mazeret imkanı sağlamaktadır.³¹³

Bilgi ve iletişim teknolojilerindeki gelişmeler çalışma yaşamındaki gözetimin de evrenini değiştirmiştir. Bu bakımdan Rule, çalışanlara yönelik gerçekleştirilen bilgisayar teknolojili gözetim şeklinin, geleneksel gözetim şeklinden bazı farklılıkları olduğuna dikkat çeker. Bu farklılıklar ona göre geleneksel izleme yönteminden daha sıkı takip ve denetim yapılabilmesi, çalışanlara işlerini yaparken daha az müdahale edilmesi ve gözetleme faaliyetleri için insan gücü minimuma indirildiği için uzun vadeli maliyetinin daha az olmasıdır.³¹⁴

Eski zamanlarda çalışma yaşamında gözetim, sadece patronun kendisinin gözetim yapması ilkel sayım aletleriyle sınırlıyken günümüzde bilgi ve iletişim teknolojilerinin etkisiyle farklı teknik ve araçlarla desteklenir hale gelmiştir. Nitekim artık çalışma yaşamındaki gözetim patronun işçinin elektronik postasını okumasından, markette barkot okuyucuların çalışanın barkottan okutturma hızını ölçmeye kadar çeşitlenmiştir. Bu çeşitliliğin yanı sıra sistematik, daha az maliyetli ve daha kolay gözetim yapılır hale gelmiştir. Bu değişimin altında yatan temel neden sadece gözetim teknolojilerindeki akıl almaz gelişim değil, aynı zamanda kişisel gizlilik alanına giren konuların da bu teknolojilerle işverenler tarafından kontrol edilebilir, izlenebilir hale dönüşmüş olmasıdır.³¹⁵

İş yerinde gözetim faaliyetleri daha kişi işe girmeden önceki sürece kadar uzatılabilmektedir. Kişi hakkında daha iş başvurusu yaptığında kendisine uygulanan uyuşturucu testleri, psikolojik tarama uygulamaları, kredi kartı incelemeleri, sabıka kaydı

³¹³ Oscar Gandy, “The Surveillance Society: Information Technology and Bureaucratic Social Control”, *Journal of Communication*, Vol 39, Issue 3, 1989, s.67.

³¹⁴ James B. Rule, “High-Tech Workplace Surveillance: What’s Really New?”, *Surveillance, Computers, Privacy*, Ed. David Lyon, *a.g.k.*, 2001, s.71 - 73.

³¹⁵ Çalışma yaşamındaki gözetleme faaliyetlerinin ulaştığı boyutlarının tehlikesinin farkına varma noktasında Amerika’da geçen aşağıdaki olayların katkıda bulunabileceği düşünülmektedir: “Consolidated Freightways çalışanları tuvaletlerdeki gizli kameraları fark ettiklerinde dehşete kapılmışlardı – bazı kameralar doğrudan pisuvarlara bakmaktaydı. Binlerce çalışan için bin saatin üzerinde video kaydı vardı. Gizli kameraları bulan liman işçisi Joe Quilty, erkeklerin sarsıldığını ve bazı kadınların ağlayarak evlerine gittiğini söyledi.”, “Apalachicola Times”ın genel yönetmeni çalışanların banyolarına gizli kamera kurdu ve kaydetmeye değer 29 video yaptı. Görüntüleri kaydedilen birçok kadından biri olan Lynn Perry hiç kimsenin gözetim için kendisinden izin almadığını söyledi. Resmi ya da gayri resmi olarak hiç kimse Perry’nin iznini almamıştı ve banyoda bir kamera olduğundan habersizdi.”, “New York Woodside’da bir yangın söndürme tesisatı firmasının başkanı olan Howard Boyle çalışanlarına cep telefonu hediye etti, ama cihazlardaki GPS hakkında bilgi vermedi. Böylece Boyle elemanlarının ne zaman çalışıp ne zaman dinlenme arası verdiğini takip edebilecekti. Böyle, çalışanlarının bunu bilmesine gerek olmadığını söyledi. ‘Önümdeki monitörden nerede bulunduklarına bakıp, telefon açıp nerede olduklarını sorabilirim’ dedi.” National Workrights Institute, “Privacy Under Siege: Electronic Monitoring in the Workplace”, <http://www.workrights.org>, (Erişim Tarihi 03.03.2013).

araştırması gibi çeşitli gözetim işlemleri gerçekleştirilmektedir.³¹⁶ İşverenler özel veri depoları ve genetik eleme metotları ile diğer gözetleme teknolojileri sayesinde işçiyi işe almadan önce, kişinin sorumlu ve çalışkan bir işçi olup olamayacağı ihtimallerine göre yargılama yapabilmektedirler. Bu süreçte işveren “sadece çalışmak isteyen kişinin” bütün özel hayatına ait bilgileri görebilmektedir. Diğer taraftan biometrik gözetim araçları vasıtasıyla da gelecekte çalışması muhtemel olan işçiler, gerçekten ne başardıkları ya da işteki kanıtlanmış performansları yerine, erken uyarı işaretlerine eğilim ve isteklerine göre kontrol edileceklerdir. Bundan ötürü, hamile olabilecek ya da bazı hastalıklara yatkın olan işçiler işe alınmayabileceği değerlendirilmektedir.³¹⁷

Çalışma yaşamında gözetim uygulamada farklı şekillerde gerçekleştirilebilmektedir. Bunlardan bazıları şu şekilde ifade edilebilir. İşverenlerin çalışanlarının elektronik postalarının alıcısının kim olduğu, çalışanlarının elektronik postayı okumak için harcadığı zamanı, elektronik postanın göndericisinin kim olduğunu, elektronik postanın işle bağlantılı olup olmadığını öğrenmek için elektronik postalarını okuması ve takip etmesi³¹⁸; çalışanların bağlantılarını ve ilgi alanlarını tespit etmek amacıyla işyerindeki bilgisayar üzerinden girdikleri internet sitelerini takip etmek; çalışanların hareketlerini ve iş faaliyetlerini kamera sistemleriyle takip etmek; çalışanların telefonlarını ortak telefon ağı vasıtasıyla dinlemek; aktif manyetik kimlik kartları aracılığıyla çalışanların fabrikada nerede olduklarını, işe kaçta gelip, gittiklerini, tuvalete hangi saatlerde gittiklerini gözetlemek.³¹⁹

Gözetim teknolojileri ile çalışma yaşamında yapılan gözetleme faaliyetleri genel anlamda yukarıda sayılanlar şeklindeyken bunların içinde en yaygın olarak kullanılanı “gözetim kameraları”dır. Bu kameralar işyerinde arkasında kimin izlediği bilinmezliğinde çalışanların iş performanslarını takip eder ve kapitalizmin maksimum kar elde etme prensibi paralelinde çalışanları daha çok çalışmaya yöneltir ve adeta çalışanlar için bir baskı aracı haline gelir.³²⁰

Bazı bilim adamlarına göre çalışma yaşamındaki gözetim faaliyetleri olumsuzlanabilir. Örneğin Cozetto ve Pedelinski, çalışanların üzerinde tehdit edici bir durum ya da taciz durumu söz konusu olduğunda, gözetimin gerekli olduğunu savunmaktadırlar. İşverenler

³¹⁶ Oscar Gandy, *a.g.k.*, 1989, s.67.

³¹⁷ *a.k.*, s.81,82,83.

³¹⁸ Ali Osman Özdilek, “Hizmet Akitlerinde Gizlilik Maddesinin Bilisim Teknolojileri Kullanımı Açısından Değerlendirilmesi”, <http://www.hukukcu.com/bilimsel/kitaplar/hizmetakitlerivebilisim.html>, (Erişim Tarihi 03.03.2013).

³¹⁹ David Lyon, *a.g.k.*, 2006, s.83.

³²⁰ *a.k.*, s.121 - 122.

onlara göre, çalışanların diğer çalışanlar üzerinde ırkçı, cinsiyetçi, tacizci ya da küfre yönelik davranışlarını engellemek ya da bu davranışlara karşı koymak için gözetim uygular. Onlara göre gözetim bu anlamda sadece işverenlerin değil, diğer çalışanların da koruyucu bir çadırı haline gelmiştir.³²¹

Rule'a göre ise çalışma yaşamında yapılan denetleme faaliyetlerinin amacı çalışanları gözetlemekten ziyade iş takibi ve iş akışını düzenlemektir. Yani asıl amaç, çalışanın kişisel bilgilerinin gözetlenmesi değil, işin sürekliliğinin ve verimliliğinin sağlanmasıdır.³²² Lee ve Kleiner'a göre düzenli gözetim endüstriyel casusluğu azaltacaktır. Buna göre gözetleme faaliyeti varlığını çalışanlar üzerinde sürekli hissettireceği için, çalışanlar yasa dışı faaliyetlerde bulunma teşebbüsünde bulunmaktan kaçınacaklardır. Ona göre işyerindeki sistematik gözetimin sağladığı bu caydırıcılık aynı zamanda işverenlerin lehine olarak onları da koruma altına alacaktır.³²³

II. GÖZETİME MAHKUMİYET SEBEBİ: GÜVENLİK

Gözetleme faaliyetleri genel olarak güvensizlik, korku, merak, cinsel sapkınlık, kar güdüsü, sömürü, ticari kaygı gibi nedenlerle yapılmaktadır.³²⁴ Bu nedenler genel anlamda doğru olsa da esasen bunların içerisinde güvenlik kaygısı büyük yer tutmaktadır. Bu bölümde gözetleme ve gözetim teknolojilerinin yaygınlaşmasında başat rol oynayan güvenlik kaygısı ele alınacaktır. Güvenlik temelli gözetleme, ortaya çıkışı - sağladığı avantaj ve zararlar ile toplumsal yaşamda vuku bulma şekli açısından değerlendirilecektir.

Gözetim teknolojilerinin gelişim seyrine dikkat edilirse, yeni gözetim teknolojileri çoğunlukla güvenliği temin etmek üzere ortaya çıkmış ve buradan özel sektöre, bireysel kullanıma doğru seyir izlemiştir. Örneğin, kameraların kullanımı ilk olarak kamu binalarının korunması ve askeri amaçla ortaya çıkmışsa da günümüzde toplumun diğer kesimlerinde de oldukça yaygınlaşmıştır. Günümüzde bir anne kreşe bıraktığı çocuğunu internet üzerinden izleyebilmekte, şirket sahipleri şirket çalışanlarını sürekli kameralar kullanarak gözetleyebilmektedir.

Lyon, bireylerin güvenliklerinin sağlanması uğruna özel yaşamlarının gizliliğinden ve mahremiyetlerinden vazgeçerek böylesine yüksek bir bedel ödemeye razı olduklarını ifade

³²¹ Don A. Cozetto, Theodore B. Pedeliski, "Privacy and the Workplace: Technology and Public Employment", *Public Personnel Management*, Vol 26, Issue 4, 1997, s.518 - 519.

³²² James B. Rule, *a.g.k.*, s.71 - 73.

³²³ Samantha Lee, Brian H. Kleiner, "Electronic Surveillance in the Workplace", *Management Research News*, Volume 26, Issue 2-3-4, 2003, s.74.

³²⁴ Julie K. Petersen, *a.g.k.*, s.11.

etmektedir.³²⁵ Petersen’a göre ise insanlar ne zaman can ve mallarına yönelik korku içerisine girseler özgürlüklerinden vazgeçmekte o kadar kabul edici olurlar. Örneğin, çoğu insan kamuya açık lavabolarda kameraların olmasına izin vermez iken, bu insanlar havaalanlarındaki, süpermarketlerdeki lavabolarda birkaç saldırı veya buralarda çocuk kaçırma vakaları olmaya başladığında lavabolarda kamera gözetiminin olmasını savunur hale gelebilirler.³²⁶

Eğer her şey görülür kılınırsa, terörizm gibi her türlü tehlikenin ve riskin daha oluşmadan tespit edilebileceği ve hemen yok edilebileceği iddia edilmektedir. Bu durumu Ball ve Webster “Toplam Bilgi Farkındalığı” (*Ing; Total Information Awareness*) olarak ifade etmektedir.³²⁷ Bu durum aslında devletin güvenlik tabanlı gözetleme hırsının sınır tanımayacağını da açıkça ortaya koymaktadır. Güvenlik güçleri “Toplam Bilgi Farkındalığı” seviyesini sürekli arttırmak için yeni gözetim teknolojileri arayışı içinde olacaklar ve bu teknolojileri ülkedeki bütün insanları izleyebilecek şekilde konumlandırmanın yollarını arayacaklardır. Bu da gözetim toplumu distopyasının ne kadar yakın olduğunun açık bir göstergesidir. Zira artık modern devlette suç her an, her yerde işlenebilir bir nitelik taşımaktadır. Bu da suçu önleme amaçlı gözetim teknolojilerinin her an her yerde uygulanabilir olmasını gerektirmektedir.

Güvenlik tabanlı gözetim teknolojilerinin kullanım alanları; yolcular ve bagajlar için kablosuz iletişim cihazlarının takibi, kontrol noktası detaylı araması, biometrik gözetimi içeren taşıma ve ulaşım güvenliği gözetim faaliyetleri, ülke sınırı güvenliği için gözetim faaliyetleri, teröristlerin konvansiyonel ve biyolojik silahlara ulaşımının engellenmesi güvenlik gözetimi, teröristler ve dolandırıcılar ile mücadele stratejileri kapsamında güvenlik gözetimi, özel güvenlik personelinin geçmişi için yapılan araştırma faaliyetleri, insan kaçakçılığı ve uyuşturucu kaçakçılığı faaliyetleri için yapılan gözetim faaliyetleri, toplumsal düzenin korunması için hırsızlık ve adam öldürme gibi asayiş suçları ile mücadele kapsamında yapılan gözetleme faaliyetleri, toplumsal olayların önlenmesi için yapılan gözetleme faaliyetleri olmak üzere on farklı başlık altında sınıflandırılabilir.³²⁸

Gözetim teknolojilerinin toplumsal yaşamda güvenliği sağladığı düşünülerek ona karşı çıkılmamaktadır.³²⁹ Zira bu teknolojilerin, suç konusunda caydırıcı olduğu ve toplumda

³²⁵ David Lyon, *a.g.k*, 2006, s.35.

³²⁶ Julie K. Petersen, *a.g.k*, s.541.

³²⁷ Kirstie Ball, Frank Webster, *a.g.k*, s.5.

³²⁸ Julie K. Petersen, *a.g.k*, s.64.

³²⁹ David Lyon, *a.g.k*, 2006, s.95.

korkuya yol açan tehditlerin önüne geçtiği değerlendirilmektedir. Ayrıca, toplumu sürekli olarak yabancıların istila alanı olarak algılamak, yabancılarla birlikte yaşıyor olmak, kişilerin toplumda her an zarar görebilecekleri endişesini barındırmalarını, bu da gözetime dayalı güvenlik isteğini körüklemektedir. Örneğin terör korkusu, insanların gözetlenmeye karşı çıkmamalarında en önemli etkenlerdendir. Hatta bu bağlamda çeşitli korku atmosferleri yaratılarak, tehdit altında olduğuna inandırılan halkların gözetime razı edilebilmeleri sağlanmaktadır. Fakat diğer taraftan güvenlik için benimsenen gözetim teknolojisi herkesi ve her şeyi güvenilmez yapmaktadır; böyle bir toplumda herkes potansiyel suçlu, her şey düzen ve huzur bozucu bir tehdit halini almaktadır. Güvenlik artırıcı her tür gözetim mekanizması, toplumun yararına olduğu için kabul edilir. Gözetim araçları, önceden bilmeye bağlı olarak, riski en aza indirmenin yolu olarak görülür.³³⁰

Güvenlik temelli gözetim faaliyetlerinin en büyük tehlikesi şüphesiz onların sinsî bir virüs gibi durmaksızın yayılmasıdır. Petersen'a göre bir değişim tedricen uygulandığında, bununla ilgili tehditler çoğu zaman fark edilmez.³³¹ Örneğin, bir kurbağayı kızgın bir tavaya aniden bıraktığınızda kurbağa birden sıçrar ve kaçır. Fakat kurbağayı tavaya bıraktığınızda tava normal sıcaklıkta olsa ve yavaş yavaş tavayı ısıtmaya başlasanız kurbağa farkında olmadan pişecektir.

Gözetim faaliyetleri ile bütünleşmiş olan kameraların beş - altı yıl önceki durumu ile şimdiki durumları karşılaştırıldığında Petersen'ın haklı olduğu görülmektedir. Günümüzde hemen hemen her dükkanda, alışveriş merkezinde, kamu binalarında, bankalarda, sokaklarda kameralar vardır. Güvenlik güçleri bunları kullanmaktadır ve zaman ilerledikçe bu kameralara yüz tanıma sistemleri gibi üst düzey teknolojiler de eklenecek; gözetim faaliyetleri ve gözetleme teknolojilerini geliştirme, bu teknolojileri kullanma hırsı devamlı artış gösterecektir. İşin kötü tarafı ise toplumun tedricen olan bu gelişim seyrinin farkında olmaması ve gözetim bilgisinin nesnesi olmayı baştan kabul etmiş olmasıdır.

Güvenlik güçlerinin gözetim teknolojileri ile silahlanmasını haklı kılacak nedenlerin başında suçluların da modernleşme ile beraber hızla gelişen teknolojik imkanları araştırması ve suç faaliyetlerini icra ederken bunları profesyonel bir şekilde kullanması yatmaktadır.³³² Bu noktada güvenlik güçlerinin suçlularla başarılı bir şekilde mücadelesi için

³³⁰ Julie K. Petersen, *a.g.k.*, s.542.

³³¹ *a.k.*

³³² Yılmaz Yazıcıoğlu, *a.g.k.*, s.111.

suçlulardan her zaman bir adım önde olacak şekilde bilgi ve iletişim teknolojilerini kullanması, bilgiyle donatılması ve bu konularda uzmanlaşması gerektiğine inanılmaktadır.

Güvenlik güçlerinin suçların izahını yapması ve çözmesi, bir takım delil ve izleri metodik olarak değerlendirip yorumlaması ve somut şekilde ortaya koyarak açıklığa kavuşturması ile mümkün olmaktadır. Diğer taraftan güvenlik güçlerinin temel fonksiyonu suç olduktan sonra suçu aydınlatmanın ötesinde proaktif polislik olarak ifade edilen suç oluşmadan suçu önlemektir. Suç oluşmadan önce suçu önlemek ise ancak güvenlik güçlerinin suç oluşma sürecini görmesi ve buna dahil olmasıyla gerçekleşebilir. Bu noktada da devreye istihbarat faaliyetleri girmektedir.

İstihbarat faaliyetleri yürütülürken gözetim teknolojilerini kullanmak güvenlik güçleri için vazgeçilmez birer araç haline gelmiştir. Örneğin, şehir merkezinde yüzlerce masum insanı öldürebilecek olan bombanın patlamadan önce tespiti için güvenlik güçleri telefon dinlemesi, kameralı gözetim, ortam dinlemesi yapabilmektedir. Bu durum esasında dünyada bir başarı göstergesine dönüşmüştür. Sayılı'nın ifade ettiği gibi gelişmiş ülkelerde polisin başarısı bilgiye hızlı ulaşımı ve teknolojik imkanları kullanması ile eşdeğer tutulmaktadır.³³³ Diğer taraftan proaktif tabanlı güvenlik anlayışında gözetim faaliyetlerinin alabileceği distopya da asla küçümsenmemelidir. Bu distopya *Azınlık Raporu*³³⁴ filminde açık bir şekilde resmedilmiştir.

Emile Durkheim gibi düşünürlere göre suç, her toplumda var olan, niteliği toplumdan topluma değişiklik gösterebilen ve engellenemeyen bir unsur³³⁵ olarak ele alınsa da, Foucault için suç işleme eğilimi ve suç riski bulunmadıkça polis gibi denetim organlarına da gerek yoktur.³³⁶ Şayet bu bağlamda biz suç olgusuna ve gözetleme eylemine Foucault'cu bir perspektiften bakmayı tercih edersek, risk üretiminin, aslında gözetim mekanizmasının varlığının sürekliliğini sağlayan bir gereklilik olduğundan, hatta suç ve gözetim ilişkisinin birbirine eklemlendiği bir devamlılıktan söz edebiliriz. Zira “normal bir fenomen” olarak suç,

³³³ Müslüm Sayılı, “Dünyada Gelişen Teknolojik Yenilikler ve Türk Polis Teşkilatına Adaptasyonu”, 21. Yüzyılda Polisin Eğitimi Sempozyumu, Ankara, EGM Yayınları, 2001, s.781.

³³⁴ Azınlık Raporu Filmi (Minority Report-2001): Ünlü bilimkurgu yazarı Philip K. Dick'in bir kısa öyküsünden yönetmen Steven Spielberg tarafından uyarlanan film, 2054'te Washington DC'de geçmektedir. Filmde suç işlemeyi düşünen insanlar, bu suçları işlemeyi önce tespit edilmektedir. Bu tespit işlemi poliste yer alan suç öncesi biriminde çalışan üç tane insanı varlık ve bazı teknolojik aygıtlar sayesinde olmaktadır. Filmdeki önemli noktalardan biri polis suçu işleyeceği öngörülen kişiyi suçu işlemeyi önce yakaladığı halde tutuklamaktadır. Film, Dedektif John Anderton (suç öncesi biriminin başı)'un cinayet suçlamasıyla karşı karşıya kalması etrafında gelişir.

³³⁵ Stephen P. Turner, Emile Durkheim, *Sociologist and Moralist*, Routledge, London, 1993, s.72., akt., İpek Görgün, “Denetim Toplamlarındaki Gözetleyen - Gözetlenen İlişkisi Bağlamında Mobese ve Nobese Projeleri”, 2009, s.7., <http://izleniyoruz.50webs.com/biz.html>, (Erişim Tarihi: 29.09.2013).

³³⁶ Michel Foucault, *a.g.k*, 2003, s.31.

nihayetinde engellenemeyen bir olgu olarak anılmakta ise, suçun önüne geçme amacıyla kurulan gözetim teknolojilerinin var oluş sebeplerini zaten Durkheim'cı bir perspektifle açıklamamız mümkün olmayabilir. Çünkü son tahlilde Durkheim'ın bulunduğu noktadan bakmaya çalışsak bile, eğer bir sistem “engellenemeyen” bir olguyu “engellemek” iddiasıyla kuruluyorsa ve bu iddia doğrultusunda gözetleme yapıyorsa bir çelişki varlığından söz edebiliriz. Başka bir deyişle, suçun önüne geçilemeyeceğini bilen bir iktidar suçu engelleyeceği vaadiyle bireylerin mahremiyet ve özgürlük alanlarına müdahaleyi kendince meşrulaştırıyorsa, burada suçun ve suçla birlikte risk unsurunun var oluşunun modern iktidar tarafından manipüle edildiğini, bu manipülasyonun da suç - iktidar ilişkisi bağlamında eklenerek geliştiğini belirtebiliriz.

Sonuç olarak her ne kadar güvenlik tehlikesi ve bundan dolayı ortaya çıkan belirsizlik ve kaotik ortam ile mücadele güvenlik güçlerinin gözetim teknolojilerini kullanmasını meşrulaştırıyor gibi gözükse de aslında suçların da artışına ve kompleks hale gelmesine yol açan gözetim tabanlı teknolojilerinin suça meyilli kişileri de içine alacak şekilde giderek toplumsallaştığı bir gerçektir. Böylece suç işleme düşüncesi olmasa da bu teknolojiler vasıtasıyla suç işlemenin kolaylaşmış olması aslında suç oranlarını azaltmayacak, arttıracaktır. Nitekim suçtan arınmış bir toplum ütopyadan ileri gidemeyecektir. Bu bakımdan güvenlik güçlerinin suç işleme oranlarını sıfırlama gibi bir amaç ile yola çıkarak gittikçe daha fazla toplumu gözetleyecek teknolojilerle donanması amaç bakımından mutlak butlan ile batıl olur.

1.Güvenlik ve Gözetim Teknolojisi

Gözetim faaliyetlerinin yaygınlaşmasında meşruiyet sebebi olarak görülen güvenliğin sağlanması içerisinde gözetimi haklı hale getiren en büyük etmen toplumun tüm kesimlerini tehdit eden terörizmle mücadeledir. Terörizmin farklı şekillerde tanımları mevcuttur. Bunlardan birkaç tanesi şu şekildedir:

“Terörizm, toplumun yapısını ve kamu otoritesini yıkmak, rejimin temel niteliğini değiştirmek için korkutma, sindirme, yıldırma ve şiddet eylemlerinin bütünüdür.”³³⁷

“Terörizm; çoğunlukla organize bir grup tarafından işlenen, savaş dışı kişiler üzerinde kasıtlı öldürme veya diğer ciddi zararlar ya da tehdit içeren politik eylemlerdir.”³³⁸

Günümüzde uluslararası tehdit olabilecek terörist saldırıları; terör örgütleri tarafından kimyasal, biyolojik ve nükleer silahların temin edilerek kullanılması; bir ülkenin bilgisayar ile desteklenen hizmet unsurlarının *hacker* ve *crackerlar* vasıtasıyla yok edilmesi, yani siber

³³⁷ Sami Denker, *Uluslararası Terör Türkiye ve PKK*, Boğaziçi Yayınları, İstanbul, 1997, s.4, akt., Ünal Acar, Ömer Urhal, *Devlet - Güvenlik, İstihbarat - Terörizm*, Adalet Yayınları, Ankara, 2007, s.321.

³³⁸ C.A.J. Coady, *Terörün Ahlakı*, Cogito Şiddet Özel Sayısı, 2005, s.265, akt., Ünal Acar, Ömer Urhal, *a.g.k*, s.321.

terörizm; kamu binaları ve kamu görevlilerine yönelik saldırılar ile uçak kaçırma tipi konvansiyonel saldırılar olmak üzere üçe ayırmak mümkündür.³³⁹

Terörizmin en riskli ve toplumda rahatsızlık uyandıran yanı kuralsız ve görünmez olmasıdır.³⁴⁰ İnsanlar evlerinde otururken, sinemada film izlerken, alışveriş merkezinde dolaşırken, otobüste - uçakta yolculuk ederken ya da işyerlerinde çalışırken hiç beklemedikleri bir anda terörizmin mağduru olabilirler. İnsanların terör eylemleriyle her an her yerde karşılaşma olasılığı, doğal olarak onlarda büyük bir tedirginlik, korku ve endişeli bir bekleyiş psikolojisi oluşturmaktadır. İnsanlar kalabalık ortamlara girmekten, toplu taşıma araçlarını kullanmaktan çekinmekte, günlük hayatlarını yaşayamaz hale gelmektedirler. Bu durum terörizmin hedeflediği her an korku ve endişe yaşayan toplum modelidir.

Terörizm neticesinde ortaya çıkan korku ve endişe toplumda geri dönülmeyecek bir güvenlik güçlerinin terörle mücadelede kullandığı yöntemleri kabullenme psikolojisini doğurmaktadır. Buna bir de dördüncü kuvvet olarak ifade edilen medyanın propagandası eklenince bu psikolojik ortam toplumun her kesimine derinlemesine nüfuz etmektedir. Nitekim medya, gösteri araçlarıyla bireyleri "Dikkat et! Bir sonraki sen olabilirsin!" şeklinde uyarmaktadır. Bu yönlendirmeler paralelinde terörizm için gözetim gerektiğine toplum inandırılmış ve devletler gerek ulusal gerekse de uluslararası düzlemde gözetim araçlarını terör ve güvenlik söylemleri üzerinden meşrulaştırarak devreye sokmuşlardır.³⁴¹

Bilgi ve iletişim teknolojilerindeki gelişmeler paralelinde gözetleme konusu kitleyi toplumun geneli oluşturmaya başlamış, gözetleyen sadece devlet olmaktan çıkarak sivil unsurları da kapsar hale gelmiş, gözetlenebilecek veri çeşitliliğinde sınır ortadan kalkmış ve gözetim sistematikleşmiştir.³⁴² Yeni gözetim teknolojileri, toplumların güvenliğini sağlama misyonuyla gündelik yaşama dahil olsa da, aslında daha çok risk yönetimi amacıyla kullanılmaktadırlar. Kayıtlama sistemlerini güvenliklerinin sağlanmasının bedeli olarak görenler için gözetim, "caydırıcı polis" gibi suçu veya tehdidi önceden önleyici bir niteliğe sahiptir. Kentlerde kavşaklara, meydanlara, ana arterlere, üniversite yerleşkelerine, kamu binalarının içine, AVM'lerin dış duvarlarına yerleştirilen kapalı devre kamera sistemleriyle önlenen suçlar ve yakalanan suçlular göz önünde bulundurulduğunda kuşkusuz bu dijital

³³⁹ Suat Doğan, *Küresel Dünyada Terörizm Konsepti*, EGM Basımevi, Ankara, 2004, s. V.

³⁴⁰ Ünal Acar, Ömer Urhal, *a.g.k.*, s.326.

³⁴¹ Kirstie Ball, Frank Webster, *a.g.k.*, s.2.

³⁴² *a.k.*

gözetim olgusunun ilk etapta ön plana çıkan özelliği, caydırıcı olması ve güvenliği sağlaması olmaktadır.³⁴³

Günümüzde giderek artış gösteren terör eylemlerine karşı gözetleme araçlarıyla donanma seferberliği dünya konjonktüründe 11 Eylül 2001 tarihinde ABD’de Newyork ve Washington şehirlerinde Dünya Ticaret Merkezi ve Pentagon’a yönelik gerçekleştirilen uçaklı terörist saldırıdan sonra ivme kazanmıştır. Bu olayın ardından daha çok toplumun güvenliği ön plana çıkartılarak gözetime ilişkin gereklilik daha da derinleştirilmiş, güvenliklileştirme söylemi meşru kılınmıştır. Bu çerçevede bütün dünya ülkeleri güvenlik politikalarını yeniden gözden geçirmiş ve terörle mücadelede yapısal bir dönüşüm sürecine girmiştir. Bu saldırılar gözetim karşıtı söylemleri susturan bir dönüm noktası olmuştur. Üstelik gözetimin daha disiplinler bir şekilde uygulanmasına ve zaten sınırları belirgin olmayan suç ve terörizm arasındaki çizginin iyice bulanık hale gelmesine neden olmuştur.³⁴⁴

11 Eylül saldırısı, uluslararası güvenlik politikaları ve siyaseti açısından en az Soğuk Savaş’ı sona erdiren Berlin Duvarı’nın yıkılışı kadar önemlidir. Çernobil faciası, modern toplumlarda teknolojinin insan kontrolünde ve denetiminde olduğu mitini neden olduğu küresel çaptaki risklerle nasıl çökertmişse, 11 Eylül terör saldırısı da özgürlük esaslı devlet mantığını yıkmış ve yerine güvenlik temelli polis devleti algısını olumsuzlaştırmıştır.³⁴⁵ Bu saldırılarının gözetime bakan yönüyle iki temel sonucu vardır. Birincisi sosyal hayatımızı şekillendiren gözetim süreçlerinin yaygınlaşması, ikincisi gözetim teknolojilerine olan toplumsal güvenin artışıdır. Bu iki temel sonuç çerçevesinde özellikle batı devletleri gözetim faaliyetlerini merkezileştirmiş, tek elden yürütmeye yönelik adımlar atmış ve gözetim faaliyetlerini yoğunlaştırmıştır.³⁴⁶

Bu paralelde güvenlik güçlerinin her türlü gözetim faaliyetlerini gerçekleştirmelerinin önündeki yasal engellerin ortadan kaldırılması gerektiği anlayışı hakim kılınarak gerekli yasal düzenlemeler yapılmıştır. Güvenlik güçleri yeni modern gözetim sistemleri satın almış ve bunları özgürce kullanmaya başlamıştır. Örneğin Lyon’un yaşadığı Kanada’da teröristlerin tespiti için ülkeye giriş yapan bütün yabancılar tek bir veritabanında toplanmış, bunlarla ilgili anlık ırk - renk analizi yapılmaya başlanmıştır.³⁴⁷ Nitekim bu durum ülkeye giriş yapan tüm

³⁴³ a.k

³⁴⁴ a.k

³⁴⁵ a.k

³⁴⁶ David Lyon, “*Surveillance after September 11, 2001*”, a.g.k, Ed. Kirstie Ball, Frank Webster, 2003, s.17 - 18.

³⁴⁷ a.k

yabancıların ülkeye girer girmez belki de daha girmeden gözetim altına alındığını göstermektedir.

11 Eylül saldırılarının gözetime olan etkileri doğal olarak en çok Amerika Birleşik Devletleri'nde hissedilmiştir. Saldırlardan hemen sonra sanki hazırda bekliyormuş gibi ileri teknoloji şirketleri sorumluları medyaya çıkmış ve halkı bu korku dolu zamanında gözetim teknolojilerinin gerekliliği noktasında sindirmeye çalışmıştır. Nitekim bazı şirket sahipleri ABD'de yaşayan herkese çip tarzında bir verici takılmasını ve böylece kimin ne zaman nerede olduğunu rahatlıkla tespit edebilecekleri teklifinde bile bulunmuş ve bu teklif halkın bir kısmı tarafından makul görülmüştür.³⁴⁸ Bu durum da terörist saldırıların halk üzerindeki etkisini açıkça ortaya koymaktadır.

Özellikle ABD'de halkın parası bu tür saldırıların tekrar olmadan önce önlenmesi için yüksek gözetim teknolojilerine, istihbarat servislerine ve güvenlik teşkilatlarına akmıştır.³⁴⁹ Nitekim ABD'de güvenlik güçlerine herhangi bir yargı denetimi olmadan telefon görüşmeleri, fax yazışmaları, mobil iletişim de dahil olmak üzere her türlü elektronik iletişimi sürekli olarak izleyebilmenin yolu açılmıştır.³⁵⁰ Böylece yeni iletişim teknolojileri ve enformasyon ağları ile anayasal haklar doğrultusunda güvence altına alınmış tüm kişisel mahremiyet haklarını çiğneyen bir gözetim toplumu oluşturma yoluna girilmiştir. Nitekim bu saldırılardan sonra Başkan Bush'un şu sözleri yeni girilen dönemi açıklamaktadır.³⁵¹

“...(11 Eylülü kastederek) Bu 19 uçak korsanının Saddam Hüseyin tarafından silahlandırıldığını, yeni silahlar ve yeni planlarla desteklendiğini düşünün. Ülkeye [yasadışı olarak sokulan] küçük bir şişe, teneke kutu ya da bir sepet, şu ana kadar tecrübe etmediğimiz bir felaketin meydana gelmesine sebep olabilir. İşte bizim yönetimimizde o günün hiç gelmemesi için elimizden gelen her şeyi yapacağız...”

Tarihi önemi bulunduğu değerlendirilen bu terörist saldırılardan sonra oluşan atmosferde gözetim adına atılan önemli adımlardan birisi de daha önce zaten özel sektörde kullanılan biometrik tanımlayıcıların güvenlik güçleri tarafından kullanımının gerekliliğinin ortaya konulması olmuştur. Bu kapsamda ABD ve İngiltere gibi batı ülkelerinde güvenlik güçlerinin biometrik verileri toplaması ve analiz edebilmesine yönelik yeni hukuki düzenlemeler oluşturulmuştur.³⁵²

11 Eylül saldırıları bir taraftan gözetim teknolojilerinin artışı ve geliştirilmesine çok büyük bir zemin hazırlamışken diğer taraftan esasında güvenlik odaklı gözetim faaliyetlerinin büyük bir başarısızlığı olmuştur. Nitekim bu saldırılar öncesinde ABD güvenlik güçleri

³⁴⁸ a.k

³⁴⁹ Bu konuyla ilgili ayrıntılı bilgilere <http://www.viisage.com> adresinden ulaşılabilir.

³⁵⁰ www.privacyinternational.org/survey, (Erişim Tarihi: 22.08.2013).

³⁵¹ George Bush'un 28 Ocak 2003 Tarihli Ulusa Sesleniş Konuşmasından alınmıştır.

³⁵² David Murakami Wood, *a.g.k.*, s.23.

“Bilgisayar Destekli Yolcu Ön Tanıma Sistemi” olarak ifade edilen gözetim teknolojisini kullanarak ABD’ye gelen ve giden tüm yolcuların ön yolcu bilgilerini daha yolculuk başlamadan önce tek bir veritabanında toplayıp, bunları analiz ederek şüpheli profilde olanlara yönelik tedbir uyguladığı halde teröristlerin saldırılarını engelleme noktasında başarısız olmuştur.³⁵³ Diğer taraftan bu teknolojiyi destekleyecek ABD’nin diğer gözetim araçları da göz önünde bulundurulduğunda gözetim faaliyetlerinin tam bir fiyaskoya dönüştüğü açıkça anlaşılmaktadır.

Klasik anlamda bilinen terörizm günümüzde hızla gelişen bilgi ve iletişim teknolojilerinin de etkisiyle sanal alemde de yerini almış ve “siber terörizm” olarak kavramsallaşmıştır. Siber terörizm, klasik terörizmin amaç ve hedeflerine ulaşmada bilişim teknolojilerinden faydalanılmasını ifade etmektedir. Siber terörizm araçlarıyla, klasik terörizm araçlarına göre çok daha geniş bir kitleyi etkileyebilecek şekilde daha maliyetli zararlar verilmesi mümkün olabilmektedir. Örneğin, siber teröristler bir ülkenin güvenliğini geniş bir coğrafyanın enerjisini keserek devre dışı bırakabilir. Böylelikle daha fazla insanı, daha az risk alarak etkileyebilir ve panik yaşatabilirler.³⁵⁴

Siber terörizm çok çeşitli şekillerde olabilmektedir. En çok duyulan şekli popüler olan bir bankayı bilişim teknolojilerini kullanarak korkutmak veya tehdit etmektir. Siber teröristler, bankanın bilgisayar güvenlik altyapısını çökerterek yöneticilere amaçlarına uygun bir mesaj bırakırlar. Teröristler, istedikleri parayı belirli bir süre içinde alamadıkları takdirde kuruma ait gizli belgelerin zarar göreceğini, müşteri dosyalarının silineceğini ya da şubelerle olan ağ yapısı bilgi akışının işlevselliğini kaybedeceğini bildirerek şantaj yaparlar.³⁵⁵ Bunun gibi kamu kurumlarının da bilişim altyapılarını hedef alan çeşitli terörist saldırılar olabilmektedir.

Siber suçlarla mücadelede suçun kim tarafından ne zaman ve nasıl işlendiği, potansiyel suçlunun hangi ülkede olduğunun tespiti, kanıt toplama ve ispat, uluslararası ilişkiler ve anlaşmalar gibi birçok alanda sıkıntı yaşanmaktadır. Bütün bu alanlarda yaşanan sıkıntılar ise siber teröristin işine gelmekte, izini kaybettirebilmektedir. Diğer taraftan siber teröristlerce saldırıya uğrayan banka, finansal kurum veya şirket ise bu tür bir saldırıya maruz

³⁵³ David Wood, Eli Konvitz, Kirstie Ball, “The Constant State of Emergency?: Surveillance after 9/11”, Ed. Kirstie Ball, Frank Webster, *a.g.k.*, s.143.

³⁵⁴ Murat Erdal, “Tekno - Güvenlik Problemlerinin Uluslararası İlişkilerdeki Yeri ve Türkiye”, *İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, Sayı 21 - 22, İstanbul, 2000, s.27.

³⁵⁵ *a.k*

kaldığını kendi imajı ve güvenilirliği açısından çoğu zaman kamuoyu ile paylaşmamaktadır.³⁵⁶

Gary T. Marx’a göre günümüzde yaygın olarak kullanılan gözetim tekniklerinin birçoğu ilk olarak sadece yüksek güvenli hapisanelerin ve askeri kurumların güvenliğini sağlamak için kullanılmaya başlanmıştır. Bu paralelde Marx gözetim teknolojilerinin giderek yaygınlaşmasına dikkat çekmek için “Acaba gözetim teknik ve araçlarının giderek sivil toplumda yaygınlaşmasıyla yüksek güvenli topluma doğru mu gidiyoruz?” sorusunu sormuştur. Marx böyle bir soru işaretiyle gözetim toplumundan belkide daha ileri bir seviyeyi göstererek “yüksek güvenli toplumu” işaret etmiş ve özel hayatın gizliliği açısından büyük bir tehlikenin varlığına dikkat çekmiştir.³⁵⁷

Yüksek güvenli toplumun bir takım özelliklerinden burada bahsedilebilir. Bunlar, bilgisayar kayıtlarının önemli rol oynadığı bir sicil toplumu; yapılan veri kategorileri, veri karşılaştırmaları ve üyelikler sonucunda bireyler tarafından gelecekte izlenecek davranışların tahminine dayanarak kararların alındığı aktüaryal toplum; herkese şüpheli gözüyle bakıldığı şüpheli toplum; tercihlerin sınırlandırıldığı ve bu tercihlerin sosyal çevre tarafından belirlendiği toplum mühendisliği; zamanın sınırlarının kalktığı, geleneksel olarak korunan bilgilerin önündeki engellerin zayıfladığı şeffaf toplum; otomatik gözetimin öncül rol oynadığı self - monitoraj toplumdur.³⁵⁸

Günümüz toplum yapısında Marx’ın dikkat çektiği bu özelliklerin büyük oranda gerçekleştiği görülmektedir. Artık gözetim toplumundan da ileri bir aşamaya yüksek güvenli topluma doğru gittiğimiz hatta içinde bulunduğumuz ifade edilebilir. Böyle bir süreçte özel hayatın gizliliği ve güvenlik dikatomisinde galip olan güvenlik için gözetleme olduğu da bir gerçektir.³⁵⁹ Aşağıda verilen örnek ve açıklamalar ile Marx’ın öngörüsünün gerçekleşmiş olduğu iddia edilebilir.

“...Anton B. sabah evden ayrıldığında üç kere kaydedilmişti bile. Ailesiyle olan telefon görüşmesi bir telefon şirketi tarafından kaydedilmişti. Apartmanında dışarı adım atar atmaz gözetim kameralarının görüş alanına girmişti. Dört yaşındaki oğluyla asansörden zemin kata indiğinde kapıcı Anton’a gülümseyerek baş salladı ve ilerleyince elindeki not defterine saat kaçta çıkış yaptığını not etti. Çocuğunu kreşe götürdü ve güvenle işine doğru gitmeye başladı, çünkü çocuğunu merak ettiğinde ofisindeki bilgisayarda bir tıklama işlemi yapacak ve kreşteki kameradan çocuğunu izleyebilecekti. Daha sonra arabasına bindi, radyoyu açtı ve güneş gözlüklerini takıp otoyola doğru yöneldi; çünkü bu yoldaki bütün radarların yerini biliyordu. Sonra yaya üst geçidindeki flaşörü görünce birden frene bastı, burayı unutmuştu - burada da bütün plakalar kaydedilip çalıntı araç plakaları ile karşılaştırılıyordu. Şirketinin garajına girene kadar toplum içindeki bütün hareketleri çoktan kaydedilmişti. Daha sonra

³⁵⁶ a.k

³⁵⁷ Gary T. Marx, *a.g.k*, 2005, s.1.

³⁵⁸ a.k

³⁵⁹ a.k

ofisine elinde bilgisayar çipi olan bir kartla girdi, bu kart saat kaçta işe giriş yaptığını kaydediyordu. Bilgisayarının başına geçti ve e-maillerine bakmak üzere bilgisayarı açtı, klavye ile bilgisayar arasında özel bir aparat bulunuyordu, bu aparat bütün klavye hareketlerini kaydediyordu. Anton güvenilir bir iş pozisyonunda bulunsay da kendi bilgisayarına da bu aparat takılmıştı. İşçiler interneti kendi şahsi amaçları için kullanabiliyorlardı, ancak yaptıkları bütün uygulamalardan ve girdikleri sitelerden bu aparatlar sayesinde sorumlu tutulduklarından kimse şahsi amaçları için internete girmeyi tercih etmiyordu.

Anton'a iki tane telefon geldi. Birisinde muhasebecisi aramıştı ve kredi kartıyla ilgili olarak ifade vermesini istiyordu. Bir yıl önce Anton'un yapmış olduğu tatilde otel parasını kredi kartından ödemişti ve yetkililer ondan habersiz kredi kartı işlemlerine girmiş ve soruşturma açmışlardı. Bu durum Anton'un içini rahatsız ederken pencereden aşağı doğru baktı. Birisi yüksek sesle şarkı söylüyordu ve şüpheli sesleri takip eden küçük bir gözetim aracından uyarı sinyali gözükte. İkinci telefon Anton'un aile doktorundan geldi. Buna göre Anton'un sağlık dijital kartına yeni bir bilgi girmesi isteniyordu. Acil durum tedavisini kolay ve ucuz yapmak için sigorta şirketleri bilgisayar çipli bir kart geliştirmişlerdi. Bu kartta kişinin kimlik bilgilerinin yanında daha önceden hakkında yapılan teşhisler, reçeteler ve tedaviler bir organ bağış sözleşmesiyle birlikte yer alıyordu.

İş bitimine yakın Anton'a kayınbabasından bir telefon geldi. Telefon konuşmalarının hepsi kaydediliyordu ve gizli görüşmeler yapılamaması için çalışma ofislerinin duvarları diğer odalardan duyulacak şekilde yapılmıştı. Telefon görüşmesinden sonra Anton mesai bitiminde iş giriş, çıkış dijital kartını makineden geçirdi ve garaja doğru yöneldi. Bina korumaları bu aletler ve kameralar sayesinde binada kimin bulunup bulunmadığını biliyorlardı. Anton işten çıktıktan sonra süpermarkete gitti. Süpermarketin girişinde kamera ve X-Ray cihazı bulunuyordu. Bu cihaz sadece çanta ve elbise altında saklanan eşyaları değil aynı zamanda kişinin vücudunun çıplak halini de gösteriyordu. Alışverişi yaptıktan sonra cüzdanından kredi kartını çıkarırken biraz çekindi çünkü kredi kartlarına kişinin satın aldığı ürünler kaydediliyordu dolayısıyla tercihleri takip ediliyordu. Daha sonra eşini almak üzere tren istasyonuna gittiğinde önce güvenlik görevlileri vücudunun her yerini, çantasını elle aradılar. Daha sonra yüz tarama sisteminden geçti. Bu cihaz aranan (cezası, borcu olanlar) ve şüpheli şahısları tespit ediyordu. Bunun çalışma sistemi veritabanına önceden girilen yüzlerdeki ölçü oranlarını kamera önündeki yüzlerin (göz-kaş arası, kulak-burun arası mesafe gibi) oranları ile karşılaştırma şeklinde olmaktadır. Bu işlem saniyenin binde biri kadar kısa bir sürede olmaktadır ve takma sakal - bıyık vs. bunun tespitini de engellemektedir. Normal şartlarda insanlar tarafından bu işlemin yapılması aylar sürebilir. Diğer taraftan istasyonun her yerinde de şüpheli hareketleri takip etmek üzere kameralar bulunuyordu. Eve gidip yatağa girdiğinde Anton şöyle bir düşündü: Bugün tek bir dakika bile takip edilmeden - gözetlenmeden geçmemiştii...³⁶⁰

Yukarıda Anton'un bir günlük yaşantısı anlatılmıştır. Bu bir günlük süreçte Anton'un hemen hemen hiçbir anı kayıt dışı kalmamıştır. Esasında ilk bakışta bu durum bir distopya gibi görünse de günümüzde anlatılanların çoğunu kendi gerçek yaşantımızda görebiliriz. Kapıcının kayıt tutması, mahallemizdeki varlığından bile haberdar olmadığımız güvenlik güçlerine çalışan muhbirler veya özel görevli personel tarafından tutulan kayıtlar ile ifade edilebilir. Telefon görüşme trafiğimiz bütün GSM operatörleri tarafından düzenli olarak tutulmaktadır. Günümüzde kreşlere veya anaokullarına yerleştirilen internet bağlantılı dijital kamera sistemleri sayesinde internetin olduğu her yerden çocuklarımızı canlı olarak izleyebilmekteyiz. Hemen hemen bütün ana yollarda trafikte hız ihlali yapan araçları tespit etmek amacıyla kurulduğu ifade edilen radar kameralar, kırmızı ışıktaki geçen araçları tespit etmek amacıyla kurulduğu ifade edilen trafik ışık kontrol kamera sistemleri ve genel güvenliği bozanları veya suç işleyenleri tespit etmek amacıyla kurulduğu ifade edilen Kent

³⁶⁰ Wolfgang Sofsky, *Privacy: A Manifesto*, Princeton University Press, Princeton, 2008, s.1 - 7.

Güvenlik Kamera Sistemleri yer almaktadır. Bu kameraların gündelik faaliyetlerimizin çoğunu kayıt altına aldığı bir gerçektir.

Hemen hemen bütün kamu ve özel işyerlerinde personelin giriş - çıkışını takip etmeye yarayan dijital personel kartları veya retina, parmak izi tarayıcı sistemleri kullanılmaktadır. İşyerinizde veya evinizde kullandığımız bilgisayarlardaki her hareketi kaydedebilen ve merkezi bir veri sunucusuna ya da başka bir bilgisayara iletebilen programları internetten rahatlıkla bulabilirsiniz. Kredi kartınızla yaptığımız bütün işlemler ilgili bankanın veri tabanlarında yıllarca saklanmakta; bankalar istedikleri zaman harcama profilinizi çıkarabilmekte, hatta bunları alışveriş şirketlerine satabilmektedirler. Tüm sağlık işlemleri (geçirilen hastalıklar, kullanılan ilaçlar vb.) sağlık çalışanlarının kullandığı internet bağlantılı programlarda anlık olarak kaydedilmekte ve saklanmaktadır. Her alışveriş merkezine X-Ray cihazından geçtikten sonra girilmektedir. Görüldüğü üzere yaşıntımız hiç de Anton'unkinden farklı değildir. İşte bu noktada gözetim toplumunun da ilerisinde olarak yüksek güvenliğini toplumun içinde olduğumuz ifade edilse yanlış olmayacağı düşünülmektedir.

Günümüzde bireyler güvenlik tabanlı veya gözetim teknolojilerinin ne kadar yaygınlaştığının ve normalleştiğinin; bu noktada kendisinin doğuştan sahip olduğu hakları daha doğuştan itibaren (doğar doğmaz bebeklerin biometrik fotoğrafları çekilmektedir) kaybetme noktasına geldiğinin farkında değildir. Bu bağlamda artık insanlar güvenlik denilince özgürlüklerini çekinmeden feda edebilir konuma gelmişlerdir. Diğer taraftan özel hayatın gizliliği seçimlerde oy getiren bir konu olmadığı için de siyasetçiler tarafından da savunulmamaktadır. Yurttaşlar özel alanlarının kısıtlanmasını protesto etmemekle birlikte bu durumu kabullenmiş gözükmemektedirler. Protestonun az oluşu tehlikenin azlığı anlamına gelmemektedir.³⁶¹

Yüksek güvenliğini toplumun en güzel örneklerinden birisi “Echelon” sistemidir. Bu sistem, Amerika, İngiltere, Kanada, Avustralya ve Yeni Zelanda arasında, dünya üzerindeki her tür iletişimi deşifre etmek, kontrol etmek ve dinlemek üzere kurulmuş, geniş istihbarat ağını ifade etmektedir.³⁶² Sistem, dünya çevresinde beş ana stratejik uyduyu kullanmaktadır. Bu uyduların her birinin yeryüzü üzerinde bir ana üssü yani istasyonu bulunmaktadır. Ayrıca sistem, 100'ün üzerinde irili ufaklı uyduyu da kullanıp, yönlendirebilmektedir. Bu uydular vasıtasıyla sistemin, dünya üzerindeki cep telefonu, e-postalar, faks, tele-faks, bilgisayar ve okyanusun altından geçen iletişim hatları da dahil olmak üzere her şeyi dinlediği, gördüğü

³⁶¹ a.k, s.8 - 10.

³⁶² Gürdilek Raşit, “Echelon”, *Bilim Teknik Dergisi*, Ekim 2001, s.36 - 37.

izlediği ve bunları kaydedip analiz ettiği; bu kapsamda dakikada 2 milyon, günde ise tam 3 milyar telefon görüşmesini takip ettiği iddia edilmektedir.³⁶³

1.1. Kameralı Gözetim

“Günde ortalama 10 kere kamera karşısındasınız.
Ona göre giyindiniz mi?”³⁶⁴

Kameralı gözetim, günümüzde hızla yaygınlaşan ve gelişen; gözetim faaliyetlerinin en görünür taraflarından birisi olan ve toplumun bilgisinin toplanıp, kategorize edilip, depolanıp analiz edilmesini içeren teknolojik sistemlerin önemli bir örneğidir. Kapalı ve açık alanlarda oldukça sık rastladığımız kameralar bireylerin günlük aktivitelerinin tespiti açısından gözetim çevresinde önemli bir yer tutmaktadır.³⁶⁵

Kameralı gözetim faaliyetleri ilk olarak İngiltere’de Londra tren istasyonunda kullanılmaya başlanmış ve sonraki yıllarda giderek kullanımı artış göstermiştir. İlk olarak Kapalı Devre Televizyon Sistemleri (KDTS) (ing; CCTV, Closed Circuit Television) kullanılmış, sonrasında dijital görüntü ve verilerin çok hızlı, kolay şekilde paylaşıldığı Dijital Ağ Kamera Sistemlerine geçilmiştir.³⁶⁶ Kapalı Devre Televizyon Sistemleri, dijital kameralardaki fotoğraflama sistemi yerine klasik radyo frekansı teknolojisini kullanarak görüntüleme sağlayan sistemlerdir. İlk olarak 1980’lerde kullanılmaya başlanmış ve görüntülü gözetim alanında maliyeti ucuz bir sistem olarak kullanışlı olmuştur.³⁶⁷

KDTS, analog televizyonlarla aynı çalışma mekaniğine sahip olan basit gözetim sistemleridir. KDTS’de yerleştirilen bir kamera belli bir yeri görüntüler ve bu görüntüyü başka bir yerdeki televizyon monitörüne gönderir. Genelde sistemde güvenlik görevlilerinin renkli ve siyah - beyaz çeşitli kamera ekranlarından izlediği tek bir güvenlik merkezi vardır. Günümüzde hala birçok şirket ve kurum KDTS sistemini ve tek bir kontrol merkezi anlayışını benimsese de çoğu kurum ve kişi para, yer, kaynak imkanları nedeniyle böyle bir sistemi artık tercih etmemektedirler. Belli bir evi, ofisi, kampüsü veya şirketi bütün kameralardan tek bir kontrol merkezine ve oradan da sistem monitörüne bağlamak oldukça pahalı, zaman alıcı ve son teknolojiler göz önüne alındığında gereksiz de durmaktadır.³⁶⁸

³⁶³ Mehmet Özcan, “Siber Terorizm ve Ulusal Güvenlik”, *İnternet ve Hukuku*, Der. Yesim M. Atamar, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s.324 - 325.

³⁶⁴ David Lyon, *a.g.k*, 2006, s.124.

³⁶⁵ Daniel Neyland, *Privacy, Surveillance and Public Trust*, Palgrave Macmillan, New York, 2006, s.19.

³⁶⁶ CCTV Code of Practice Information Commissioner's Office, Temmuz 2000, akt., Nigel Gilbert, *a.g.k*, s.23.

³⁶⁷ Anthony C. Caputo, *a.g.k*, s.3.

³⁶⁸ *a.k*, s.4.

Teknolojik gelişmeler paralelinde günümüzde teyp - kayıt gözetim sistemleri demode gözetim teknolojisi haline gelmiştir. Bu açıdan KDTS sistemleri de tercih edilen gözetim teknolojisi olmaktan çıkmıştır. Modern gözetim sistemleri artık kapalı devre değildir. Kapalı devre sistemlerinin yerini dijital ağ ve dijital kamera teknolojisi almıştır.³⁶⁹ Dijital Video Güvenlik Kamera Sistemleri, KDTS'nin yerini alan ve bunlara göre oldukça maliyeti düşük, kullanışlı ve etkili olan sistemlerdir. KDTS'de her kamerayla ilgili monitörün başına bir kişi oturtulması gerekmektedir. Ancak günümüzde bunu 7 gün 24 saat bütün kameralar için gerçekleştirmek oldukça maliyetli ve kullanışsız gözükmektedir. Bunun yerine hareketliliğe duyarlı, tanımlama tabanlı dijital sistemler kullanılarak çok az görevli ile daha yüksek performans elde edilebilmektedir.³⁷⁰

Dijital Video Kamera Sistemlerinin avantajlarından birisi de internet veya mobil ağın olduğu herhangi bir yerde kameraların görüntülerine ulaşılabilmesidir. Hatta bu sistemler, kameraların sistem dışı bırakılması veya elektrik - kablo aksamı gibi altyapısal sorunların ortaya çıkması benzeri sisteme bir saldırı olduğunda veya hırsız girdiğinde vb. tanımlanmış cep telefonu veya elektronik postaya ileti yollayarak haber verebilmekte, kaydetmiş olduğu görüntüleri de aynı şekilde belli periyotlarla buralara gönderebilmektedir. Akıllı cep telefonlarına yüklenen programlar sayesinde kamera görüntülerini canlı olarak izlemek mümkündür.³⁷¹

Gözetim kameralarının bugünkü kapasitesine gelmesinde ve yaygınlaşmasında İngiltere'nin rolü büyüktür. 11 Eylül 2001 tarihinde Amerika'da İkiz Kulelere yapılan saldırı sonrasında İngiliz hükümetinin tüm ülkeyi 2,5 milyon akıllı kamera ile donattığı bilinmektedir. Bu kameralar 24 saat boyunca İngiltere sokaklarını izlemekte ve aranan suçluları tanıyarak polisi harekete geçirebilmektedir. Kameraların yakaladığı görüntüler, 24 saat boyunca oluşturulan özel izleme merkezlerine aktarılmakta ve bu izleme merkezlerinde, kameralardan gelen dijital görüntüler özel bir yazılım ile analiz edilip suç arşivlerindeki sabıka kayıtları ile karşılaştırılmaktadır. Akıllı güvenlik sistemi olarak ifade edilen bu sistemin saç ayaklarında gözetim kameraları, veri depolama merkezi, analiz yazılımı yer almaktadır. Bu yazılım, suç işleme eğilimindeki veya suç işleyen insanların davranışlarını analiz edebilmektedir. Böylece, gelen görüntülerde, suç işlemiş insan davranışı sergileyenler

³⁶⁹ Nigel Gilbert, *a.g.k.*, s.23.

³⁷⁰ Anthony C.Caputo, *a.g.k.*, s.7.

³⁷¹ *a.k.*, s.11.

şüpheli sıfatıyla izlenmekte; hatta güvenlik güçlerinin aradığı plakaya veya renk ve modele sahip araçlar birkaç saniye içinde tespit edilebilmektedir.³⁷²

Kameralı gözetim, her ne kadar minyatürleştirme ve gizleme yaygınlaşmaya başlasa da, gözetimin günümüzdeki en gözle görülür yüzüdür. Sokaklarda, özellikle İngiltere’de, kameralar alışılmış bir görüntü halini almıştır. Kameralar otobüslere, trenlere, taksilere, telefon kulübelerine ve asansörlere kadar girmiş durumdadır. Kuruldukları yerde yurttaşlar onların varlığını doğal karşılar hale gelmişlerdir. Hatta Stephen Graham’a göre günümüzde bunlar su, gaz, elektrik ve telefon gibi “beşinci bir kamu hizmeti” olmuştur.³⁷³

Kamerayla gözetim faaliyetlerinin varlığı dört ana gerekçe çerçevesinde ele alınabilir.³⁷⁴ Birincisi kameraların suç işleme konusundaki caydırıcılık gücüdür. Suç işlemeye meyilli şahıslar izlenme ve kaydedilme ihtimalinin farkına vardıklarında suç işlemekten vazgeçebilmektedirler. Günümüzde caydırıcı bir unsur olarak kamerayla gözetim gazinolardan, kamu taşımacılığına kadar hemen hemen her yerde kullanılmaktadır. Dünyadaki bütün ülkeler kamu taşımacılığı ve kamu alanları yoğunluklu olmak üzere kameraları kullanmaktadırlar. Yapılan kent araştırmalarına göre bu kameraların %86’sı hırsızlığın önlenmesi ve tespiti için, %39’u (içinde hırsızlık amacı olan da var) diğer adli suçları önleme amacı ile kullanılmaktadır.³⁷⁵

Kameraların suç önleme noktasındaki başarısı çevre şartlarına ve sistemin pasif, açık veya her ikisi modelinde olup olmadığına göre değişmektedir. Pasif sistemler, suç olduktan sonra suçun unsurlarının tespiti amacıyla kullanılan sistemlerdir. Aktif sistemler, başında birer güvenlik görevlisinin bulunduğu ve görevlinin bir anlık bile gözlerini kameralardan ayırmadığı sistemlerdir. Açık sistemler suç önleme noktasında daha başarılı olmaktadır. Nitekim buna dramatik bir örnek olarak Chicago’s Farragut Lisesi örnek gösterilebilir. Bu okul şiddet olayları, hırsızlık, kapkaç ve gasp olayları ile ünlü bir okul iken Kapalı Devre Kameralı Gözetim Sistemleri geldikten sonra daha önce işlenen suçlar yok denecek kadar azalmıştır. Birçok Amerikan şehri de aynı şekilde kameralı gözetim sistemlerine kavuştuktan sonra suç oranlarında gözle görülür oranda azalmayla karşılaşmıştır.³⁷⁶

Kamerayla gözetimin suçları caydırıcılığı noktasındaki verimliliğine dair Birleşik Krallık İçişleri Bakanlığı tarafından 2010 yılında gerçekleştirilen bir araştırma projesinde,

³⁷² Murat Erdal, *a.g.k.*, s.30.

³⁷³ David Lyon, *a.g.k.*, 2003, s.123.

³⁷⁴ Anthony C. Caputo, *a.g.k.*, s.2 - 3.

³⁷⁵ *a.k.*, s.1.

³⁷⁶ *a.k.*, s.2 - 3.

Amerika ve İngiltere'nin kamusal alanlarında yapılan 46 kamuoyu araştırmasında 22 tanesinin yayımlanacak kadar yeterli veriye sahip olduğu tespit edilmiştir ve bu 22 kamuoyu araştırması soygun, araç hırsızlığı, diğer adi suçlarda en az %50'ye varan oranlarda azalma olduğunu göstermiştir.³⁷⁷

Gerçek kamera sistemlerinin yanı sıra sahte kamera sistemlerini kullanan çeşitli şirketler ve kuruluşlar da bulunmaktadır. Bunlar da kısa vadede suç işlenmesi noktasında caydırıcı olabilmekte ve kameraları gören yurttaşlara kendilerini güvende hissetmelerini sağlayabilmektedir. Ancak bunun da şöyle bir dezavantajı bulunmaktadır; eğer sahte kamera sisteminin olduğu yerde bir suç işlenir ve bundan yurttaşlar zarar görürse kuruma açacakları davada kazanma oranları oldukça yüksek olabilmektedir. Ayrıca sahte kamera sistemlerinin toplumda iyice yaygınlaşması yurttaşlarda kameralı gözetim sistemlerine karşı güvensizlik duygusunun artması ve suç işlemeye meyilli olanlarda caydırıcılık etkisinin giderek azalması şeklinde netice verebileceği değerlendirilmektedir.³⁷⁸

İkincisi, kamera sistemleri suçla mücadelede ve suçları önlemede kaynakların etkili ve verimli kullanılmasında faydalı olmaktadır.³⁷⁹ Kamera sistemleri sayesinde suç yoğunluğunun anlık bölgesel analizi yapılabilmekte, böylece güvenlik personelinin görevlendirme yerleri maksimum fayda sağlayacak şekilde planlanabilmektedir. Bu bakımdan doğru personel ve malzeme planlaması yoluyla daha az maliyetle daha etkin koruma sağlanabilmektedir.

Kameraların varlığı, alan koruma görevlilerinin sayısının azaltılmasına veya kaldırılmasına imkan sağlayabilmektedir.³⁸⁰ Örneğin 2007 yılında Dallas Polis Teşkilatı 559 olayın aydınlatılmasında kameralı gözetimi kullanmış ve 159 tutuklama yapmıştır. Dallas Polis Teşkilatı yöneticileri bu olaylardan edindikleri tecrübeye göre tek bir polis memurunun kamera başında devamlı izleme yapmasının alanda görevlendirilen bir polis memurundan çok daha verimli olduğu sonucuna ulaşmışlardır. Zira kamera başındaki memur hem daha geniş alanı kontrol altında tutabilmekte hem de yaklaşık 300 metre öteden suçlu tespitinde kullanılmak üzere şahıs fotoğraflama yapabilmektedir.³⁸¹

Üçüncüsü kameraların giderek akıllı sistemlerle entegre çalışabilir hale gelmesidir. Bugünkü gözetim teknolojisinde artık kamera odasında devamlı bütün görüntüleri izleyen güvenlik görevlisinin bulunmasına gerek yoktur. Artık gelişmiş programlar sayesinde

³⁷⁷ a.k

³⁷⁸ a.k

³⁷⁹ a.k

³⁸⁰ a.k

³⁸¹ www.dallaspolice.net/dpd_crimereport.html, (Erişim Tarihi: 17.02.2013).

muhtemel suç unsurlarını, suç oluşma durumlarını sistem kendi izleyip, tarayıp analiz ederek görevliye haber verebilmektedir. Örneğin kırmızı araba geldiğinde uyarı verme, programa girilen şahıs eşkaline uygun olanların varlığının otomatik taranıp haber verilmesi, şüpheli hareketleri olanların bulunması gibi akıllı dijital formasyonlar yapılabilmektedir.³⁸²

Dördüncüsü kameraların tespit yeteneğinin yüksek oluşudur. Başarılı bir kamera gözetim sistemi ile suçluların veya suça meyilli kişilerin suçu işlemeyen önce veya suçu işledikten sonra hızlı bir şekilde tespiti mümkün olabilmektedir. Örneğin iki yüz bin kamerasıyla Londra, dört milyondan fazla kamerasıyla İngiltere, şüpheli şahısların otomatik takibe alınmasıyla ilgili olarak uygun yasal düzenlemeyi de kendi içinde gerçekleştirmiş olması sayesinde birçok suçluyu, intihar bombacısını, soyguncuyu tespit edip, takibe almış ve yakalamıştır.³⁸³ Hızla gelişen kamera sistemleri bünyesine yüz tanıma teknolojisi, retina algılama, plaka okuma, analiz gibi yeni nesil teknolojileri kattıkça aranan şahısları veya araçları anında tespit etme konusunda gittikçe mükemmelleşmektedir.

“Genç iri yapılı bir adam lüks mağazaya adımını atar atmaz kameralar hemen yüzüne odaklanıyor. Yüz hatları ve göz bebekleri analiz ediliyor. Sistem, veritabanından mağazaya giren kişinin kimliğini belirliyor. Hoparlörden “Hoş geldiniz Bay Brown” sesi yükseliyor. Bay Brown, evlilik yıldönümü için eşine bir hediye alıp apar topar mağazadan çıkıyor. Aldığı ipek giysinin üzerindeki radyo vericisi sürekli olarak uydulara Bay Brown’un hareketlerini bildiriyor... 4 dakika uzaklıktaki otoparka yürüyene kadar 6 kez kapalı devre güvenlik kameraları tarafından görüntülenen Bay Brown, eşini 1,5 saattir beklettiği için çok gergin ve acele ediyor. Teröristlerin şüpheli davranışlarını tanımaya programlı kameralar uyarı sinyali vermeye başlıyor. Bay Brown otomobile binince gaza yükleniyor ve 2 kez hız sınırını aşıyor. Hız kameraları Brown’un plakasını merkeze aktarıyor. Sistem, DNA ve kimlik veritabanını otomatik olarak inceliyor. Sonunda “şüpheli davranışlarda bulunan” Bay Brown’un terörist Bay Black ile 12 yıl önce lisede aynı sınıfta olduğu ortaya çıkıyor. Sistem alarm veriyor: Bay Brown saldırı hazırlığında olabilir! Polis, GPS sisteminden aracın konumunu belirliyor ve tek suçu eşini bekletmek olan Bay Brown yaka paça gözaltına alıyor.”³⁸⁴

Kameralı gözetim faaliyetlerinin toplumda sosyal, politik ve teknik olarak sorun oluşturan üç temel özelliği bulunmaktadır.³⁸⁵ Birincisi, kameralı gözetimin nesnesi kamu alanlarında dolaşan masum yurttaşlardır. Bu gözetleme durumu öncesinde halk tarafından kamu alanlarında hep birlikte güzel bir şekilde yaşanan “kamu mahremiyetini” yok etmektedir. İkincisi, yurttaşlar gözetimi kabul etme veya kabul etmeme konumunda değillerdir, bu hak onlara verilmemiştir. Bu durum yurttaşların sabah evinden çıkıp izlenmeden ve gözetlenmeden işine gitmesine engel olmaktadır.

Üçüncüsü, kamerayla gözetleme sistemleri hızla gelişim göstermektedir. Artık günümüzde bu sistemler, görüntü - ses kaydeden ve bunun yanında bireyleri tanıma sistemleri

³⁸² Anthony C.Caputo, *a.g.k*, s.2 - 3.

³⁸³ *a.k*

³⁸⁴ <http://www.vatanim.com.tr/root.vatan?exec=haberdetay&tarikh=06.11.2006&Newsid=92233&Categoryid=7>, (Erişim Tarihi: 18.02.2013).

³⁸⁵ Nigel Gilbert, *a.g.k*, s.23.

(yüz tanıma, plaka tanıma sistemleri) ile yeni dijital profillemeye sistemleri sayesinde bireylerin hal ve hareketlerine, duruşlarına göre yorum yapma - şüpheli ilan etme kabiliyetleri göstermektedirler.

Kamu kamera gözetleme sistemlerinin temel varlık sebebi potansiyel suçların işlenmesinde caydırıcı olmak, suçlar gerçekleştiğinde faillerin tespit edilmesi ve suçun işlenmesinin durdurulması olarak ifade edilmektedir. Ancak bunlar çoğu zaman trafik akışını izlemek gibi farklı amaçlar için kullanılmaktadır. Son zamanlarda da terörizmle mücadele amacı kameraların kullanım kapsamını genişletmiştir. Bu perspektiften sosyal faydalar bireysel hakların önüne geçmiş gözükmektedir. Halbuki ABD’de sokak kameralarının arttırılmasındaki kamu tutumları üzerine yapılan araştırmalarda giderek artan orandaki kameraların kamusal faydasının bu kadar büyük olmadığı ortaya çıkmıştır. Buna göre kameraların sayısının arttırılması sonrasında halktaki kendini güvende hissetme oranı eskisine göre daha azalmıştır. Zira eskiden varolan polis bekleme noktalarının ve karakolların halkın kendini daha çok güvende hissetmesini sağladığı ortaya çıkmıştır. Diğer taraftan halkın gözünde zencilerin ve erkeklerin yoğun olarak oturduğu mahallelerde kamera gözetleme faaliyetlerinin çok daha fazla yapıldığı, bu noktada ırksal ve cinsel bir ayırım algısının olduğu anlaşılmıştır.³⁸⁶

Gözetim faaliyetlerinin yapılması ve bunların kamerayla gerçekleştirilmesinin toplumsal anlamda yapısal bozukluklara yol açtığı; bu kameraların temel varlık sebebi olan güvenli ortam oluşturma açısından da halk nezdinde çok da başarılı olmadığı görülmektedir.³⁸⁷ Kameralı gözetim faaliyetlerinde sıradan yasalara uyan yurttaşlar da gözetime maruz kalmaktadır. Kameraların sadece “şüphelileri” değil, “bütün müşterileri”; “hırsızları” değil “bütün çalışanları” izlediği bir gerçektir. Bu durumun birinci sonucu bütün yurttaşlara “güvenilmez” yaftasının yapıştırılarak toplumsal bilincin zarar görmesi iken ikinci sonucu da herkesin özel hayatının gizliliğinin ihlal edilebilir olması algısının oluşturulmasıdır.

Masum yurttaşların özel alanlarına müdahale söz konusu olmadan gözetleme faaliyetleri yapılsaydı gözetim sistem ve teknolojileri daha kabul edilebilir bulunabilirdi. Şu an için masum yurttaşların özel alanlarına minimum seviyede müdahale kameraların saatlerce aralıksız gözetleme yapmaları yerine sadece şüphelenilen suç durumu ve şartlarında çalıştırılması veya şüpheli hareket ve durumlar olması durumunda otomatik devreye girmesi

³⁸⁶ Clive Norris, Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Berg Publishers, Oxford, 1999, s.10 - 11., akt., Nigel Gilbert, *a.g.k.*, s.34.

³⁸⁷ Nigel Gilbert, *a.g.k.*, s.34.

ile mümkün olabilir gözükmetedir. Bu şekilde kameraların sadece amacına yönelik kullanılmasının ve sıradan yurttaşların mahremine girmemesinin sağlanabileceği değerlendirilmektedir.³⁸⁸

Kamera gözetiminin temel dayanağı suçları önlemektir; fakat suç eğilimi ve riskini ortadan kaldırmak ya da azaltmak kamera kullanımıyla gerçekleşmez, bu sadece indirgemeci ve mekanik bir yaklaşımdır.³⁸⁹ Sineklerle mücadele etmek istiyorsanız sineklerin çoğalma ortamları ve nedenleri ile mücadele etmeniz gerekir. Suçla mücadele de buna benzemektedir. Suçla gerçek anlamda mücadele etmek isteniyorsa suçun oluşma şartları ve ortamları, nedenleri araştırılarak bunlarla mücadele etmek gerekir.

Günümüzde gözetleme kameraları kişileri hareket halindeyken bile şehir içinde takip edebilir duruma gelmiştir. Buna örnek olarak taksilerde uygulanan kamera gözetim sistemleri gösterilebilir. Örneğin; 2003 yılında San Francisco Taksiciler Federasyonu, San Francisco'daki tüm taksilere güvenlik kamerası yerleştirilmesine karar vermiştir. Bu uygulama San Francisco'da hem taksi şoförlerini hem de müşterileri oldukça rahatsız edici bir hale sürdüğünden taksi şoförleri kameraları kapatma ya da görüntü almasını engelleyici tedbirlere başvurmuştur. Bunun üzerine şehir yönetimi taksi kameralara zarar veren veya görüntü almasını engelleyenlere cezai yaptırıma başvurmuş ve taksiler üzerine şu uyarılar konulmuştur.³⁹⁰

“Taksiler üzerindeki kameralara zarar verdiğiniz takdirde 400 Dolar cezaya çarptırılacaksınız!
Güvenlik kameraları sizin korunmanız içindir!
Güvenlik kameraları suçun işlenmesinde caydırıcılık sağlar.
Kameralar sadece fotoğraflarınızı çeker, video çekimi yapmamaktadır.
Kameraların ses kayıt özelliği yoktur.
Sadece polis merkezindeki görevliler kameralardan çekilen fotoğraflara ulaşabilir.”

Taksi kameralar suç işlenmesinde caydırıcılık, müşterilerin güvenliğinin temini gerekçeleri altında yaygınlaştırılrsa da tüm taksilere kamera yerleştirilmesi, bunların bakımı, veri depolama, analiz program ve donanımlarının ortaya çıkaracağı maddi gelir, gözetim teknolojilerinin altında yatan kapitalist kaygıları bir kez daha ortaya koymaktadır. Ayrıca polisin suç şüphesi altında yer alanları izlemek amacıyla fiziki takip yapması için mahkemeden karar alabilmesi, şahsın suç işleyeceğine dair şüphe oranının kuvvetli olmasını gerektirirken, tüm yurttaşların fiziki takip edilir gibi nereden nereye gittiği, günlük konum

³⁸⁸ a.k, s.42.

³⁸⁹ İpek Görgün, a.g.k, s.16.

³⁹⁰ Donald N. Anderson, “The Spy in the Cab: The Use and Abuse of Taxicab Cameras in San Francisco”, *Surveillance and Society*, Sayı 10, 150 - 166. <http://www.surveillance-and-society.org>, (Erişim Tarihi:16.08.2013).

profilinin nasıl olduğunu bu kameralar sayesinde rahatlıkla takip edilebilir olması, fiziki takip için mahkeme kararı almada güvenlik güçlerinin şahsın suç işleyeceğine dair kuvvetli deliller getirmesi şartındaki özel hayatın gizliliğini ihlal etme kaygısı ile çalışmaktadır. Dolayısıyla güvenlik güçlerinin herhangi bir mahkeme kararı almadan tüm yurttaşları izleyebilmesinin önü açılmıştır.

Kameralı gözetim faaliyetlerinde en büyük tehlike ve kaygı verici durum, yurttaşların yani iktidar tarafından izlenen objelerin hangi sokakta, hangi otobüste, hangi dükkanlarda kameralarla kim tarafından ve hangi saatlerde izlendiğini bilmemesi, kendisine bildirilmemesidir.³⁹¹ Bireyin evden dışarı adımını attığında her an her taraftan kameralarla izlendiği düşüncesi, onun bilinç altında açık cezaevinde olduğu fikrini uyandırmaktadır ki bu durumun psikolojik, sosyolojik bir çok deformasyonu tetikleyeceği de aşıkardır.

Günümüzde kameralar genel nüfus içinde tehdit unsuru olarak görülenleri (azınlıklar, farklı din ve mezhep sahipleri, göçmenler vb.) kontrol altında tutmak amacıyla da kullanılmaktadır. Bu bakımdan siyasal otoriteye karşı toplumsal etnik bir hareketlenmenin olup olmadığının tespiti, etnik grupların liderlerinin belirlenmesi gibi siyasal örgütlenmeye özgü gayeler halk üzerinde siyasal dayatmacı bir baskıya dönüşmektedir. Bu tip faaliyetler farklı dile - dine - ırka mensup olan yurttaşların devlete olan bağlılığını arttırmaz; bilakis toplumun genelinden farklı dile, dine veya etnik kimliğe sahip olmasından dolayı kendisinin bir tehdit unsuru olduğunu hisseder, devlete ve otoriteye dair ne varsa hepsine olan güvenini zedeler. Bu noktada aslında kameralı gözetim faaliyetlerinin toplumsal ayrışmaya yol açtığı söylenebilir.³⁹²

2010 yılında İngiltere'nin Birmingham şehrinde Müslüman nüfusun oturduğu bir mahalleye 3 milyon pound ödenerek 200 kamera yerleştirilmiştir. Bu kameralar ilk yerleştirilirken polis yetkilileri mahalle sakinlerine araba hırsızlığı ve antisosyal davranışlarla savaşmak amacıyla böyle bir proje başlattıklarını açıklamıştır. Uzmanlar kapalı devre kamera güvenlik sistemleri, otomatik plaka okuma ve yüz tanıma kameraları ile terörizme yönelik tedbir alındığını iddia etmişlerdir. Ancak polis kuvvetleri daha sonra bu kameraları sökmüştür. Bunun nedeni de bu nüfus kesiminde kaybolan güvenin tekrar inşası olarak

³⁹¹ Nigel Gilbert, *a.g.k.*, s.49.

³⁹² "CCTV Aimed at Muslim Areas in Birmingham to Be Dismantled", *The Guardian*, 25 Ekim 2010, <http://www.guardian.co.uk/uk/2010/oct/25/birmingham-cctv-muslim-areassurveillance>, (Erişim Tarihi: 15.07.2013).

belirtilmiştir. Polis kuvvetleri suç ve terörle savaşmada bölge halkının güven ve desteğini kazanmanın kolluk kuvvetleri için en önemli şey olduğunu açıklamıştır.³⁹³

Alışveriş merkezlerinde veya dükkanlarda kullanılan güvenlik kameraları hırsızlığı önlemek gerekçesi ile günümüzde kuralsız bir şekilde yaygınlaşmıştır; artık güvenlik kamerası olmayan bir dükkana rastlamak istisna haline gelmiştir. Halbuki bu dükkanların, alışveriş merkezlerinin kameralarla donatılmasındaki gerekçe sadece hırsızlığı önlemek kadar masum değildir. Günümüzde alışveriş merkezlerindeki kameralardan elde edilen görüntü kayıtlarını kullanarak müşteri hareketlerini analiz eden program çeşitliliğinde de giderek artan bir yükseliş bulunmaktadır. Nitekim bu kamera - optik analiz programları sayesinde müşterilerin hareketleri, yüz ifadeleri, hangi reyonda ne kadar durdukları, günün hangi saatlerinde hangi etnik gruba mensup olanların geldiği gibi analizler yapılabilmekte ve bu analizlerin sonucunda pazarlama stratejileri geliştirilmektedir.³⁹⁴

Microsoft tarafından geliştirilmiş olan “*Kinect Sensör*” sistemleri alışveriş merkezlerindeki kameralardan elde edilen görüntü kayıtlarını kullanarak müşteri hareketlerini analiz eden programlara örnek gösterilebilir. Bu sistemler kendi ürün reklamlarında şu şekilde anlatılmaktadır.³⁹⁵

“Alışveriş merkezlerindeki veya süpermarketlerdeki gözetim sistemleri, genelde anormal davranışların tespiti amacıyla kullanılmaktadır. Biz, satışa sunulan kamera sistemlerimizi, alışveriş yaparken müşterilerin davranışlarını değerlendirerek onlara satış seçenekleri sunmak için dijital alışveriş asistanları olarak dizayn ettik. Bu dokümanda, insanların alışveriş merkezinde ürünlere olan yaklaşımları, genellikle aradıkları ürünler, ürünlere bakışları, alışveriş kartını eline aldıklarındaki tavırları gibi ürünlere karşı tepkilerini ölçebilecek, insan davranış profillerini ortaya koyabilecek bir sistemi size teklif ediyoruz.”

Kinect sensörü, insanların silüetlerini, temel hareket algılayıcısı ile onların ayırt edici tavırlarını ve hareketlerini tespit etmektedir. Bunları tespit ettikten sonra farklı sınıflandırma metotları, farklı istatistikler ile aralıksız çekilen silüetler arasındaki farklılıklar profillenmektedir. Neticede %80 oranında doğru sonuçlara ulaşılabilen analizler yapılmaktadır. Sistem; alışveriş merkezine yerleştirilen kameralar, *kinect* sensörü ve analiz programından oluşmaktadır.³⁹⁶

Kameralı gözetleme sistemlerindeki gelişmeler ışığında kameralarla dolu bir şehirde kayıt altına alınıp veri deposunda görüntü bilgilerinin saklanmadığını iddia edebilecek çok az kişi bulabilirsiniz. KDTS analog sistemlerinden dijital kamera sistemlerine geçişle birlikte

³⁹³ a.k

³⁹⁴ <http://www.videomining.com/technologies/main.html>, (Erişim Tarihi: 15 Temmuz 2013).

³⁹⁵ Mirela Popal, Alper Kemal Koç, “Kinect Sensing of Shopping related Actions”, s.1.

³⁹⁶ a.k, s.3.

kamera arkasındakilere iki avantaj doğmuştur. Dijital kayıt kapasitesi demek sınırsız kayıt ve kolay analiz yapabilmeyi ifade etmektedir. Dolayısıyla dijital kayıt sistemleriyle sınırsız sayıda yurttaş kayıt altına alınabilmekte ve bunlar arasında çok kısa süre içerisinde sorgulama yapılabilmektedir. İkincisi bu verilerin dijital ortamda kopyalanması da oldukça kolaydır ve dijital ortamda olan bu özel hayata ilişkin bilgilerin hep gizli kalabileceği garanti edilemez.³⁹⁷

Yukarıda ifade edilenler doğrultusunda kameraların bireysel yaşamda ve toplumsal düzende özellikle orta ve uzun vadede ortaya koyduğu zararlar oldukça fazladır. Günümüzde güvenlik politikalarında nasıl ki terörle mücadele önemli bir yer tutuyorsa önümüzdeki süreçte de kameralı yaşamın mücadele edilmesi gereken bir alana dönüşeceği değerlendirilmektedir. Zira er ya da geç insan haysiyetine zarar veren bu uygulamalara karşı toplumsal bilincin tepki vereceği düşünülmektedir.

1.2. Biometrik Gözetim

Biometrik gözetim; biyo - teknoloji, nöro - teknoloji, biometri, sinyal istihbaratı ve genetik mühendisliği gibi oluşumları içeren gözetim türüdür. Biometrik gözetim bilgi ve iletişim teknolojileri ile birleşerek, gözetimin kapsamının, yoğunluğunun ve şiddetinin artmasında etkili olmuştur.³⁹⁸ Biometrik gözetleme sistemleri özellikle 1990'lı yıllarda yaygın, etkin, ucuz bir şekilde üretilmeye ve kullanılmaya başlanmıştır. Süreç içerisinde bu sistemleri üreten şirketler, devlet kurumlarına, malibirimlere yönelik satış oranlarını yüksek oranda arttırmaya başlamıştır.³⁹⁹

Biometrik gözetleme sistemlerinin kullanılmaya başlanmasının nedenlerinden en önemlisi dolandırıcılık suçlarıdır. Dolandırıcılık suçlarına karşı etkili bir tedbir olarak biometrik kimlik tanımlama sistemleri kullanılmaya başlanmıştır. Batılı ülkelerde 1990'lı yıllarda kimlik kopyalama ve imza taklidi vakalarının çok oluşu nedeniyle özellikle sağlık sigortası dolandırıcılığı, çek dolandırıcılığının yaygın olduğu bilinmektedir.⁴⁰⁰ Bu nedenle kopyalanması zor olduğu düşünülen biometrik veriler imza ve kimlik tanımlayıcılarına alternatif olarak görülmeye başlanmıştır.

İnsan vücudundan alınan biometrik verilerin toplanıp, takip edilmesini Lyon “beden gözetlemesi” olarak ifade etmektedir. Buna göre bedenlere ait olan ya da bedenlerden alınan veriler, biometrik gözetleme için aranan en önemli şeydir. Beden, sadece bir veri kaynağı

³⁹⁷ Nigel Gilbert, *a.g.k.*, s.48.

³⁹⁸ Manuel Castells, *a.g.k.*, 2008, s.624.

³⁹⁹ Julie K. Petersen, *a.g.k.*, s.739.

⁴⁰⁰ *a.k.*, s.741.

olarak görülmektedir. Beden gözetlemesi faaliyetleri içerisinde başat rolü beden parçaları kullanarak kişinin kim olduğunu bulmak oynamaktadır. Bu noktada parmak izlerini oluşturan karışık çizgiler, elin geometrisi, başparmak ya da diğer parmaklar ve retinadaki koni ile çubuklar, ses modülasyonları, yüzün imgeleri ve bedenden alınan sıvılar beden gözetlemesinde kimlik tespiti için kullanılan en yaygın araçlardır. Biometrik verilerdeki gözetimin bu hakimiyeti bedeni, gözetlemenin alanı olmakla birlikte kaynağı haline getirmiştir.⁴⁰¹

Bedenler tarih boyunca şekli nasıl olursa olsun, her zaman gözlem altında olmuştur. Yüz sene öncesinde suç antrometresi, beden şekillerinin yasa dışı eğilimlerini açığa çıkarabileceğini iddia etmiştir. Bugün, biometrik teknolojilerin gelişimiyle bedenin kendisinin gözetleme verisi olarak soruşturulduğu ve sorgulandığı bir aşamaya gelinmiştir. Günümüzde artık bedenin davranışlarının ve nerede bulunduğunun takip edilmesi için açıkça klasik yöntemlerle fiziksel olarak izlenmesine gerek kalmamıştır. Gözetleme artık, kimlik belirlemek ve sınıflandırmak amacıyla izlemek, denetlemek, test etmek için derinin altına kadar inmiştir.⁴⁰²

Biometrik verinin bireyleri tanımlamada kullanımı iki şekilde olmaktadır. Birincisi, bir kişinin kimliğini kontrol etmek amacıyla kullanılabilir. Örneğin, kişinin parmak izi alınarak veritabanında kayıtlı parmak izleriyle karşılaştırarak veya pasaportta, kimlik kartında kayıtlı parmak iziyle karşılaştırmak suretiyle kişinin kimliği kontrol edilebilir. İkincisi, biometrik izlerden kişinin kimliği tespit edilebilmektedir. Örneğin, suç mahallindeki parmak izleri, parmak izi veritabanındaki parmak izleriyle dijital programlar vasıtasıyla karşılaştırılmak suretiyle kişinin kimliği tespit edilebilir.⁴⁰³

Biometrik kimliklendirmenin gerçekleşmesi için parmak izi, iris şekli gibi biometrik verilerin kopyalanamayacağına veya taklit edilemeyeceğinin garanti edilmesi gerekmektedir. Biometrik pasaport veya kimlik kartı gibi parmak izinin şeklinin net olarak gözüktüğü bir resimden “sakız parmak” (*Ing; gummy finger*) metoduyla parmak izinin taklit edilebildiği bilinen metotlardan birisidir. Bu metotta bir dijital okuyucu cihaz sayesinde parmak izi kopyalanabilmektedir ki bu kopyalanan parmak izinin cinayet işlenen bıçak üzerine bırakılabildiğini düşündüğümüz takdirde durumun vahameti gözler önüne serilmektedir.

⁴⁰¹ David Lyon, *a.g.k*, 2006, s.139 - 143.

⁴⁰² *a.k*

⁴⁰³ Nigel Gilbert, *a.g.k*, s.23.

Kopyalanan bu parmak izinin biometrik bankacılıkta kullanıldığı değerlendirildiğinde insanların hesaplarındaki paraların rahatlıkla çalınabileceği ihtimali de bir gerçektir.⁴⁰⁴

İnsanlar biometrik ölçü olarak ifade edilebilecek birçok kendine özgü biometrik verilere sahiptir. Örnek olarak parmak izleri, ayak parmak izleri, ses karakteristikleri, iris kalıpları, retina kalıpları, DNA genotipleri, yüz ölçüleri, koku karakteristikleri vb. gösterilebilir. Bütün bunlar şahsa münhasır özellik gösteren biometrik tanımlayıcılardır. Bütün bu veriler ölçülebilir, sayısallaştırılabilir, depolanabilir ve en önemlisi başka benzer biometrik verilerle karşılaştırılabilir. Bu verilerin takip edilmesi, kaydedilmesi, sayısallaştırılması, depolanması ve karşılaştırılması biometrik gözetlemeyi oluşturan faaliyetlerdir.⁴⁰⁵

En yaygın biometrik gözetim araçları şunlardır.⁴⁰⁶ Birincisi, yaşayan tüm canlılarda bulunan temel molekül olan DNA (*İng: Deoxyribonucleic Acid*)'dır. DNA genetik kodlarımızdan oluşan, bizim kişisel karakteristik özelliklerimizi, zayıf ve güçlü yönlerimizi, sağlık durumumuzu, atalarımızı, ırkımızı, yaşayan akrabalarımızı içeren biyolojik yapı birimidir. Bu önemli bilgileri barındıran DNA molekülleri vücudumuzdaki bütün hücrelere kodlanmıştır. Günümüzde bilim adamları vücudun kan, kıl, doku gibi parçalarından bu kodu büyük oranda çözmüştür. Dolayısıyla insanların vücudundan elde edecekleri bir parça ile DNA'nın içerisinde barındırdığı yukarıda belirtilen özellikler rahatlıkla açığa çıkarılabilmektedir.⁴⁰⁷

Diğer birçok gözetim şekilleriyle karşılaştırıldığında DNA'nın elde edilmesi ve değerlendirilmesi daha kolaydır. Bu bakımdan DNA çözümleme teknolojisi kişiler hakkında diğer bilgi toplama metotlarına göre oldukça kapsayıcı, elde edilmesi ve değerlendirilmesi kolay, önemli bir bilgi toplama metodudur. Nitekim günümüzde insanların telefonlarını dinleyebilmek için güvenlik biriminde çalışmak, belli hukuki şartların yerine gelmesi ve teknolojik imkanların olması gerekirken, DNA'sını çözümlmek istenilen her hangi birisinin saçından dökülen bir kıl veya vücudundan kopan bir deri kırıntısı elde etmek ve labarotuvara götürmek yeterlidir.⁴⁰⁸

Güvenlik güçlerinin doğum esnasında bebeklerden birer doku parçası alarak ülkedeki tüm insanların DNA verilerini toplayıp analize tabi tuttuğunu ve bu verinin veritabanlarında

⁴⁰⁴ a.k

⁴⁰⁵ Julie K. Petersen, *a.g.k.*, s.733.

⁴⁰⁶ a.k, s.734 - 735.

⁴⁰⁷ a.k, s.802 - 803.

⁴⁰⁸ a.k

saklandığında farklı bilgi toplama teknolojilerine gerek kalmadan tüm yurttaşların doğuştan itibaren fişlenebileceğini ve riskli olanların devamlı surette yoğun gözetime tabi tutulabileceğini düşündüğümüzde bu biyolojik verinin önemini ve kapsayıcılığını daha iyi anlayabiliriz. Nitekim günümüzde örneğin Hollanda’da dört yıl ve üzerinde hapis cezası alan suçluların hepsinin DNA’larının bir veritabanında muhafaza edildiği göz önüne alınınca doğum esnasında herkesin DNA’sının kaydedilerek dijitalize edilmesi çok da uzak gözükmemektedir.⁴⁰⁹ ABD’de 1992 yılından beri askerlik yapanların düzenli olarak DNA örnekleri alınarak depolanmaktadır.⁴¹⁰ Bu durum Türkiye gibi askerliğin zorunlu olduğu ülkeler için düşünüldüğünde ülkedeki tüm erkeklerin DNA verilerinin askeri güçler elinde depolanabileceği hazin bir gerçektir.

Günümüzde DNA verisinin sağlık taramalarında, bir takım hastalıklara hızlı müdahalede ve hastalıklardan korunmada sağladığı fayda oldukça önemli gözükmektedir. Mesela Haziran 2000’de açıklanan insan genomu taslak dizisiyle, tedavisi mümkün olmayan kalıtsal hastalıkların çözüme kavuşacağı; hatta hastalıklı embriyoların tespitinden sonra bunların genetiğinin değiştirilerek sağlıklı embriyolara dönüşümünün sağlanabileceği anlaşılmıştır.⁴¹¹ Fakat DNA verileri zamanla veritabanlarında toplanarak analize tabi tutulduğunda bunların bir sosyal ayrıştırma aracı haline de gelebileceği aşıkardır. Buna 1997 yapımı *Gattaca* filminde çizilen senaryonun güzel bir örnek teşkil ettiği düşünülmektedir. Filmde sosyal yaşamda ayrıcalıklı olan “Geçerliler” ile biyolojik bir alt sınıfı oluşturan “Geçersizler” arasında kalıtımsal bir ayrım tasvir edilmektedir.⁴¹²

DNA verilerinin bir sosyal ayrışma aracı olarak kullanılabileceği gerçeğinin yanı sıra toplanan bu biyometrik verilere kimlerin sahip olacağı, bu verilerin kimler tarafından hangi amaçlar için kullanılacağı, bu verilere sahip olanları kimlerin ve nasıl denetleyeceği de ortaya çıkacak diğer problemler arasında yer almaktadır. Sahip olunan DNA verileri, söz dinleyen ve itaat eden nesiller oluşturmak adına suistimal edilme tehlikesini barındırmaktadır. İnsan yaşamının ilk yıllarında, hatta daha yaşam başlamadan programlanan genlerle organizmalar mükemmellik isteği doğrultusunda düzenlenebilecek, böylece itaatkar ve toplumsal düzen için tehdit oluşturmayan organizmalarla ilerleyen aşamalardaki denetim ve gözetim faaliyetlerine olan gereksinim de ortadan kalkacaktır.⁴¹³

⁴⁰⁹ David Lyon, *a.g.k.*, 2003, s.63.

⁴¹⁰ *a.k.*, s.96.

⁴¹¹ Manuell Castells, *a.g.k.*, 2008, s.73 - 74.

⁴¹² David Lyon, *a.g.k.*, 2006, s.139 - 143.

⁴¹³ *a.k.*

İkinci biometrik gözetim aracı türü parmak izleridir. Parmak izi⁴¹⁴ en yaygın kullanılan biometrik tanımlayıcıdır. Genelde adli takibat amaçlı kullanılmaktadır. Buna göre olay yerinden elde edilen parmak izleri parmak izi veritabanındakilerle karşılaştırılarak eşleşenler tespit edilir. Böylece faillerin ve mağdurların kimlikleri tespit edilir, faillerle ilgili delillendirme yapılır ve suçun aydınlatılması sağlanır. Ayrıca bazı bankacılık işlemlerinde, kurumlara giriş - çıkışlarda, hapishane yoklaması almada kullanıldığı da bilinmektedir.⁴¹⁵

Parmak izlerinin üç temel özelliği bulunmaktadır.⁴¹⁶ Bunlardan birincisi parmak izlerinin değişmezlik - değiştirilemezlik özelliğidir. Ana rahmindeyken oluşan papillerin meydana getirdiği şekiller insan doğduktan sonra yaşam boyu ve ölüm sonrası eller çürüyünceye kadar değişmezler ve değiştirilemezler. Parmak izlerinin yok edilmesi ve değiştirilmesi amacıyla tahrip edilmeleri halinde kesilen bir tırnağın yeniden büyümesi gibi tahribatın yok olmasıyla birlikte papiller aynı şekilde tekrar belirirler.

İkincisi parmak izlerinin benzemezlik (aynı olmama) özelliğidir. Günümüze kadar yapılan incelemelerde birbirinin aynı olan iki parmak izi bulunamamıştır. Bir elde yan yana iki parmaktaki papil şekilleri, iki eldeki aynı cins parmakların izleri, tek yumurta ikizlerinin parmaklarındaki papil şekilleri hiçbir zaman birbirinin aynı değildir. Parmak izleri aynı olmadığı gibi birbirlerine de benzetilememektedir. Üçüncüsü parmak izlerinin tasnif edilebilirlik özelliğidir. Her insanın parmakları farklı karakterde izler taşımaktadır. Bu farklı karakterler sınıflandırılabilen ve aranması durumunda bulunulabilmektedir. Günümüzde gelişen teknoloji sayesinde parmak izleri artık bilgisayar ortamında sınıflandırılarak, karşılaştırma işlemleri yapılabilmektedir.⁴¹⁷

Parmak izlerinden şahısların; yaşına, sigara ya da uyuşturucu kullanıp kullanmadıklarına hatta kullandıkları bakım ürünlerine kadar bilgi edinilebilmektedir. Zira insanların bıraktıkları parmak izlerinin büyük bölümü, yağ molekülleri içermektedir. Bu yağ

⁴¹⁴ Parmak izleri, parmakların ilk boğumlarından itibaren olmak üzere, parmak uçlarında bulunan papillerin (papil, parmak uçlarının iç yüzeylerinde muntazam aralıklarla değişik desenlerde dizilmiş olan kabartma şeklindeki çizgilerdir) dokunulan cisimler üzerinde bırakmış olduğu izlerdir. Mustafa Kaygısız, *Adli Bilimler*, Seçkin Yayınları, Ankara, 2005, s.93.

⁴¹⁵ Julie K. Petersen, *a.g.k.*, s.734 - 735.

⁴¹⁶ Mustafa Kaygısız, *a.g.k.*, s.93 - 94.

⁴¹⁷ Parmak izlerinin sınıflandırılmasında bilgisayar teknolojisinin ulaştığı noktayı anlama açısından bu örnek olayı inceleyelim: “19 Aralık 1998 tarihinde İzmir-Ankara arasında tren seferi yapan İzmir Ekspresinde iki valiz içinde beş parçaya ayrılmış halde kimliği meçhul bir kadın cesedi bulunmuş, Ankara Emniyet Müdürlüğü Olay Yeri İnceleme Uzmanları tarafından cesetten alınan parmak izleri EGM Asayiş Daire Başkanlığı Merkez Parmak İzi Laboratuvarı tarafından AFIS (Otomatik Parmak İzi Belirleme Sistemi) programı kullanılarak 2.5 milyon adet parmak izi incelenmiş ve söz konusu parmak izlerinin Manisa’da bir gece kulübünde konsomatris olarak çalıştığı için arşivde parmak izi kaydı olan S.’ye ait olduğu tespit edilmiştir. Maktûlün kimliğinin parmak izi kaydı sayesinde tespitiyle birlikte cinayetin S’nin kocası M. tarafından işlendiği tespit edilmiştir.” Mustafa Kaygısız, *a.g.k.*, s.94.

molekülleri çocuk, yaşlı ya da yetişkinlerde farklılaşır. Böylece yağ moleküllerinden şahısların karakteristik izlerini sürmek mümkündür.⁴¹⁸

Biometrik verilerin kaydedilmesinin ilkel formları yüzyıllar öncesine dayansa da modern zamanlarda biometrik tanımlamanın en bilinen şekli şüpheli ve suçlu şahısların tanınması için parmak izlerinin alınması şeklinde olmuştur. Bugün ABD ve Avrupa adli tanımlama amacıyla yıllardır topladığı parmak izlerini, analize ve çevrimiçi sorguya uygun olacak şekilde, farklı veritabanları ile de ilişkili olarak tek bir veritabanında toplamıştır. Bundan dolayı artık suç mahallinde veya istihbari amaçlı olarak tespit edilen bir parmak izinin kime ait olduğunu tespit etmek için bu veritabanlarından birkaç saniyede sorgu yapılabilmektedir.⁴¹⁹

Her ne kadar parmak izi halkın anladığı ve bildiği suç ve adli amaçlar için kullanılsa da bunun yanı sıra özellikle ABD ve Avrupa'da yasa dışı göç ve giderek büyüyen siyasi sığınmacı kontrolleri için de kullanılmaktadır. ABD ve Avrupa'da parmak izi toplanması faaliyetleri oldukça yaygındır ve araç sahipleri, sınırdan girip - çıkanlar, herhangi bir kulüp - dernek üyeleri parmak izlerini gönüllü olarak vererek merkezi parmak izi veritabanında toplanmasına müsaade etmektedir. Bu bakımdan veritabanına parmak izini vermeyi kabul eden normal yurttaşlara yurtdışı giriş - çıkışlarda kolaylık gibi bazı imtiyazlar da tanınabilmektedir.⁴²⁰

Üçüncü biometrik gözetim türü avuç izleridir. Parmak izlerinde görülen papil çizgilerinin karakteristik özellikleri avuç izinde de mevcuttur.⁴²¹ Çok yaygın olmamakla beraber kapı tanıma sistemlerinde ve adli amaçlı olarak kullanılmaktadır. Dördüncüsü ayak ve ayak parmağı izleridir. Bazı hastanelerde yeni doğan çocukları tanımlamak, kaydetmek amacıyla ve bazen suçun aydınlatılmasında kullanılmaktadır.⁴²² Beşinci biometrik gözetim türü iris taramalarıdır. Kişinin gözünün renkli kısmının teknolojik cihazlarla görsel olarak taranmasını ifade eder. Genelde korunaklı yerlere (istihbarat servisleri vs.) giriş - çıkış için kullanılmaktadır.⁴²³ Fakat sokaklardaki kameralardan iris tanımlaması yapmaya yönelik çalışmalar da bulunmaktadır.

İris taramaları, kısmen pozisyon araçlarını ve ışınlarını dağıttıkları için, otomasyonlu banka makineleri tarafından tercih edilmektedir. Müşteri geldiği zaman, videolar, kişiyi şekil

⁴¹⁸ <http://www.yasanacakdunya.net/index.php?URL=kategorie&id=1023>, (Erişim Tarihi: 25.03.2013).

⁴¹⁹ David Lyon, *a.g.k.*, 2003, s.60.

⁴²⁰ *a.k*

⁴²¹ Mustafa Kaygısız, *a.g.k.*, s.102.

⁴²² Julie K. Petersen, *a.g.k.*, s.734 - 735.

⁴²³ *a.k*

olarak belirlemek için yakın çekime geçer ve kişinin koordinatlarını belirler. Bir metre uzaktan, dosyadaki dijital olarak şifrelenmiş imgeyle karşılaştırılmak için, bir göz imgesi alınır ve birkaç saniye içinde eşleşme tamamlanır. Japonya'daki OKI Elektronik Endüstrisi ve İngiltere'nin Londra şehrindeki NCR Bilgi Laboratuvarı iris tarama araçlarını uygulayanlar arasındadır.⁴²⁴

Altıncı biometrik gözetim türü retina taramalarıdır. Gözün arka tarafında bulunan retina kısmının teknolojik cihazlarla görsel olarak taranmasını ifade etmektedir. Retina taramaları iris taramalarına göre daha zordur ve kişinin gözünü retina tarayıcıya iyice yaklaştırmasını gerektirir. Bazı kurumlarda kapı giriş - çıkışlarında kullanılmaktadır.⁴²⁵ Lyon'a göre retina taramaları en doğru kimlik belirleyicileridir; fakat genelde diğer biometrik doğrulayıcılarla birlikte kullanılmaktadır. Örneğin CIA, Virginia Langley'deki en üst düzey korumalı bilgisayar kasası için retina tarayıcılarını ses izleriyle beraber kullanmaktadır. Kişi, gözün üzerinden kırmızı bir ışık huzmesi geçiren ve makinenin yanında olan bir tabakaya yüzünü yapıştırmak zorundadır.⁴²⁶

Sekizinci biometrik gözetim türü ses izleridir. İnsanın ses karakteristiği ayırt edicidir ve her insanda tektir. Bu bakımdan gelişmiş teknolojiler vasıtasıyla sesin kime ait olduğu rahatlıkla tespit edilebilmektedir. Diğer taraftan kişinin duygusal özelliklerini ve değişkenlerini tespit etmede de kullanılmaktadır. Bu amaçla bazı ülke mahkemelerinde yalan makineleri kullanılmaktadır.⁴²⁷ Dokuzuncu biometrik gözetim türü yüz izleridir. Göz - burun - kulak - çene aralarındaki "altın oran" olarak ifade edilen ölçüler kişiye özeldir ve ayırt edicidir. Kameralarla entegre olarak yüz tanıma sistemleri ile hedef şahıs veya şahısların nerede olduğu, nerelere gittiğini tespit etme amacıyla İngiltere, ABD gibi gelişmiş ülkeler tarafından güvenlik amaçlı olarak kullanılmaktadır.⁴²⁸

Biometrik tanımlayıcı olarak ifade edilen bedene ait olan verilerin temin edilmesi, depolanması, analiz edilmesi esasında "vücut bütünlüğü" hakkının ihlali anlamına gelmektedir. Örneğin, trafikte alkol ve uyuşturucu testi yapılması bile basit anlamıyla vücut bütünlüğü hakkının ihlali iken mahkemeler bu uygulamayı haklı bulur hale gelmiştir. Diğer taraftan günlük hayatımızda sıklıkla karşılaştığımız X-Ray kontrolünden geçirilme, vücuda bir takım ışınların çarpıp geri dönmesiyle oluşan uygulamadır. Burada vücut bütünlüğü iki

⁴²⁴ David Lyon, *a.g.k*, 2006, s.165.

⁴²⁵ Julie K. Petersen, *a.g.k*, s.734 - 735.

⁴²⁶ David Lyon, *a.g.k*, 2006, s.165.

⁴²⁷ Julie K. Petersen, *a.g.k*, s.734 - 735.

⁴²⁸ *a.k*

şekilde ihlal edilmektedir. Birincisi vücuda çarpan bu ışınlar insan sağlığı için tehlike arz etmektedir ve insan vücudunda kanserojen hücrelerin gelişmesine yol açabilmektedir. İkincisi, X-Ray cihazında insanın biometrik fotoğrafının çekilmesidir. Bu biometrik fotoğrafta kişinin vücudunun genel hatları ortaya çıkmaktadır.⁴²⁹

Bazı ülkelerde işe alım esnasında kadınlar gebe olup olmadıklarını anlamaya yönelik kan ve idrar örnekleri alınarak teste tabi tutulmaktadır. Örneğin, Amerika’da 1990’ların sonunda, Kaliforniya’daki Lawrence Berkeley Ulusal Laboratuvarı, işe alınmadan önce yapılan sağlık testleri için alınan kan ve idrarın, frengi ve gebelik (kadınlar için) testlerini yapmak amacıyla kullandığını öğrenen yedi işçi tarafından dava edilmiştir. Müracaat edilen mahkeme, bu tip testlerin, çalışanın iş konusundaki kabiliyeti üzerinde doğrudan etkisi olmadığı durumlarda, testin kişinin izni olmadan yapılamayacağı sonucuna varmıştır.⁴³⁰

Günümüzde özellikle Avrupa Birliği üyesi ve aday ülkelerde uygulanan biometrik pasaportlar da biometrik gözetim güncel bir örnektir. Bu pasaportlar dijital olarak kaydedilmiş biometrik verileri içermektedir. Genelde bu veriler “biometrik fotoğraf”⁴³¹ ve dijital parmak izini içermektedir. Gelecekte iris şablonlarını da içermesi planlanmaktadır. Bütün bu veriler pasaport üzerinde olduğu gibi merkezi bir sistemde de depolanmaktadır.⁴³²

Burada iki sorun ortaya çıkmaktadır. Birincisi bu bilgilere pasaport kontrolündeki memur haricinde üçüncü şahısların da ulaşabilme ihtimalidir. İkincisi pasaport çalındığında veya kaybedildiğinde bu önemli bilgilerin tehlikeli şahısların eline geçmesi olasılığının varlığını sürdürmesidir. Böylece dolandırıcılık gibi suçlarda bunlar kullanılabilir, hatta suç mahallinde bu kişilerin parmak izleri bırakılarak iftira suçu işlenebilecektir. Biometrik verilerin korunmasına yönelik olarak şifreleme ve kodlama sistemleri geliştirilse bile bu bilgilerin bulunduğu merkezlerin kodlarının bilgisayar korsanlarınca illegal yollardan elde edilmesi söz konusu olabilecektir.⁴³³

Sonuç olarak şu ifade edilebilir ki biometrik verilerin gözetim faaliyetlerinde kullanılmaya başlanmasıyla birlikte artık bedenler sayısal birer değere dönüştürülmüş ve gözetim faaliyetlerini yürüten analizcilerin önünde analize hazır birer veri konumuna indirgenmiştir. Bedenden çıkarılan tüm somut veriler (parmak izi, el geometrisi, retina taraması, ses modülasyonları, yüz taraması, beden sıvıları vs.), bürokratik dosyalar veya

⁴²⁹ David Lyon, *a.g.k.*, 2003, s.68.

⁴³⁰ David Lyon, *a.g.k.*, 2006, s.162.

⁴³¹ Biometrik fotoğrafta bütün resim arka planda sayısallaştırılmaktadır.

⁴³² Nigel Gilbert, *a.g.k.*, s.21.

⁴³³ *a.k*

dijital belgelerde soyutlaşarak, her an kullanılmaya hazır biçimde bekletilirler. Gözetim faaliyetlerinin bu kadar ilerlemiş olması orta vadede büyük tehlikelerin sinyali vermektedir. Bu tehlikelerin en büyüğü şüphesiz insanın dijitalleştirilmesi ya da Lyon'un tabiri ile "kaybolan bedenler"⁴³⁴ problemidir. Diğer taraftan biometrik verinin veri tabanları arasında dolaşması ve şirketler arasında alınıp satılması ile neo - kölelik olarak ifade edebileceğimiz bedenlerin köleleştirilmesi tehlikesi de yadsınamaz bir gerçektir.

III. GÖZETİME DAİR ELEŞTİREL BİR DEĞERLENDİRME

Gözetim teknolojilerinin görünürde sağladığı faydalar insanları, kurumları cezbedebilmektedir. Ancak ne gözetim teknolojilerini oluşturan ve satan kapitalist düzen temsilcilerinin, ne bu teknolojileri kullananların, ne de bu teknolojilerin hedef kitlesinin cevap veremediği tek soru gözetimin ezici gelişim evreninde mahremiyetin ne olacağıdır. Gözetim teknolojileri ile ilişkili olarak ihlal edilen temel mahremiyet konusu kişisel veridir. Kişisel veriler kişilerin mahremiyetleri yok sayılarak toplanıp depolanabilmektedir. Kişisel veri içinde bir gerçek kişinin adı, soyadı, doğum tarihi, doğum yeri, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, fotoğrafları, görüntü ve ses kayıtları, parmak izleri, genetik bilgileri, IP adresi, e-posta adresi, cihaz kimlikleri, hobileri, tercihleri, etkileşimde bulunduğu kişiler, grup üyelikleri, aile bilgileri gibi kişiyle özgü olan veriler sayılabilir.⁴³⁵

Gözetim toplumu süreci özel hayatların gizliliğine; yani kişilerin mahremiyetine bir darbe indirmiştir. Zira gözetim teknolojilerindeki gelişmeler paralelinde veri toplama ve bunları otomatik olarak işleme imkanlarındaki hızlı artış, bununla birlikte verilere erişim, paylaşım ve transfer maliyetlerindeki ucuzluk, kişisel verilerin ticari metaya dönüşmesi kişisel verilere olan ilgiyi arttırmıştır.⁴³⁶ Dolayısıyla bireye ait olan özel alanda geçmişe oranla ciddi daralmalar meydana gelmiştir.

Yukarıda da ifade edildiği üzere kişisel verileri toplama arzusu bireye rağmen hızla artmaktadır. Ekim 2012'de Kaliforniya Üniversitesi'nde yapılan bir araştırmaya göre ülkede en sık girilen 100 internet sitesinde toplamda yaklaşık 5000 civarında internet takip dosyasının olduğu tespit edilmiştir.⁴³⁷ Bu internet takip dosyaları, siteleri ziyaret edenler farketmeden onların bilgisayarlarına sızmakta ve internette giriş yaptıkları siteler, internet

⁴³⁴ David Lyon, *a.g.k.*, 2006, s.56 - 57.

⁴³⁵ TC. Cumhurbaşkanlığı Devlet Denetleme Kurulu, *Denetleme Raporu*, Sayı 2013 / 3, 27.11.2013, s.778.

⁴³⁶ *a.k.*

⁴³⁷ Seeta Pena Gangadharan, "Joining the Surveillance Society", *New America Foundation*, Eylül 2013, s.2. <http://newamerica.net>, (Erişim Tarihi 15.12.2013).

üzerindeki mesajlaşma, yorum yazma gibi faaliyetleri ile ilgili olarak haklarında profillemeye yapmaktadırlar. Bu örnekte görüldüğü üzere kişisel verilere ulaşmak için veri avcıları her türlü yolu denemektedirler.

Gözetim faaliyetlerinin günümüzde sahip olduğu teknik imkanlar ve yandaşları sayesinde varlığı toplumsal bilinçte normalleşmiştir. Esasında gözetim faaliyetleri hayatın rutini içinde kendini gün geçtikçe meşrulaştırmaktadır. Bu bölümde yaygınlaşan gözetim faaliyetlerinin bireysel ve toplumsal olumsuz etkileri incelenecek; akabinde de toplumsal fayda açısından olumlu olarak değerlendirilebilecek olan sonuç ve etkilerinden bahsedilecektir.

Bu bölümde mahremiyet kavramı özel hayatın gizliliği ölçeğinde incelenecek, gözetim faaliyetlerinin mahremiyeti sıradanlaştırması paralelinde oluşturduğu toplumsal ve bireysel büyük zarar ortaya konulmaya çalışılacaktır.

1. Topluma Bakan Yönüyle Gözetim Tartışması

“Yanlış hayat doğru yaşanmaz”⁴³⁸
Adorno; 1998

Gözetim faaliyetlerinin yoğunlaşması neticesinde meydana gelecek toplumsal değişimi Foucault “norm toplumu” olarak ifade etmektedir.⁴³⁹

“...Yasanın iktidarının gerilemekte değil, çok daha genel bir iktidara dahil olmakta olduğu bir toplum türüne girdik: Kabaca, norm toplumu. Ceza kurumunun, ortaya çıkmasını gerektiren edimi - hüküm vermek – günümüzde mevcut haliyle kabul etmekte ne kadar güçlük çektiğine bir bakın. Sanki bir suçu cezalandırmanın hiç anlamı yokmuş gibi suçlu giderek hastayla özdeşleştirilmekte, mahkumiyet ise bir tedavi reçetesi yerine geçmektedir. Bu esas olarak yasaya dayanan bir hukuk toplumu olmaya son vermekte olan bir toplumun karakteristik özelliğidir. Esas olarak norma dayalı bir toplum haline gelmekteyiz. Bu toplum çok daha başka bir gözetleme ve kontrol sistemi gerektirir. Bitip tükenmeyen bir görünürlük, bireylerin sürekli sınıflandırılması, hiyerarşikleştirme, nitelendirme, sınırların oluşturulması, teşhis koyma. Norm, bireyleri bölümlere ayırmanın ölçütü halini alır. Oluşmakta olan toplum bir norm toplumu olduğu anda, normalin ve patolojik olanın en üstün bilimi olan tıp, bilimlerin kraliçesi olacaktır...”

Gözetimin toplumsal etkilerinden en büyüğü ırksal, sınıfsal kategorilerde toplumsal ayrışmayı körüklemesidir. Zira günümüz gözetim ilişkileri insanları risk durumlarına ve değerlerine göre kategorilere ayırmaktadır. Esasında derin bir ayrışma gözükmektedir ki bu

⁴³⁸ Theodor W. Adorno, *Minima Moralia*, Çev. O. Kolçak, A. Doğukan, Metis, İstanbul, 1998, akt., Gamze Yücesan Özdemir, *a.k.*, 2008, s.8.

Gözetimin her ne kadar olumlu ve olumsuz sonuçları olabileceği ifade edilse de kökten yanlış olan, temelleri sakat ve çıkış noktasında bireyi iktidarın hakimiyeti altına alma gayesiyle yapılan gözetim faaliyetlerinin ortaya çıkarabileceği faydalar batıl olmaya mahkûm olduğu ifade edilmek istenmiştir.

⁴³⁹ Michel Foucault, *a.g.k.*, 2003, s.77 - 78.

nedenle gözetimi sadece kişisel özel yaşamın değil aynı zamanda sosyal adaletin de bir meselesi olarak görmek gerekmektedir.

Toplumsal ayrışma konusunda 1993 yılında Oscar Gandy “panoptik çeşitlilik” kavramını kullanarak özellikle müşteri - tüketici gözetimi konusunda yapılan takibata dikkatleri çekmiştir. Bu bağlamda çok alışveriş yapanların veya maddi açıdan iyi durumda olanların neleri daha fazla satın aldıklarına dair bir gözetim faaliyetinin yürütüldüğünü bunun da toplumda sınıfsal ayrışmaya neden olduğunu açıkça ortaya koymuştur.⁴⁴⁰

Sınıfsal ayrışmaya din ve ırk faktörlerinde atılan ayrılıkçı adımlar da eklenirse durum daha da tehlikeli olmaktadır. Örneğin; 2006 tarihli İngiltere İç Güvenlik Bakanlığı verilerine göre İngiltere’de güvenlik ve önleme aramalarına veya alkollü araç kullanma kontrol durdurmalarına zencilerin diğer beyazlara göre maruz kalma oranı altı kez daha fazladır.⁴⁴¹ Bu durum toplumda devletin yurttaşlarına eşit mesafede yaklaşmadığının bir göstergesi olarak tarihe geçmiştir.

11 Eylül 2001 terörist saldırılarından sonra özellikle Batı ülkelerinde uçuş bilgilerinde Arap veya Müslüman olan ya da bütün ülkeye gelen yabancılarla ilgili yapılan ayrıntılı istihbari analiz çalışmaları neticesinde kökeninde Araplık veya Müslümanlık olanların havaalanlarında veya sınırlardaki kontrol noktalarında ayrı muamele altına alınıp, sürekli gözetime tabi tutulması veya bir Arap ülkesine giden Yahudi kökenli birisinin riskli görülüp hemen gözetime tabi tutulması gözetimin oluşturduğu ayrışmaya örnek gösterilebilir.⁴⁴²

Gözetim toplumunda toplumsal ayrışma adeta bir salgın hastalık gibidir. Devlet ve ticari kurumların çok geniş olan kişisel bilgi veritabanlarında; terörist gruplar, riskli toplumsal gruplar, hedef alıcı (ticari satışlarda) kitle veya hedef pazar grubu gibi sınıflandırmalar yapılagelmektedir.⁴⁴³ Tüketici gözetimi alanında “amazon.com” gibi bir şirketin müşterilerini profilemek için oldukça gelişmiş veri elde etme teknikleri kullandığı ileri sürülmektedir. “Amazon.com” birisiyle ne kadar çok ilgileniyorsa o kişi hakkında o kadar çok bilgiye sahiptir demektir. Örneğin, bu siteden kişiye ne kadar çok elektronik posta veya cep telefonu mesajı gönderiliyorsa o kişiyle ilgili şirketin veritabanında o kadar çok kayıtlı bilgi bulunmaktadır.⁴⁴⁴

⁴⁴⁰ David Lyon, “Surveillance as Social Sorting: Computer Codes and Mobile Bodies”, *Surveillance as Social Sorting*, Ed. David Lyon, Taylor and Francis e-Library, New York, 2005, s.2.

⁴⁴¹ Home Office, *Operational Policing – Impact: about the Programme*, 2006, viiii.

<http://police.homeoffice.gov.uk/operationalpolicing/impact/impact-about-the-programme/>, (Erişim Tarihi 15.05.2013).

⁴⁴² Oscar Gandy, *The Panoptic Sort: A Political Economy of Personal Information*, Westview Press, Boulder, 1993., akt., David Murakami Wood, *a.g.k*, 2006, s.8.

⁴⁴³ *a.k*

⁴⁴⁴ David Murakami Wood, *a.g.k*, s.8.

Bu durumun şöyle bir dezavantajı vardır. Eğer veritabanına bir kere girmişseniz oradan çıkmanız, yani silinmeniz oldukça zordur ve size ait verilere başkaları da bakabilir veya başka şirketlere bu veriler satılabilir. Bu süreçte bireyin kendi bilgisine dair hiçbir müdahale şansı da bulunmamaktadır.

Sosyal ayrışma aslında gözetim toplumunu açıklayıcı bir durumdur. Gözetim toplumlarında farklı gruplara farklı imkanlar sunulur ve böylece toplumdaki demokratik hava yok edilir. Bazı grupların oturduğu semtlerdeki gözetim faaliyetleri onların kitlesel özel alanlarını tamamen yok ederken başka bir toplumsal grubun oturduğu semtte gözetleme faaliyetleri yapılmamaktadır. Bu durum da toplumda “onlar ve bizler” ayrımının yapılmasına ve dolayısıyla toplumsal ayrışmanın körüklenmesine neden olmaktadır.⁴⁴⁵

Gözetimin önemli sonuçlarından birisi de kendi meşruiyet temellerini toplum nezdinde oluşturmaktır. Böylece gözetime olan toplumsal tepkilerin önüne geçmiş olur ve aynı zamanda halkı kendisinin toplum için vazgeçilmez nitelikte olduğuna dair ikna eder. Gözetimin bu güçlü toplumsal meşruiyet dayanakları teknoloji - toplum arasındaki ilişkiden kaynaklanmaktadır. Zira özellikle günümüzde toplum tarafından bütün teknolojilere devrimsel ve olması gereken gelişmeler olarak bakılmaktadır. Ayrıca yeni dünya düzeninde lider ülke veya merkez ülkelerden olma da bu teknolojik gelişmelere sahip olma ve bunları kullanma oranları ile ölçülmektedir. Bu kapsamda gözetim teknolojileri de teknolojik gelişme olarak değerlendirilmekte ve bu görüşlerin potasında erimekte, toplum nezdinde normalleşmektedir.⁴⁴⁶

Kişî ve kurumlar gözetim teknolojilerinin varlığını o kadar çok kabullenmişlerdir ki artık bu teknolojilerin bulunmadığı bir çevreyi ekonomik ve sosyal anlamda bir güvensizlik ortamı olarak değerlendirmektedirler. Genelde uzun vadede gözetim teknolojilerinin ortaya çıkardığı ve çıkaracağı zararları çoğu kişi görmezden gelmekte, daha çok kısa vadede onlardan elde edeceği faydaya bakmaktadır.⁴⁴⁷

Gözetimin sosyal kabul ve sosyal dışlanma gibi iki vechesi bulunmaktadır. Bir yurttaş olarak toplumun parçası olmak istiyorsanız gözetlenmeyi de kabullenmek zorundasınızdır (resmi makamlara adresinizi, sağlık bilgilerinizi bildirme zorunluluğu, vergi numarası alma zorunluluğu vb.) ve bunun karşılığında yurttaş olmanın sağladığı imkanlardan da faydalanabilirsiniz (seçme ve seçilme imkanı, sağlık imkanları, sosyal imkanlar vb.). Buna

⁴⁴⁵ a.k

⁴⁴⁶ William G. Staples, *a.g.k.*, s.130.

⁴⁴⁷ a.k

karşın gözetlenmek istemeyen ve gözetimden kaçan kişi için zorluklar baş gösterecek ve bu kişi toplumda disiplini sağlamak isteyen kurumların dikkatini çekecektir. Esasında bugünün dünyasından kendini soyutlamak demek “tehlikeli şahıs”, “şüpheli şahıs”, “tehdit unsuru”, “yabancı” olarak gözetim odaklarının merkezine daha çok oturmak demektir. Kısacası günümüz dünyasında kişi ya kendi isteğiyle gözetlenmeye razı olacaktır ya da kendisi istemese de zaten gözetlenecektir.⁴⁴⁸

Gözetimin doğrudan bireye etki eden sonuçlarından en önemlisi bireyi hayatın öznesi olmaktan çıkarıp dijital işlemlerin ya da gözetleme faaliyetlerinin konusu olan dijital bir kod, sayı veya takip edilmesi gereken bir nesneye dönüştürmesidir. Lyon’a göre gözetlenen toplumların yükselişi bütünüyle kaybolan bedenlerle ilgilidir. Bir şeyleri uzaktan gerçekleştirdiğimiz zaman, bedenler yok olur.⁴⁴⁹ Bir telefon açmak sesle iletişim kurmak anlamına gelir; ama elektronik posta gönderdiğimiz zaman, bu tip somutlaştırmanın izi bile kalmaz. Nitekim gülen yüzler gibi harf karakterleriyle belirlenmiş sembollerin, görülmeyen yüzün yerine geçmesi bundan dolayıdır. Özellikle bilgisayar tabanlı veri iletişimde ilişkilerin çoğunluğunda somutlaştırılmış kişiler yok olmuştur.

Gözetleme faaliyetleri kapsamında bazı durumlarda tüm ülkeyi saran şekilde konuşlandırılmış kamera sistemleri aracılığı ile hedeflenen şahısların hareketleri, birlikte hareket ettikleri diğer şahıslar devamlı surette izlenebilmektedir. Fakat bu durumda gözetlemeyi yapanın karşısındaki bir birey değildir; bilgisayar oyunlarında olduğu gibi belki bir oyun karakteridir, ya da dijitalize olmuş isim soy isimidir. Uydu üzerinden yapılan gözetlemelerde adeta tüm insanlar, üç boyutlu bir oyunun dijital karakterleri haline dönüştürülür.

Gözetim altında bulunmayı mahremiyet ihlali olarak görmeyenler için gözetimin pozitif ve üretici yanları ağır basmaktadır. Gözetimin bu pozitif ve üretici yanları aslında gözetimin toplumsal meşruiyet kaynaklarını oluşturmaktadır. Bu kısımda gözetimi meşrulaştıran bu pozitif yanların neler olduğu incelenecektir.

Gözetim teknolojileri sayesinde devlet kurumlarının birbirleri ile olan ilişkilerinin daha hızlı, kontrollü ve etkin olacağı, böylece kamu kaynaklarının etkin ve verimli kullanılabileceği ifade edilebilir. Yurttaş herhangi bir devlet dairesine gittiğinde bürokratik işlerinin birçok evrak ve kırtasiye işlemi olmaksızın, “bugün git yarın gel” anlayışı olmadan

⁴⁴⁸ Kirstie Ball, Frank Webster, *a.g.k.*, s.12.

⁴⁴⁹ David Lyon, *a.g.k.*, 2006, s.33 - 34.

hızlı bir şekilde halledildiği görülmektedir.⁴⁵⁰ Örneğin, Türkiye’de PTT’den e-Türkiye şifresi aldığınız takdirde dava takibinden tutunda yurt dışından getirdiğiniz cep telefonun IMEI’sini pasaporta işletme işlemine kadar birçok işlemi hiçbir kamu görevlisi ile muhatap olmadan internet üzerinden halledebilirsiniz.

Gözetimi meşrulaştıran en önemli alan toplumsal güvenliğin sağlanmasıdır. Güvenlik birimleri için güvenlik kontrollerinde şahsın sabıka kaydının olması, hakkında yakalama kararının bulunması, daha önce suça karışmış olan şahıslarla irtibatının olması gibi çeşitli risk faktörleri önem arz etmektedir.⁴⁵¹ Yurttaşlar herhangi bir polis yol uygulamasına maruz kalabilir veya polis merkezine herhangi bir nedenden ötürü gelebilirler. Bu durumda şahısla ilgili yapılacak ilk şey onun hakkında yukarıda ifade edilen tipte bir risk faktörünün olup olmadığının tespiti. Gözetim teknolojileri sayesinde araştırılan güvenlik risklerine dair şahıslar hakkındaki tüm bilgilerin bulunduğu veritabanlarına dijital olarak ülkenin her yerinden ulaşmak mümkün hale gelmiştir. Eğer böyle bir yetenek olmasa idi ilgili kayıtları bulmak için belki saatlerce belki günlerce kişiler gözaltında tutulabilir ve dolayısıyla yurttaşlar mağdur olur, hürriyetleri haksız yere kısıtlanırdı.

Günümüzde gözetim teknolojileri vasıtasıyla yukarıda belirtilen konularda sorun yaşanmamaktadır. Türkiye örneğinde Genel Bilgi Tarama (GBT) gibi sistemler aracılığı ile herhangi bir şahısla ilgili bütün polis kayıtlarına ulaşılabilir. Ayrıca güvenlik güçleri; nüfus, adli sicil kaydı, yurt dışı giriş - çıkış kaydı gibi kendi ihtiyaç duyduğu bilgileri de, elektronik ortamda gereksiz evrak, kırtasiye, yazışma, bürokrasi gibi engellerle karşılaşmadan süratli bir şekilde alabilmektedir.

Toplumsal genel güvenliğin sağlanması adına tehlikeyi daha olmadan önce tespit edebilme açısından gözetim faaliyetlerinin olumlu bir sonucu olduğu ifade edilebilir.⁴⁵² Bir metro istasyonunda veya alışveriş merkezinde intihar bombacısının bombayı patlatmadan önceki şüpheli hareketleri veya bir kuyumcu soyan hırsızın eşkalinin belirlenerek yakalanması eylemleri insanların güvenlik kameralarını adeta bir gereklilik olarak görmesine yol açmaktadır. Gözetim teknolojilerinin faydalı olduğu başka bir alan arama - kurtarma faaliyetleridir. Örneğin deprem - göçük - çıkış gibi felaketlerde kaybolanları bulma ve denizde -

⁴⁵⁰ Hakan Yıldırım, *a.g.k.*, s.XV.

⁴⁵¹ *a.k.*, s.136.

⁴⁵² Julie K. Petersen, *a.g.k.*, s.69.

ormanda kaybolanların yerini tespit etme noktasında gözetleme araçları (GPS, Yer Tespit Cihazları) önemli fayda sağlayabilmektedir.⁴⁵³

Sınır gözetimi faaliyetlerinin ulusal güvenliği sağlama açısından önemli fonksiyon gördüğü kabul edilmektedir. Sınırların kamera tespit ve X-ray cihazları ile donatılması ülkeye nükleer bomba, silah, uyuşturucu madde gibi tehlikeli maddelerin sokulmasını engellemeye, uluslararası ticaret kurallarını uygulamaya, göç ve insan haklarının kötüye kullanılmasının önlenmesine yardımcı olmaktadır. Diğer taraftan sualtı güvenliği gibi insan olarak korumanın oldukça zor olduğu alanlarda sonar sistemler gibi gözetleme teknolojileri kullanılmak suretiyle bu alanların korunması da sağlanabilmektedir.⁴⁵⁴

Doğal kaynakların ve milli servetlerin korunması açısından gözetleme teknolojileri makul görülebilmektedir. Doğal kaynakların ve milli servetlerin korunması ulusal kültürel mirasın ve iktisadi canlılığın birer garantörüdür. Bunların korunması yapılmadığı takdirde ulusal kaynakların tükenmesi söz konusu olabilir. Bu koruma faaliyetleri de gözetleme teknolojileri ile rahatlıkla sağlanabilmektedir.⁴⁵⁵

Devletin denetim ve gözetim faaliyetlerini otomasyon sistemleri ve dijital araçlarla yapması, kamu görevlilerinin işlemlerinde din, dil, ırk, cinsiyet ve sınıf ayrımcılığı yapmalarını engelleyebilir.⁴⁵⁶ Zira “her tık iz bırakır” prensibi dolayısıyla dijital ortamda gerçekleştirilen işlemler açık ve şeffaf olduğundan dolayı devlet görevlileri dijital ortamda yapılan takibatta belli bir ırk veya din, ideolojik yaklaşımda olanları görmezden gelme işlemi yapamaz. Örneğin radar hız ihlali yapan araçlara ceza verme açısından herhangi bir ayrımcılık yapılamamaktadır. Zira radar hız ihlali yapan araçların plakaları merkezi otomasyon sisteminde kayıt altında tutulduğundan dolayı böyle bir ayrımcılık yapılması ilgili görevli hakkında cezai işlemi gerektirmektedir.

Dünyada, toplumsal yapı ve yönetsel alanda meydana gelen değişim ve dönüşümler genelde eski sistemin bazı noksanlıklarından veya güncelin beklentilerine cevap verememesinden kaynaklanmaktadır. Genel olarak bakıldığında gözetim teknolojilerinden yoksun klasik yönetsel alanın kamu hizmetlerinin yurttaşlara sunulmasında yetersiz olduğu görülmektedir. Bu yetersizlikler; aşırı kırtasiyeciliğin varlığı, bürokrasinin fazla oluşu, hizmetlerin maliyetlerinin artışı, hizmetlerin nitel ve nicel olarak çoğalmasına karşın yanlış personel istihdam politikalarının devam etmesi, bütün bunlarla bağlantılı olarak hizmetlerin

⁴⁵³ a.k

⁴⁵⁴ a.k, s.71.

⁴⁵⁵ a.k, s.72.

⁴⁵⁶ a.k

kalitesinin düşmesi ve hizmetlerin sunumunda gecikmelerin meydana gelmesi şeklinde sıralanabilir. Bütün bu yetersizlikler bilgi ve iletişim teknolojileriyle giderilmiş, kamu hizmetlerinin sunulmasında alternatif bir çıkış yolu bulunmuştur. Artık yukarıda ifade edilen yetersizliklerin aksine kamu hizmetleri internet - mobil uygulamalarla sunulur hale gelmiştir. Yani gözetim teknolojileriyle gelen elektronik devlet uygulamaları kamu hizmetlerinin sunumunda yaşanan çıkmazda bir tedavi metodu olarak görülmektedir.

Elektronik devlet uygulamaları günümüz kamu hizmetlerinin sunulmasında bir tedavi metodu olarak görülmesi dolayısıyla her kamusal hastalığa ilaç olarak sunulmaktadır. Bu anlayışın temelinde de kırtasiyecilik ve bürokrasinin büyük oranda azalması, bu nedenle maliyetlerin düşmesi, yurttaşların hizmetlere ulaşma hızlılığının devlet memurlarının kapris ve keyif dereceleri yerine kullanılan internetin hızlılığına bağlı olması, yedi gün yirmi dört saat hizmet anlayışıyla sürekliliğin varlığı, devlet kurumlarının kurumsal bilgilerini dijital ortamda paylaşmasıyla ortaya çıkan şeffaflık, ihale ile bütçe ve bütçe harcamaları süreçlerini yurttaşların izleyebilmesiyle ortaya çıkan hesap verebilirliğin artması ve böylece yolsuzluğa kayma girişim tohumlarının önlenmesi, bir açıdan yolsuzluktan haberdar olmanın kolaylaşması ve bunun sonucu olarak halk güveninin kazanılması gibi nedenler yatmaktadır.⁴⁵⁷

Elektronik devlet uygulamaları ile paralel bir şekilde dijital bölünme göz ardı edildiğinde, yurttaşların yönetimde bilgisayar ağlarını kullanabilmesi, bilgisayar ağları üzerinden demokratik aktiviteleri yapabilmesi, siyasal katılım için elektronik postayı, interneti ve mobil uygulamaları kullanabilmesi; bu sayede seçilmiş makamlara yön verme ve hesap sorma yolu ile kendi hakkını savunabilmesi, tepkisini gösterebilmesi olan e-demokrasi gözetim teknolojilerinin sağladığı avantajlardan birisi olarak gösterilebilir.⁴⁵⁸

E-demokrasi, yurttaşların bütün medeni haklarını kullanması; yani yerel ve genel seçimlerin, oylama ve referandumların dijital ortamda yapılması, elektronik başvuru ve elektronik dilekçenin internetten kamu kurumlarına ulaştırılabilmesi, elektronik yurttaş ağlarının oluşturulması, seçilmişler ile seçenlerin dijital hızlı iletişimi ve böylelikle seçmenlerin nabzının yoklanması, internette özgürce düşüncelerini ifade edebilme ve ilgili makamlara bunları ulaştırabilme garantörlüğü gibi süreçleri bünyesinde barındırmaktadır. Sayılan bu araçlar vasıtasıyla yurttaşın siyasal katılım imkanları genişlemekte, yurttaş bir

⁴⁵⁷ Veysel Eren, Uğur Durna, “Kamu Hizmetlerinin Daha İyi Görülebilmesi İçin Alternatif Bir Yönetim Yaklaşımı: Elektronik Devlet”, *İ.Ü. SBF Dergisi*, Sayı: 32, Mart 2005, s.155 - 156.

⁴⁵⁸ Ali Şahin, H. Temizel, M. Temizel, “Türkiye’de Demokrasiden E-Demokrasiye Geçiş Süreci ve Karşılaşılan Sorunlar”, s.1. <http://iibf.ogu.edu.tr/kongre/bildiriler/06-02.pdf>, (Erişim Tarihi: 04.06.2013).

“tık” kadar hızlı bir şekilde sürece dahil olabilmekte ve kendisini temsil edenlerin düşünceleri ile değil kendi bireysel düşünceleri ile temsil edilerek yönetimde söz hakkına sahip olabilmektedir.⁴⁵⁹

2. Mahremiyet Sorunsalı

Mahremiyet kelime olarak Türk Dil Kurumu sözlüğüne göre Arapça kökenli olup “gizlilik” anlamına gelmektedir.⁴⁶⁰ Lyon’a göre kişinin “dokunulmazlık bölgesini” ifade etmektedir.⁴⁶¹ Gözetim toplumunda mahremiyet çerçevesinde değineceğimiz konuların kapsamı gereği “mahremiyet” kelimesi “özel hayatın gizliliği” ile eşanlamli olarak kullanılacaktır. Bu kapsamda “özel hayat” kelime olarak; kişinin kendine özgü yaşayışı, yaşama tarzı, kendisini ilgilendiren tutum ve davranışı anlamına gelmektedir.⁴⁶² Özel hayatın gizliliği ise kişinin kendine özgü yaşayışına dair konuların kişinin rızası olmayanlarca bilinmemesi ve bunlara müdahale edilmemesidir.⁴⁶³

Özel hayatın gizliliği kapsam olarak fiziksel alan, verisel alan, psikolojik ve duygusal alan, örgütsel alan olmak üzere dört çevrede ele alınabilir. Gözetim teknolojileri bu dört alanı da tehdit altında tutmaktadır. Zira potansiyel olarak bu alanlara müdahale yetisine sahip gözükmektedir. Fiziksel mahremiyet, kişinin fiziksel alanına veya bütünlüğüne başkalarının müdahalede bulunmamasıdır.⁴⁶⁴ Bunun kapsamı içerisine kültürel duyarlılık, kişisel saygı, utanma gibi değerler ilgisinde kişinin vücudunun, hareketlerinin kendi özel mülkiyetindeyken (evinde, arabasında vs.) başkaları tarafından izlenmemesi, kaydedilmemesi konuları girmektedir.

Verisel mahremiyet, kişi veya kişilerle ilgili olarak herhangi birisine atfedilebilecek nitelikte özel olan bilgilerin, kişilerin rızası olmaksızın dijital veya başka formlarda toplanmamasını, depolanmamasını ve kategorize edilmemesini ifade etmektedir. Verisel mahremiyet alanı içerisine kişinin inancı, cinsel tercihi, siyasi ilişkileri, finansal durumu, medikal bilgileri, dijital hareketlilikleri (elektronik posta bilgileri, internet ziyaret adresleri vb.), özel aktiviteleri girmektedir. Örgütsel mahremiyet, kişinin bağlantılı olduğu sivil toplum kuruluşları, siyasi partiler gibi örgütsel oluşumlar çerçevesinde yaptığı aktivitelerin, bu kapsamda bağlantıda olduğu diğer kişilerle olan ilişkilerinin kendi rızası dışında takip

⁴⁵⁹ Veysel Eren, *a.g.k.*, s.156.

⁴⁶⁰ <http://www.tdk.gov.tr>, (Erişim Tarihi 11.11.2012).

⁴⁶¹ David Lyon, *a.g.k.*, 2006, s.13.

⁴⁶² <http://www.tdk.gov.tr>, (Erişim Tarihi 11.11.2012).

⁴⁶³ <http://en.wikipedia.org/wiki/Privacy>, (Erişim Tarihi 11.11.2012).

⁴⁶⁴ *a.k.*

edilmesi, araştırılması faaliyetlerini kapsamaktadır. Psikolojik ve duygusal mahremiyet, kişinin duygusal ilişkilerinin, psikolojik durumunun gizli kalmasını ifade etmektedir.⁴⁶⁵

Devlet - birey ilişkilerinde kamu düzeni, kamu güvenliği, kamu sağlığı, sosyal devlet uygulamaları gibi birçok nedenler ileri sürülerek, kişiler hakkında bilgi toplanması normal bir durum haline gelmiştir. Ancak bu durum bilgi ve iletişim teknolojilerindeki hızlı gelişim ile birlikte yeni bir boyut kazanmıştır. Bu yeni boyut toplanan verilerin dağınık halden ziyade birbirleriyle ilişkilendirilerek analitik hale getirilmesi ve veri toplama araçlarındaki artış ve gelişmeler sayesinde bu analitik veritabanlarının çok güçlü ve düzenli bir şekilde beslenebilmesidir.

Azgın dalga misali kişisel verileri toplamaya olan bu ilgidaki artış da kişisel verilerin korunması merkezinde özel hayatın gizliliğinin ihlali tartışmalarını ortaya çıkarmıştır. Bu tartışmanın merkezinde de gözetim olgusu karşısında mahremiyetin korunması yatmaktadır. Mahremiyetin korunması devlet - birey ilişkileri içerisinde devletin niteliğinin belirlenmesi açısından önemlidir. Zira özel hayatın korunmadığı bir yerde liberal - demokratik bir devlet - toplum yapısından bahsedilemeyeceği açıktır.⁴⁶⁶

Bilgi ve iletişim teknolojilerindeki gelişmeler paralelinde kişisel mahremiyete ilişkin verilerin toplanması, depolanması ve verilerin birbiriyle ilişkilendirilmesi araçları, metotları da çeşitlilik göstererek artış sağlamıştır. Örneğin, internet teknolojisiyle birlikte insanlar kişisel alanlarına ilişkin bilgileri internet üzerinde depolamaya başlamışlar, interneti bir iletişim aracı olarak kullanmaya yönelmişlerdir. Böylece internet iktidar güçleri için önemli bir gözetim veri kaynağı haline dönüşmüştür.

Cep telefonlarındaki son teknolojik gelişmelerle birlikte ses paylaşımının yanı sıra yazılı, görsel mesaj - veri paylaşımı da yapılabilecek hale gelmiştir. Dijital kamera ve ses kayıt sistemlerindeki son gelişmelerle birlikte kamera ve ses kayıt cihazlarının ölçüleri böcek boyutuna kadar inebilmiştir. Bütün bunlar kişilerin mahremiyetlerine daha kolay müdahale edilebilmesine yol açmış; toplumsal yaşam bu şekilde evrilmiştir.

Böyle bir toplumsal süreçle birlikte özel hayatın gizliliğinin ve dokunulmazlığının yasalarla teminat altına alınması gerekliliği ortaya çıkmıştır. Özel hayatın gizliliği ve dokunulmazlığına yönelik bir takım ulusal ve uluslararası yasal düzenlemeler bulunmaktadır. Ulusal anlamda özel hayatın gizliliğini koruma altına alan düzenlemeler; Anayasanın “Temel

⁴⁶⁵ a.k

⁴⁶⁶ Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers*, The University of Michigan Press, 2. Edition, 1971, s.28.

Haklar” kısmında “Özel Hayatın Gizliliği” başlıklı 20. maddesi, “Konut Dokunulmazlığı” başlıklı 21. maddesi ile “Haberleşme Hürriyeti” başlıklı 22. maddesidir.⁴⁶⁷ Türk Ceza Kanununun da “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı 9. bölümünde haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğini ihlal, kişisel verilerin kaydedilmesi ayrıntılı olarak düzenlenmiştir. Uluslararası alanda BM İnsan Hakları Evrensel Beyannamesinin 12. maddesinde, hiçbir kimsenin özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamayacağı ve herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı olduğu ifade edilmektedir. Avrupa İnsan Hakları Sözleşmesi’nin 8. maddesinde ise herkesin özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahip olduğu belirtilmiştir.

Özel hayatın gizliliğine yönelik bazı yasal düzenlemelerin olduğu bir gerçektir; ancak bu yasal düzenlemelerin günün şartlarına uygun olarak, bilgi ve iletişim teknolojilerindeki gelişmelere göre teorik ve uygulama revizyonlarının yapılması gerektiği düşünülmektedir. Nitekim bu gerekliliği ortaya koyabilecek eksikliklerin bazıları şu şekilde açıklanabilir: Mevcut durumda cep telefonları, GPS cihazları, RFID etiketlerinin kullanıldığı teknolojiler, bireylerin zaman ve mekan bağlamındaki davranışları hakkında şimdiye kadar görülmemiş boyutlarda verinin toplanmasına olanak sağlamaktadır. Diğer taraftan internet ortamında bireyler, kendi bilgileri üzerinde tam kontrole sahip olamamaktadır. İnternet siteleri üzerinde kişiler kendi bilgilerini görme, kimlerle bu bilgileri paylaşacağına karar verme, istediği an tüm bilgilerini değiştirebilme ve kalıcı olarak silme hakkına sahip olması gerekirken, bu

⁴⁶⁷ “A. Özel hayatın gizliliği Madde 20: Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hakimın onayına sunulur. Hakim, kararını el koymadan itibaren kırk sekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

B. Konut dokunulmazlığı Madde 21: Kimsenin konutuna dokunulamaz. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin konutuna girilemez, arama yapılamaz ve buradaki eşyaya el konulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hakimın onayına sunulur. Hakim, kararını el koymadan itibaren kırk sekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

C. Haberleşme hürriyeti Madde 22: Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakimın onayına sunulur. Hakim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.”

konuda birçok sorun yaşanabilmektedir. Ayrıca dijital ortamda her bir birey kendi bilgilerinin başkaları tarafından kullanıldığını öğrendiğinde, bu durumun hemen değiştirilmesini isteme hakkına sahip olmalıdır. Ancak internet sitelerinde bu konuda iletişim mekanizmalarının iyi çalışmadığı ve süreç konusunda sıkıntıların yaşandığı bir gerçektir.⁴⁶⁸

Başkalarına ait kişisel bilgileri kullananların tespit edilmesi ve gerekli hukuki yaptırımların etkin bir şekilde uygulanabilmesi için internet sitesi sahiplerinin, üzerlerine düşen sorumlulukları yerine getirmeleri konusunda eksikleri vardır. İnternet sitelerinin, sahip oldukları kişisel bilgileri ancak kendi faaliyetleri doğrultusunda kullanabilmesi ve ilgili kişilerin onayları alınmadan hiçbir koşulda ticari amaçla kullanamaması gerekmektedir. Bu konuda sitelerin gizlilik politikası belgelerinde muğlak ifadeler kullanılarak özel hayatın gizliliğini ihlal etmelerini sağlayacak hareket alanları oluşturulabilmektedir. İnternet siteleri özel hayatın korunması konusundaki ilkelerini açık bir şekilde ifade etmeli ve bu ilkelerde yapılacak değişiklikler önceden kişilere iletmelidir. Ayrıca bütün bunların yasal olarak teminat altına alınması ve uymayanlara karşı yaptırım uygulanması gerekmektedir.⁴⁶⁹

Özel hayatın gizliliği konusunda, internet dışı bilgi ve iletişim teknolojilerinde de internet üzerindeki benzer sorunlar yaşanmaktadır. Örneğin, ülkemizde aracınıza kasko yaptırdıktan sonra yılın belirli aralıklarında çeşitli sigorta şirketlerinden sizi cep telefonundan arayarak kendi şirketlerinin kasko uygulamalarını anlatmak isteyenler olabilmektedir. Bütün sigorta şirketleri “Tramer”⁴⁷⁰ adında ortak bir otomasyon sistemi kullanarak aralarında müşterilerin cep telefonu numaraları da dahil olmak üzere bütün kişisel bilgilerini paylaşmaktadırlar ve bundan hiçbir yurttışın haberi olmamaktadır.

Bireyin hakları göz önüne alındığında, bilgi ve iletişim teknolojileriyle elde edilen verilerin kimler tarafından toplanacağı, nasıl ve ne süreyle saklanacağı, bu verilere erişime kimlerin hangi koşullar altında yetkili olacağı, bu veriler analize tabi tutulurken hangi teknik

⁴⁶⁸ <http://www.stratejikboyut.com>, (Erişim Tarihi 11.11.2012).

⁴⁶⁹ a.k

⁴⁷⁰ Tramer, kendi resmi internet sitesi olan “<http://www.tramer.org.tr>” de şu şekilde açıklanmaktadır: “Tüm sigorta şirketlerinin trafik sigortası poliçe kayıtlarının tutulduğu ilişkisel bir veritabanı oluşturmak ve verileri en çok bir günlük gecikme ile sürekli güncellemek, tüm sigorta şirketlerinin trafik sigortasına ilişkin hasar verilerini almak ve bu kayıtları sigorta kayıtları ile ilişkilendirmek, merkezi olarak; ‘Hasar Durum Belgesi’ düzenlemek, sigorta verilerini, sigortalılık oranlarını ve hasar verilerini hazırlanacak formatta yönetim raporlarına/bilgi raporlarına dönüştürmek ve kamuoyunun bilgisine sunmak, yetkili kullanıcıların konuyla ilgili tüm bilgi ihtiyacını karşılamak, Emniyet Genel Müdürlüğü’nden motorlu araçlara ait trafik tescil kayıtlarını elektronik ortamda günlük olarak almak ve bu kayıtları sigorta kayıtları ile ilişkilendirmek, sigorta şirketlerinin rücu alacaklarına ilişkin mahsuplaşma işlemlerini kolaylaştırmak, mevcut ve gelişmekte olan teknolojileri kullanarak, görev alanı kapsamına giren konularda sektörün gelişimine katkıda bulunmak amacıyla trafik sigortasına ilişkin tüm verilerin merkezi bir veritabanında toplanmasını, günlük olarak güncellenmesini ve bu verilerin ilgili tarafların ortak kullanımına sunulmasını sağlayan otomasyon sistemidir.”

ve yöntemlerin kullanılacağı, çıkan analiz sonuçlarının ticari haklarının kime ait olacağı ve hangi uluslararası kanunlar çerçevesinde değerlendirileceği gibi konuların hızla tartışılması, toplumun bu konuda bilinçlendirilmesi ve gerekli düzenlemelerin hayata geçirilmesi gerekmektedir. Diğer taraftan toplumsal düzeyde internet veya diğer bilgi - iletişim teknolojileri yoluyla kişilerin özel hayatlarına yapılan tecavüzler konusunda yeterli bir bilinç ve duyarlılık bulunmamaktadır.

Bireylerin özel hayatlarını, ilişkilerini, varlıklarını, zamanlarını ve statülerini internetten ve diğer bilişim sistemleri araçlarından kaynaklanabilecek zararlardan korumak istemeleri doğal bir haktır. Bu nedenle, tüm ülkelerin üzerinde mutabık olacağı uluslararası bir belge/anlaşma ile bilişim sistemleri ve internetten kaynaklanacak tehditlere karşı özel hayatın gizliliğinin; yani mahremiyetin korunması gerektiği değerlendirilmektedir. Bu noktada Birleşmiş Milletler başta olmak üzere ilgili uluslararası örgütlere önemli görevler düşmektedir.

Buna paralel olarak, kimi ülkelerde olduğu gibi, özel yasalar çıkarılarak sorumluluklar ve yaptırımlar belirlenmesi gerektiği de düşünülebilir. Ancak uygulamada böyle bir uluslararası düzenlemenin önünde yapısal engeller bulunduğu gerçeğini de göz önünde bulundurmak gerekir. Buradaki başat yapısal engel, mahremiyetin dönemle ve yerle çok ilintili olması durumudur. Mesela Japonya’da mahremiyete en yakın olan ifade, aynı aile, şirket ya da kulüp içinde paylaşılan içerideki hayata ilişkin bir sözcüktür. Buna karşın Batı kültüründe mahremiyetin alanı daha sınırlı durmaktadır. Diğer taraftan 1970’li yıllarda mahremiyet alanına giren konular 2000’li yıllarda mahremiyetle ilişkilendirilmesi tuhaf karşılanabilmektedir.⁴⁷¹

Veri toplama, toplanan verileri analize tabi tutma ve depolama noktasında dijital tekniklerde yaşanan gelişmeler sayesinde artık “bireye” ait olan her şeyi izleyebilmek, kaydedebilmek ve bunları depolayabilmek mümkün hale gelmiştir. Bu noktada bireyin artık hemen hemen her zaman kamusal ve özel alanlarda gözetlenebilir bir hedef olduğu ifade edilebilir. Burada önemli olan bu hedef kategorisine sadece hakkında suç şüphesi olan şahıslar değil sıradan insanların da giriyor olmasıdır. Bu durumda iki olasılık ortaya çıkmaktadır. Ya tüm insanlığa suçlu şüphesi ile yaklaşılmaktadır ya da masum insanların mahremiyeti önemslenmemekte, yok sayılmaktadır.

⁴⁷¹ David Lyon, *a.g.k*, 2006, s.48.

Gözetimin hedef kitlesine sıradan insanların da oturtulmuş olmasının altında yatan en büyük etmen kent yaşamının artan ağırlığıdır. Mitcell'e göre kent yaşamında bireyler her zaman başkalarını izleyebilecek ve izlenebilecek duruma gelmişlerdir. Kent yaşamının yararlarına karşılık, bu yararlardan faydalanabilmek için özel yaşamın bir kısmının feda edilmesine göz yummak durumunda kalınmaktadır. Çünkü elektronik veri toplama ve dijital karşılaştırma teknikleri, geçmişte kullanılan veri toplama tekniklerinden çok daha güçlüdür.⁴⁷² Bu nedenle yeni gözetim teknolojileriyle birlikte mahremiyet kavramı da bir dönüşüm yaşamıştır. Bu dönüşüm içinde bireylerin mahremiyetlerine ilişkin kaygıların niteliği değişirken “sıradanlık” kavramı öne çıkmıştır. Çünkü sıradan olmak, bireylerin kişisel verilerinin kamusal alana çıkmasında veya pazar sisteminin bir verisi olma durumunda endişeleri azaltan bir etken olarak gözükmemektedir.

Kişisel bilgilerin her gün binlerce kuruluş ve devlet tarafından toplanarak mahremiyetin ya da özel alanın yok edilme durumuyla karşı karşıya kalınmasına rağmen, gözetim araçları, toplu ya da bireysel bir tepkiyle karşılaşmadan çok hızlı bir şekilde artmaktadır. Bu noktada gözetime direniş eksikliğinin nedenleri önem kazanmaktadır. Bu nedenler bir anlamda gözetime karşı meydan okuyamamanın birer göstergesi niteliğindedir.⁴⁷³

Günümüzde öyle bir dönem içerisinde yaşıyoruz ki adeta “birey hakkında ne kadar çok bilgi o kadar ilgi!” sloganıyla herkes, herkes hakkında her şeyi bilmek istiyor. Pazarlama açısından bakılırsa, potansiyel müşteriler hakkında çok şey bilmek onların ihtiyacına yönelik çok şeyi üretebilmektir. Benzer şekilde devlet de birçok kayıt tutmaktadır. Bunlar, yurttaşların vergi, sağlık, eğitim kayıtlarından günlük aktivitelerine kadar uzanabilmektedir. Çünkü devlete göre her geçen gün giderek artan suçlularla mücadele edebilmek için olabildiğince bilgiye sahip olunması gerekmektedir.⁴⁷⁴ Bireye ilişkin olanı bilme arzusu, bireylerde kendilerine ilişkin veriler üzerindeki hakimiyetlerini kaybetme ve bu bilgileri elinde bulunduranların etkisi altına girme riskini oluşturmaktadır. Tabii ki buradaki en önemli sorun, gözetim toplumunun gelişmesiyle birlikte mahremiyetin aşınması ve bundan geri dönüşün oldukça zor oluşudur.

Bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte mahremiyet konusunun bu kadar tartışılmasının en önemli nedenlerinden birisi, insanların farkında olmadan kendi rızalarıyla gözetimin mahremiyete saldırısına izin vermeleridir. Ayrıca mahremiyetin tanımı

⁴⁷² William J. Mitchell, *a.g.k.*, s.159.

⁴⁷³ David Lyon, *a.g.k.*, 2006, s.22.

⁴⁷⁴ Felix Stalder, *a.g.k.*, s.120 - 124.

hakkındaki belirsizlik de insanların bu bilinçsizliğinde önemli bir etkiye sahiptir. Özellikle yeni teknolojilerle birlikte bireylerin mahremiyet alanına ait olarak uğradıkları kayıpların farkında olup olmadıkları, bu kayıplar karşısında rızalarının olup olmadığı ile ilgili sorular mahremiyet kavramının tanımlanmasında başvurulacak sorulardır. Bu sorular, objektif bir mahremiyet kavramının oluşmasına engel olmaktadır.⁴⁷⁵ Örneğin bir kişi elektronik posta adresinin ve cep telefonu numarasının ne olduğunun başkaları tarafından bilinmesini istemeyebilirken bir başkası da bunu hiç önemsemeyebilmektedir. Bu kişisel görüş farklılıklarına toplumdaki yükselen güvenlik kaygısı da eklenince bazı durumlarda bireyler mahremiyetlerine ilişkin olanları devletle ya da başka örgütlerle paylaşmada kendinden istekli olabilmektedirler.

Bilgi ve iletişim teknolojilerinin olanakları sayesinde hayatın en sıradan ve mahrem alanlarının bile gözetime tabi tutulabildiği günümüzde gözetim güçlerinin mahremiyete saldırıları türlerine; bireyler hakkındaki toplanan özel bilginin yayılması, bireyleri dikizleme, takip etme, izleme ve onların fotoğraflarını çekme, hususi yerlere girme ya da zorla girme; başkalarının konuşmalarını veya telefon görüşmelerini gizlice dinleme, telefon ya da elektronik posta irtibatlarına gizlice ulaşma, internet akışını takip etme örnek olarak gösterilebilir.

Gözetim toplumunda mahremiyete müdahale sorunsalı insanlar nezdinde giderek normalleşmekte ve bir sorun olmaktan çıkmaktadır. Bunda etkili olan temel sebep gözetim teknolojilerinin her yere yayılması ve insanlar için sokağın, işyerinin, internetin doğal birer parçası haline gelmesidir. Bu yaygınlaşmanın kaynakları çeşitlilik arz etmektedir. Örneğin, günümüzde medya bunun en önemli kaynaklarından birisini oluşturmaktadır. Bunun yanı sıra resmi otoriteler daha sağlıklı kamu hizmetleri sunmak, güvenliği sağlamak, vergi toplamak gibi makul nedenlerle düzenli olarak sıradan insanlar hakkında veri toplamaktadır. Devlet otoritelerinin yanı sıra bilginin güç olduğunu bilen işletmeler de sokaktaki insan hakkında sürekli olarak veri toplayıp, bunları depolayıp kategorize edebilmektedir.⁴⁷⁶

Herhangi bir alışveriş merkezine girdiğinizde kapalı devre kamera sistemleri, *loyalty* kartlar, termal kameralar aracılığıyla sürekli kayıt altına alınabilmektesiniz. Bütün bunların ötesinde depolanıp, kategorize edilen kişisel özel verilerin kamu kurumları arasında, özel şirketlerin kendi arasında veya kamu kurumları ile özel şirketler arasında paylaşılabildiği düşünüldüğünde gözetim toplumunda mahremiyete saldırının boyutları öngörülebilir.

⁴⁷⁵ a.k, s.122.

⁴⁷⁶ Veysel Bozkurt, a.g.k, s.5 - 8.

Kişilerle ilgili olarak dijital ortama girilen bilgilerin yok edilmesinin de giderek imkansız hale gelmesi olayın vahametini arttırmaktadır. İnsanlar kendileri ile ilgili bir takım bilgilerin tespit ve kayıt edildiğini bildikleri halde bu bilgilerin nerede ve kimlerin elinde olabileceği hakkında bilgi sahibi olamaması gözetimin özel hayat üzerindeki görünmez, rahatsız edici elidir. Bu rahatsız edici elin yıllar geçtikçe yeni nesiller tarafından normalleştirilmesinin insanlık için ağır bir kayıp haline geleceği değerlendirilmektedir.⁴⁷⁷

Gözetimin mahremiyete müdahalesinin temel gerekçelerinden birisi kamu yararadır. Gözetim toplumlarında kamu yararı denildiğinde adeta akan sular durur ve kimse bu sözün üstüne söz edemez hale gelmiştir. Amitai Etzioni, mahremiyet ile kamu yararı arasında makul bir denge kurulması gerektiğini ifade ederek, bu dengenin kriterlerini şu şekilde sıralar: ⁴⁷⁸

- a) Özgür bir toplum, kamu yararını, kamu sağlığını ve güvenliğini ciddi şekilde tehdit eden iyi belgelenmiş makro düzeydeki bir tehlikeyle yüz yüze gelindiğinde mahremiyeti sınırlandırmalıdır. Ancak, sadece farazi bir tehlikeye atfen bunu yapmamalıdır.
- b) Kamu yararının bulunduğuna karar verildikten sonra, söz konusu amaca mahremiyeti sınırlandırmaksızın varılıp varılamayacağı tartışılmalıdır. Örneğin sağlık kuruluşlarındaki tıbbi kayıtlara ihtiyaç duyulması halinde, isim, adres ve sosyal güvenlik numarası gibi kişiyi tanımlayan bilgiler verilmeksizin mevcut veriler araştırmacılara sunulabilir.
- c) Mahremiyete yönelik sınırlamalar, mümkün olduğunca minimum düzeyde kalmalıdır. Örneğin uyuşturucu testleri ve benzeri uygulamalar, sadece başkalarının yaşamından sorumlu olanlara (okul servis sürücülere ve pilotlara gibi) uygulanmalıdır.
- d) Mahremiyeti zorunlu olarak sınırlandıran önlemlerin istenmeyen yan etkilerini önlemeye yönelik tedbirler alınması, bu etkileri görmezlikten gelmeye tercih edilmelidir. Bu tür tedbirler, hem insanları gereksiz müdahalelerden korumak için hem de ihtiyaç duyulan politikalara kamu desteğini sürdürmek bakımından gereklidir. Böyle bir yaklaşımla örneğin, bir yandan tıbbî kayıtların güvenliği sağlanırken, diğer taraftan AIDS hastalığını teşhis etmek için uygulanan HIV testleri, kamu sağlığının gerektirdiği ölçüler içinde yapılabilir.”

Gözetim toplumunda mahremiyete saldırı araçları arttıkça kamusal alan - özel alan ayrımı bir dikatomi haline dönüşmektedir. Eskiden beri özel alan - kamusal alan arasındaki sınır net olarak ortaya konulamamıştır. Ancak günümüzde gözetim teknolojilerinin giderek artan bir şekilde dönüşüm ve gelişim göstermesi ve böylece gözetim toplumunun varlığını daha çok hissettirmeye devam etmesiyle kamusal alan karşısında, özel alanın daralması biçiminde bir eğilim ortaya çıkmaktadır. Özel alanın kamusal alana göre daha geniş tanımlandığı ülkelerde mahremiyet konusundaki duyarlılıklar da o derece fazla olmaktadır.⁴⁷⁹

Özel alanların kamusallaştığı toplumlarda her ihtiyacı, arzusu, zevki ve düşüncesi, kamusal bir soruşturmaya veya denetime konu olan şahıs, bireyselliğini yitirerek ortalama bir

⁴⁷⁷ Julie K. Petersen, *a.g.k.*, s.9.

⁴⁷⁸ Amitai Etzioni, “The Right to Privacy vs. the Common Good”, *USA Today Magazine*, 129/2664, 2000, s.13 - 15., akt; Mehmet Yüksel, “Mahremiyet Hakkına Ve Bireysel Özgürlüklere Felsefi Yaklaşımlar”, *Ankara Üniversitesi SBF Dergisi*, Sayı 64 - 1, Ankara, Haziran 2009, s.292.

⁴⁷⁹ Veyssel Bozkurt, *a.g.k.*, s.5 - 8.

varlığa dönüşür. Oysa kollektif düşüncenin, bireyin bağımsızlığına müdahalesinin bir sınırı olmalıdır. Bu sınırı bulmak ve onu saldırılara karşı korumak, toplumsal yaşamın iyi bir şekilde sürdürülebilmesi bakımından vazgeçilmez öneme sahiptir.

Yukarıda tartışılan gözetim faaliyetlerinin mahremiyete saldırısının ortaya çıkardığı sorunlara karşın mahremiyet karşısında gözetim faaliyetlerinin haklı görülebileceğini savunan görüşler de vardır. Fischer ve Hubner özel hayatı bölgesel, kişisel ve bilgisel olmak üzere üç temel alana bölmektedir. Bu noktada tartışma bilgisel özel hayat hakkında ortaya çıkmaktadır.⁴⁸⁰ Buna göre kişisel bilgileri almayla ortaya çıkacak maliyet kazancı ve amaçlara kısa yoldan ulaşım bilgisel özel hayatın korunamamasından kaynaklanan zararları telafi edecektir.⁴⁸¹

Kişilerin kendileri ile ilgili veriler üzerinde kendi kullanım tekellerinin olmaması; kişisel verilerin kimler tarafından, hangi amaçla, ne şekilde, ne zaman toplandığı; nerede ve ne uzunlukta saklandığı; kimler tarafından ne şekilde kullanıldığı gibi konularda tamamen edilgen olmak insanları endişeye sevk etmektedir. Kimliği ve çoğu zaman da araçları belirsiz gözetimler, hiç farketirmeden topladıkları verileri değiştirme, çarpıtma, istedikleri gibi yansıtma; hatta bu verilerden yola çıkarak yeni veriler yaratma lüks ve tekeline her zaman sahiptirler.

Devlet, ticari kuruluşlar, bireyler vs. her türlü kişisel kayda (telefon konuşmaları, elektronik postalar, bilgisayar kayıtları, sağlık kayıtları, ekonomik kayıtlar, vs.) rahatlıkla ulaşabilmekte, bu kayıtlar, kişilerin izni olmaksızın depolanmakta, bilinmeyen kişi ve kurumlarca, bilinmeyen biçimlerde, bilinmeyen nedenler için kullanılabilir. Dolayısıyla bu kişi ve kurumlar, bilgisi toplanan kişiyle ilgili, kişinin kendisinden daha fazla bilgiye sahip olabilmektedirler. Bu konuda devletin ve resmi kurumların iddiası, bireylerin güvenliğinin bireyler hakkında elde edilen verilerle doğru orantılı olduğu noktasında toplanmaktadır. Ne kadar çok bilgi, o kadar çok güvenli ortam. Bu durum, bireylerin, kendilerine ait bilgiler üzerindeki hakimiyetlerini kaybetme ve bilgiyi elinde bulunduranların etkisi altına girme riskiyle karşı karşıya kalmalarına neden olmuştur. Kişilerin özel alanları kamunun paylaşımına sunulmuştur. Bireysel özgürlüklerin artma eğilimi, devlet, kurum ve bireylerin, teknolojik gelişmelerle birlikte artan oranda özel hayata müdahil olma eğilimiyle paralel gelişmektedir.

⁴⁸⁰ Hubner Fischer, *IT-Security and Privacy: Design and Use of Privacy - Enhancing Security Mechanisms*, Springer, New York, 2001, s.26., akt., Kirstie Ball, Frank Webster, *a.g.k.*, s.13.

⁴⁸¹ Alan Moore, "Privacy and the Encryption Debate", *Knowledge, Technology and Policy* Vol 12, No 4, Winter 2000., akt., Kirstie Ball, Frank Webster, *a.g.k.*, s.13.

3. Veri Güvenliği Tehlikesi

Günümüzde bilgi ve iletişim teknolojileri hızla gelişmekte, teknoloji çevreleri “yeni nesil” olarak adlandırılan sistemlerle çevrenmektedir. Bu gelişme ve değişimler insanların bilgi ve iletişim teknoloji girdabına kendilerini daha çok kaptırmasına yol açmakta; bir anlamda “yaşam”, “elektronik yaşam”a evrilmektedir. Elektronik yaşam, yaygınlaşıp geliştikçe, hayatın her alanına girmektedir.

Elektronik ortamda hizmet alan kişiler, kendilerine özel tanımlanan numaralar ile bütün şirket, vakıf, kurumlarla ve diğer bireylerle olan işlerini gerçekleştirebilmekte ve bu işlerin kendi adına internet üzerinden otomatik olarak halledilmesini sağlayabilmektedirler. Bu bakımdan elektronik yaşam içinde yer alan birey her elektronik işlemde bir kayıt tutulduğu ve kendi özel hayatına ilişkin bilgi verdiği için “izi sürülebilir” hale gelmiştir.

Birey ile ilgili elektronik ortamda kolaylıkla toplanabilen veriler, bireyin özel hayatının gizliliği ile bireyin ve ailesinin mali ve can güvenliği için sürekli bir tehdit olacaktır. Zira artık elektronik ortamda olan bu veriler şirketler, vakıflar, kurumlar ve diğer bireyler arasında paylaşılabılır, depolanabilir ve kullanılabilir hale gelmiştir. Bu bakımdan artık, bireyin elektronik ortamda paylaşılan bu verileri kontrol edebilme imkanı kalmamıştır. Bireyin verilerinin güvenliğinden şüphe duyması ve buna rağmen verilerini paylaşacak şekilde hareket etmeye devam etmesi, bilgi ve iletişim teknolojilerinin cazibesi ve bireyin bunların fetişisti haline getirilmesinden kaynaklanmaktadır.

Devlet veya özel kuruluşlar eliyle bireye ait verilerin toplanması, depolanması ve işlenmesi sürecinde en büyük tehlike bu verilerin yetkisiz kişilerin veya kuruluşların eline geçmesi, hukuka aykırı olarak kullanılması ve üçüncü şahıslara ifşa edilmesidir. Bu tehlikenin bertaraf edilmesi bir anlamda veri güvenliğinin sağlanmasını ifade etmektedir.⁴⁸² Kamusal anlamda bilgi ve iletişim teknolojileri kullanılırken veri güvenliği iki şekilde görülebilir. Bunlardan birincisi, kamu kurumlarının yurttaşlara ve kurumlara bu teknolojileri kullanarak hizmet verirken bireye özgü kişisel verilerin kötü niyetli üçüncü şahısların eline geçmesi sorunudur. İkincisi, kamuya ait verilerin ulusal güvenliği tehlikeye düşürebilecek şekilde düşman unsurlarının eline geçmesidir. Bu nedenlerle bireye ve kamuya ait veriler güvenli bir ortamda saklanmalı ve bilişim gizlilik protokolleri hatasız bir şekilde oluşturulmalı ve uygulanmalıdır.⁴⁸³

⁴⁸² Lee Bygrave, “Data Protection Pursuant to the Right to Privacy in Human Right Treaties”, *International Journal of Law and Information Technology*, Vol. 6, No. 3, s.247 - 284.

⁴⁸³ Mete Yıldız, *a.g.k.*, s.318.

Yurttaşların kamusal ve özel işlemlerinde kullandıkları verilerin üçüncü şahısların eline geçmesi esasında bilgi - iletişim teknolojileri ve ağ güvenliği problemlerini aşan ve temel haklarla ilgili olan bir sorundur. Örneğin; internet ortamında özel veya kamu internet sitelerine kişisel tanımlayıcı bilgiler rahatlıkla girilebilmektedir. Fakat bu kişisel verilerin çoktan üçüncü şahıslar tarafından çalınarak veya üçüncü şahıslarla paylaşılması durumunda bir kimlik dolandırıcılığı ile karşı karşıya kalınabilir.⁴⁸⁴

Kimlik dolandırıcılığı veya kimlik hırsızlığı, ekonomik fayda (örneğin internet üzerinden yapılan alışverişler) elde etmek için veya cezalardan (hız ihlal cezaları, kiralık araç kullanırken yapılan kazalar vs.) korunmak için başka birisinin kimliğini edinmedir.⁴⁸⁵ Kimlik dolandırıcılığına örnek olarak, kişisel bilgilerin çalınarak bunların sürücü belgesi veya nüfus cüzdanı çıkarılmasında kullanılması ve çıkarılan bu belgelerle bankalardan büyük borçlar alınması gösterebilir. Bu tür durumlarda mağdur şahısların kendilerinin suçsuz olduklarını veya borç almadıklarını ispatlayabilmeleri çetrefilli bir süreçtir, ispatlayamadıkları takdirde de ceza alabilirler. Bu veriler bireylerin çeşitli elektronik işlemleri neticesinde üçüncü şahısların eline geçebileceği gibi diğer taraftan devlet korumakla yükümlü olduğu kişisel verileri kendi dijital depolarından çaldırabilir. Tüm ülkedeki telefon abone kayıtlarının veya nüfus yurttaşlık bilgilerinin çalınarak internette satılmasını buna örnek gösterebiliriz.

Giddens, çağdaş devlet organizasyonlarının, yurttaşları ile ilgili doğum, okul ve iş kayıtlarından, vergi toplamak için kullanılan mali konular ile ilgili verilere ve ulusal sigorta numaralarına kadar çok büyük ölçüde veriyi toplamalarına dikkat çekmektedir. Ona göre, her türlü bilgi ve iletişim teknolojilerinin gelişmesiyle gözetim, yaşamımızın her köşesine girerek özel yaşamın gizliliğini tehdit eder hale gelmiştir. Bu tehlikeyi şu örnekle açıklamaktadır:⁴⁸⁶

“Diyelim ki, devletin her bir yurttaşı hakkında ortalama 20 dosya içeren, 2200 veritabanı işlettiği 26 milyon nüfuslu bir ülke biliyoruz. Bu ülkenin nüfusunun yüzde onunun isimleri, merkez polis teşkilatının bilgisayarlarında var. Buranın diktatörlük altında yönetilen bir ülke olduğunu düşünebilirsiniz. Gerçekte bu ülke Kanada'dır.”

Kanada örneği, e-devlet konusunun veri mahremiyeti boyutuna ilginç bir vurgu yapmaktadır. Bireysel hakların ve özel hayatın gizliliğinin korunabilmesi için anayasal çerçevenin e-devlet hizmetlerini kapsayacak şekilde yeniden düzenlenmesi veya yorumlanması bu bağlamda giderek önem kazanmaktadır. Diğer adli vakaların takibinde olduğu gibi bireylerin gizli kalmasını istediği bilgilerin e-devlet ağı içinden soruşturulmasında hukuki bir yetkilendirmeye dayanan uygulamalar esas alınmalıdır. Ayrıca e-devlet veri

⁴⁸⁴ Nigel Gilbert, *a.g.k.*, s.25.

⁴⁸⁵ *a.k.*

⁴⁸⁶ Anthony Giddens, *Sosyoloji*, Çev. Talip Kabadayı, Ayaç Yayınevi, Ankara, 2000, s.312.

tabanlarını işletenlerin özel bilgilerin gizliliğini sağlama konusunda yasal bir sorumlulukla yükümlü hale getirilmesi gerekmektedir. Bu sistemlerde kayıtlı bilgilerin, bu bilgilerin sahiplerinin izni olmaksızın üçüncü şahısların eline geçmesi suç sayılmalıdır.⁴⁸⁷

Kişisel verilerin üçüncü şahısların eline geçmemesi ile ilgili veri güvenliğinin temin edilmesinde devletin sorumluluğu kadar özel sektörün de sorumluluğu bulunmaktadır. Zira artık özel sektörün yurttaşlar üzerinde kamusal sektörden daha fazla veri sahibi olduğu ve kendi arasında veri takası yaptığına yönelik çeşitli örnekler bulunmaktadır.⁴⁸⁸

Günümüzde özel sektörün elindeki verilerin artışıdaki en büyük neden, özelleştirme neticesinde devletin elindeki bilgi depolarının özel sektöre devredilmesi ve özel sektörün hayatımızın her alanında faaliyet gösterir hale gelmesinden kaynaklanmaktadır. Bu durum da kişisel verinin daha kontrolsüzce akması ve dolayısıyla veri konteynırlarının daha sızdırıcı olmasına neden olmaktadır.⁴⁸⁹ Örneğin, ülkemizde herhangi bir bankadan alacağınız kredi ve ödeme sürecinizdeki işlemlerinizi ile kredi çektiğiniz bankanın sizin mali durumunuz ile ilgili yorumu diğer bütün bankalarla sizin rızanıza bakılmaksızın rahatlıkla paylaşılabilir. Her gün alışveriş yaptığınız marketten aldığınız market kartı sayesinde bütün alışveriş geçmişiniz bir çırpıda kasa görevlisi tarafından görülebilmekte, bu veriler marketler arasında bile paylaşılabilir. Hayatın her alanına giren özel sektör karının maksimizasyonu için yurttaşların kişisel verilerini başkalarıyla paylaşmaktan hiç çekinmemektedir.

Bilgi ve iletişim teknolojilerindeki veri güvenliği sorununun ikinci boyutunda biraz daha genele ve devlete bakan yönüyle kamusal bilgilerin ulusal güvenliği tehlikeye düşürebilme ihtimali yer almaktadır. Nitekim devletin elinin altında bütün yurttaşların kimlik, adres, telefon, hesap bilgileri gibi her türlü bilgiyi içeren inanılmaz bir veri sirkülasyonu bulunmaktadır. Bu veriler bilgi ve iletişim teknolojileri kullanılarak daha rahat ve istenilen formatta saklanabildiği gibi onlarabilgi ve iletişim teknolojilerini kullanarak daha rahat dijital saldırılar da gerçekleştirilebilmektedir.⁴⁹⁰ Örneğin, ülkemizde Nüfus ve Vatandaşlık İşleri

⁴⁸⁷ a.k, s.312.

⁴⁸⁸ R.Laperriere, *Veri Korunmasının Quebec Modeli*, Bennet ve Grant, 1999, s.183., akt., David Lyon, *a.g.k*, 2006, s.90. “Quebec, 1980’lerin ortasında Fransa’da özel sektörün vatandaşlar üzerinde kamusal sektörden daha fazla veri sahibi olduğu ve veri takası yaptığını gösteren kanıtlar sunmuştur. Özel olarak yönetilen kişisel veri tabanlarının sınırlarını ifşa eden bu rapor, L’Identite Pratee olarak adlandırılmış ve bir farkındalık oluşmasını sağlamıştır.”

⁴⁸⁹ David Lyon. *a.g.k*, 2006, s.90 - 91.

⁴⁹⁰ “FBI tarafından yapılan araştırmalara göre ABD’de işten çıkarılan her 100 kişiden 81’i eski şirketlerine dijital saldırıda bulunuyor. Ülkelerin yüzde 21’i diğer ülkelerin sistemlerini çökertiyor. Her 100 firmadan 44’ü rakip şirketin bilgilerine saldırı yoluyla ulaşıyor. Günümüzün teknolojik devrimi internet kendi kazdığı kuyuya mı düşüyor? 1970’li yılların başında hiçbir güvenlik kaygısı olmadan geliştirilen sistem bugün dijital saldırılara karşı korunmaya çalışıyor. Firmalar sistemlerini çökerterek kendilerini milyonlarca dolarlık zarara uğratan saldırılara çözüm bulunmasını istiyorlar. Sınırsız iletişim ve bilgi özgürlüğünün mekanı internet ‘güvenlik’

Genel Müdürlüğü'nün resmi internet sitesinde, tüm yurttaşlar internet sitesinde istenilen belli veriler üzerinden TC kimlik ve diğer kimlik bilgileriyle ilgili çeşitli sorgular gerçekleştirebilmektedir. Aynı internet adresinden terör örgütleri veya yabancı düşman unsurlar tarafından bilgi - iletişim sistemleri ve programları kullanılarak ülkemizdeki bütün yurttaşların temel kimlik ve adres bilgileri, soy bilgileri çalınabilir. Böyle bir durum da esasında ulusal güvenliği tehlikeye düşürebilir. Bu tip tehlikelerin altında bilgi ve iletişim teknolojilerinin yaygınlaşmasıyla ortaya çıkan “bilişim tabanlı tekno - güvenlik problemleri” yatmaktadır. Yani “sanal ortam tehditleri/bombaları”, “bilgi/bilişim savaşları”, “dijital savaş teknikleri”, “elektronik savaş”, “bilgisayar korsan savaşı” gibi çeşitli teknik ve uygulamalar söz konusu olabilmektedir. Mesela bunlardan elektronik savaş ile rakibin hareketlerini, bilgi akışını ve iletişim sistemini çözmek ve kendi faaliyetleriyle ilgili karşı tarafa ipuçları vermemek için yapılan bilişim saldırıları anlaşılmaktadır. Bilgisayar korsan savaşında bilgisayar korsanları askeri veya ticari bilgi sistemlerine girebilmekte, güvenlik problemlerine yol açabilmektedirler. Bunların, hedeflenen ülke, kişi veya kuruma ait sistemlerde zarar meydana getirmek, geçici veya tamamen durmasını sağlamak, stratejik dosya ve bilgileri kendi çıkarları doğrultusunda kullanmak gibi çok çeşitli amaçları olabilmektedir.⁴⁹¹

Kişisel veri güvenliğinin bozularak, bunların üçüncü şahısların veya kurumların eline geçmesi bazen kasıtlı⁴⁹² yapıldığı gibi bazen de verileri kullanan görevlerinin hatalarıyla da olabilmektedir. 1999 yılının Şubat ayında Michigan Üniversitesi Sağlık Bölümü'nde yapılan rutin bir çevrimiçi araştırmanın sonucunda, bazı gizli tıbbi kayıtlar hastaların çizelge

savaşı veriyor. FBI dijital saldırılara karşı savaş açan kurumların başında geliyor. Kurum tarafından yapılan araştırmalara göre ABD'deki kuruluşların %90'ı bugüne kadar en az bir kez dijital saldırıya uğradı. Bu kuruluşların yüzde 70'inin gizli bilgileri çalındı yada zarar gördü. Araştırmaya göre dijital saldırıların büyük bölümü iç kaynaklı. Örneğin işten çıkarılan her 100 çalışanın 81'i eski şirketine dijital saldırı girişiminde bulunuyor. Bu kişilerin yaptıkları saldırılar verdikleri zararların boyutuna göre değişiyor. Hangi seviyede olursa olsun bir çalışanın bazı şifreleri biliyor olması zarar vermesine yetiyor. Araştırmaya göre her 100 firmadan 44'ü rakip firmaların sistemlerini çökertiyor. Yalnızca şirketler değil devletler de dijital saldırı yapıyorlar. Buna göre dünyadaki ülkelerin yüzde 21'i diğer devletlere ait bilgi işlem sistemlerine ulaşmak için dijital saldırılar düzenliyorlar.” Hürriyet İnsan Kaynakları, 10 Mart 2002, Pazar, s.20.,www.meslekiyeterlilik.com, (Erişim Tarihi: 10.06.2013).

⁴⁹¹ Murat Erdal, *a.g.k*, s.23 - 34.

⁴⁹² Intel firması Pentium III'ü çıkarırken kullanıcılara sunduğu tek şeyin hız olmadığı savunulmaktadır. Bu iddiaya göre; bilgisayarların beyni olan işlemcilerde, tam olarak ne için kullanacağı açıklanmayan bir kimlik numarası da verilmiştir. İşlemcinin içinde bulunan bir çip, her kullanıcıya bağımsız bir kimlik numarası veridiği ve bu numara sayesinde, kullanıcının internet üzerindeki her adımı takip edilebildiği belirtilmektedir. Pentium III bilgisayarlara ilişkin en büyük itiraz Çin Hükümetinden gelmiştir. Çin bu seri numarasının, ulusal güvenliğini tehdit ettiğini söyleyerek, ülke sınırları içerisinde Pentium III işlemcili bilgisayarların satışını ve devlet kurumlarında bu bilgisayarlarla internete bağlanmayı yasaklamıştır. Bu alandaki bir başka tehlike ise, bilgisayarlara kurulan bazı yazılım ve kullanılan donanımların gizli servislerle işbirliğidir. Almanya gibi bir ülkenin Microsoft ürünlerini devlet kurumlarında kullanmaktan kesin olarak vazgeçtiğini bildirmiştir. Almanya'nın yanı sıra Fransa, Rusya, Finlandiya gibi ülkeler de, özellikle devlet kurumlarında açık kaynak kodlu Linux işletim sistemlerine geçmekte ve Linux'un yaygınlaşması için çaba harcamaktadırlar. Bilal Şen, “Elektronik Gözetim”, s.1, <http://www.genbilim.com/content/view/8025/91>, (Erişim Tarihi: 10.06.2013).

kütüğünde ortaya çıkmıştır. Böbrek yetersizliği, bağırsak kanseri, zatürre ve yüzlerce başka hastalığa bağlı isimler, adresler, sosyal güvenlik numaraları, iş durumları ve tedavi kayıtları ifşa edilmiştir. İnsan hatası sonucu bu veriler, yanlışlıkla güvenliği sağlanmamış bir internet sitesinde paylaşılmıştır.⁴⁹³ Bu olayla hemen hemen aynı dönemde Kanada’da çevrimiçi kayıt olan Air Miles toplayıcıları, diğer 50.000 çevrimiçi kaydının kişisel detaylarına serbest erişimleri olduğunu fark etmişlerdir. Bu detaylarda isimler, adresler, telefon numaraları, e-posta adresleri, kullanılan kredi kartı tipleri, sahip olunan araç sayısı ve kayıtlı olunan diğer müşteri bağlılık programları (sık kullanılan uçuş firmaları gibi) yer aldığı bilinmektedir.⁴⁹⁴

Günümüzde en mükemmel dijital sistemlerde bile veri güvenliğinin kesin olarak sağlandığı iddia edilemez. Özellikle bir şekilde internet ile bağlantılı sistemlerde ve bilgisayarlarda bulunan gizli verilere bir şekilde ulaşılabilir. Çünkü bir tarafta veri güvenliği sistemleri son teknolojiye uygun olarak geliştirilse bile karşı tarafta da virüs, truva atı, casus programlama dilleri gibi sistemler son teknolojiye uygun olarak geliştirilmektedir.

Veritabanı internete bağlı olmasa bile sisteme girmeye yetkili kimselere rüşvet vermek suretiyle bu bilgilere ulaşım mümkün olabilmektedir. Örneğin, ulusal çocuk bilgi sistemlerinde yer alan ülkedeki bütün doğan bebeklere ait isim, kan gurubu, adres ve herhangi bir sağlık problemine yatkınlık gibi bilgiler, organ hırsızları gibi kötü niyetli insanlar tarafından bu verileri saklamakla görevli personele rüşvet vermek veya şantaj yapmak suretiyle elde edilebilir.⁴⁹⁵

Ağ korsanlığı, bilgisayar virüsleri, truva atları, solucanlar gibi kötü niyetli yazılımlar kullanılarak kredi kartı numaralarının ve şifrelerinin, *Facebook - Twitter* gibi arkadaşlık sitelerinde profile özgü özel verilerin, devletin resmi kurumlarının internet siteleriyle bağlantılı çalışan veritabanlarında yer alan bilgilerin çalınması, kötü niyetli kişilerin bunlar aracılığıyla başkaları adına işlemler yapmaları mümkün olmaktadır.⁴⁹⁶

E-devlet uygulamaları, yurttaşların bütün bilgilerini web tabanlı sistemler üzerinde bulundurması açısından veri güvenliği boyutuyla oldukça tedirginlik oluşturunca bir tehlike olarak karşımızda durmaktadır. Ayrıca casus yazılımlar aracılığıyla kişilerin iş veya kişisel bilgisayarlardaki her hareketi kaydedilebilmekte, dosyalar okunabilmekte, dijital fotoğraf ve videolara bakılabilmektedir. Video kameralar sadece bulundukları yerde insanların görsel

⁴⁹³ David Lyon, *a.g.k.*, 2006, s.12.

⁴⁹⁴ T. Hamilton, “Güvenlik İhlali Özel Air Miles Verilerini Açıkladı.”, *The Globe and Mail (Toronto)*, 22 Ocak 1999., akt., David Lyon, *a.g.k.*, 2006, s.12.

⁴⁹⁵ Nigel Gilbert, *a.g.k.*, s.22.

⁴⁹⁶ Serhat Baştan, *a.g.k.*, s.12.

hareketlerini kaydederken, bu casus yazılımlar bilgisayar açık olduğu müddetçe hem özel hayat ihlal edici araçlar hem de dijital ortamda suç işleyebilecek mekanizmalar olarak varlığını sürdürebilmektedir.⁴⁹⁷

Kişisel verilerin güvenliği ve dijital mahremiyetin yok sayılmasına yol açan ünlü casus yazılımlarından; *Promis*, *Carnivore*, *Truva Atı*; sahip oldukları güç ve yetenekleri ve kişisel veri güvenliğinin sağlanmasında oluşturdukları risklerin boyutlarını anlamak için burada bahsedilecektir. *Promis*; bankaların, holdinglerin ve devlet dairelerinin gizli veri depolarına, fark edilmeden girme ve istenilen bilgiyi çalma imkanını tanıyan, 1990'ların başından beri ABD, Kanada, İtalya, Hollanda ve İsrail istihbarat servisleri tarafından kullanıldığı bilinen bir casus yazılımdır.⁴⁹⁸ Ersanel'in belirttiğine göre *Promis*, başlı başına bir istihbarat silahıdır. Zira hedefin belli olmadığı zamanlarda veya bulunamadığı durumlarda, hedefin özelliklerine yakın değerler bu casus yazılıma girildiğinde, dünyadaki internet üzerinden herhangi bir şekilde bağlantısı olan bütün bilgi bankalarını kendisini gizleyerek tarayıp tüm dünyada hedef kişi ve kurumların mahrem bilgilerini toplayıp, analiz edebilmektedir.⁴⁹⁹

Carnivore; ABD Federal Soruşturma Bürosu (FBI) tarafından internet servis sağlayıcıları kullanılarak hedef elektronik posta adresindeki bütün posta hareketliliklerini izlemeyi sağlayan bir gözetim yazılımıdır. Bu yazılım bir ağ üzerinde geçen tüm e-posta hareketlerini toplayarak analiz edebilmektedir. Ayrıca bu sistem, gelen ve giden mesajların başlık kısmını okuyarak mesajların kimden kime gittiğine yönelik irtibat analizi de yapabilmektedir.⁵⁰⁰

Truva Atı; ABD'nin istihbarat örgütü Ulusal Güvenlik Birimi NSA (National Security Agency) tarafından geliştirilmiş olan günümüzde istihbarat örgütleri, hatta internet üzerinden şahıslar tarafından da temin edilerek kullanılabilen bir gözetim yazılımıdır. Bu gözetim yazılımı temel olarak takip edilmek istenen bilgisayara bir ara programcığın kurulmasıyla devreye girmektedir.⁵⁰¹ Bilgisayar korsanları truva atları kullanarak istedikleri kişilerin e-postalarına ve bilgisayarlarındaki kayıtlı bilgilere ulaşabilmektedir.⁵⁰² Bu yazılımlar

⁴⁹⁷ Anthony C. Caputo, *a.g.k.*, s.7.

⁴⁹⁸ Ersanel Nedret, *a.g.k.*, s.18.

⁴⁹⁹ *a.k.*, s.5.

⁵⁰⁰ Bilal Şen, *a.g.k.*, s.4 - 6.

⁵⁰¹ Yılmaz Yazıcıoğlu, *Bilgisayar Suçları*, Alfa Yayınları, İstanbul, 1997, s.155.

⁵⁰² Truva atlarının bilgisayarlara ne kadar kolay bulaşabildiğine yönelik olarak Genel Merkezi ABD'nin California bölgesinde bulunan Symantec firmasının kişisel bilgilerin ele geçirilmesine yönelik tehditlerde bir artış olduğu dair olarak 2004 yılında yayınladığı rapor sonuçları konunun boyutlarının önemini ortaya koymaktadır. Bu rapora göre; 1 Temmuz - 31 Aralık 2004 tarihleri arasın da 6 aylık dönemde, tespit edilen en tehlikeli 50 zararlı kodun %54'u gizli bilgilere yönelik tehditlerden oluşmaktadır. Bundan önceki raporda ise bu

kendilerini farklı uygulamaların veya elektronik postaların arkasına gizleyebilmekte ve bunlar çalıştırıldığında kullanıcı farketmeden işlevini yerine getirebilmektedir. Adını da zaten bu özelliğinden almıştır.

Yukarıda belirtilen gözetim programları olmadan da başkasının bilgisayarına sızarak onun bilgisayarındaki bütün bilgi ve belgelere ulaşmak, elektronik yazışmalarını ve incelediği internet sitelerini görmek, bankacılık şifrelerini öğrenmek, hatta bilgisayarın kamerasından bilgisayarın kullanıcılarını izlemek mümkündür. Bu işlemleri hedef bilgisayarın IP numarasını biliyorsanız yapmak oldukça basittir. Örneğin, bilgisayar üzerinde denetim masası menüsündeki “yönetimsel araçlar - bilgisayar yönetimi - eylem - başka bilgisayara bağlan” aşamalarını takip eder ve hedef bilgisayarın IP numarasını buraya yazarsanız hedef bilgisayar internete bağlandığında adeta bir kullanıcı gibi bilgisayara nüfuz edebilirsiniz.⁵⁰³ Ayrıca “netscantools” gibi programlar kullanarak da hedef bilgisayardaki verilere ulaşmak mümkündür.⁵⁰⁴

Kişisel verinin hem işlenmesi hem de imha edilmesi veya ham halde bekletilmesi aşamalarının tümü gizlilik ve güvenlik kurallarına uyarak yapılması gerekir. Ayrıca kişisel verilerin gizliliğinin sağlanması söz konusu işletmelerin faaliyetlerine başlamadan önce yapması gerekenlerden başlayıp, uygulama ve denetleme aşamasına kadar bir bütün olarak ele alınmalıdır. Dolayısıyla yapılması gereken ilk şey işletme imtiyazı, ruhsatı veya genel izni verilecek işletmelerden kişisel verileri nasıl ve ne şekilde koruyacakları hakkında provizyon istemek olabilir. Bu yeterliliği sağlayamayan işletmeye, izin verilmeyebilir.⁵⁰⁵

İşletmelerin veya çalışanlarının, kişisel verilerin gizliliği kuralına uymaması halinde ilgili işletmenin kapatılması da dahil ağır cezaların belirlenmesi gerektiği düşünülmektedir. Bu da mutlaka güçlü, amaca uygun, tecrübeli ve özel hayatın gizliliği konusunda hassasiyet derecesi yüksek personelden oluşan tüm kurum ve kuruluşları kapsayacak bir denetim mekanizmasının varlığını gerektirmektedir. Aksi halde bu verilerin gerçek anlamıyla korunması sağlanamaz. Yine bu denetimin sürekli, caydırıcı ve etkili olması için teknolojinin sunduğu imkanlardan faydalanılmalı, güvenlik boşluğu meydana getirebilecek teknolojik gelişmeler takip edilmelidir.

oran firma tarafından yüzde 36 olarak tespit edilmiştir. “Kişisel Bilgilere Yönelik Saldırılar Artıyor”, <http://turk.internet.com/haber/yazigoster.php3?yaziid>, (Erişim Tarihi 21.03.2013).

⁵⁰³ www.wardom.org, (Erişim Tarihi: 11.02.2013).

⁵⁰⁴ www.netscantools.com, (Erişim Tarihi 17.02.2013).

⁵⁰⁵ Hakan Yıldırım, *a.g.k.*, s.266 - 267.

Türkiye’de de bilgi ve iletişim teknolojilerinin hızla yayılan çehresine karşın veri güvenliği bir zafiyet olagelmektedir. E-devlet, e-dönüşüm gibi adlar altında özellikle kamu sektöründe kamusal faaliyetlerin sürdürülmesiyle yurttaşlık numaralarının verilmesi ve nüfus bilgilerinin elektronik olarak kaydedilmesi, işlenmesi süreçlerini içeren Mernis projesi gibi yoğun olarak kişisel verilerin işlenmesine dayanan projeler her geçen gün artmaktadır. Kişisel verilerin işlenmesine ilişkin faaliyetlerin artması bu alanda güvenlik sorununu gündeme getirmiştir. Türkiye’deki veri güvenliğinin sağlanamamasındaki en büyük sorunlardan birisi bütün kamu ya da özel kurum ve kuruluşların uyması gereken standartların önceden belirlenmemiş olmasıdır. Türkiye’de kişisel verilerinin korunmasıyla ilgili kurumsal bir bilinç oluşmamıştır.⁵⁰⁶

4. Etik Boyutu

"Yasalar karşısında insan, başkalarının hakkına tecavüz ettiği zaman suçludur. Etiksel olarak ise bunu aklından geçirdiği anda bile suçludur."
Immanuel Kant (1724-1804)⁵⁰⁷

Bu bölümde denetim ve gözetim faaliyetlerinin etik boyutu ele alınacaktır. Öncelikle etik kavramsal olarak incelenecek, sonrasında denetim ve gözetim faaliyetlerinde ve günümüzde bunların yapılmasını yaygınlaştıran ve kolaylaştıran bilgi ve iletişim teknolojilerinin etik boyutuna dair tespitler yapılacaktır. Son olarak denetim - gözetim faaliyetlerinin kamusal muhatabı olan kolluk kuvvetlerinin gözetime konu olan davranışlarının etik boyutu değerlendirilecektir.

Etik sözcüğü, Yunancada “karakter” anlamına gelen “*ethos*” sözcüğünden türetilmiştir. Badiou’ya göre etik; insanların kurduğu bireysel ve toplumsal ilişkilerin temelini oluşturan değerleri, normları, kuralları doğru - yanlış ya da iyi - kötü gibi ahlaksal açılardan araştıran bir felsefe disiplinidir. Etik; Yunancada iyi bir var oluş tarzı, bilgece bir eylem yolu arayışına karşılık gelir. Etik, öznel eylem ve onun temsil edilebilir niyetlerinin evrensel bir yasa ile nasıl bir ilişki içinde olduğu meselesidir.⁵⁰⁸ Bauman’a göre etik; her ahlaklı kişinin itaat etmek zorunda olduğu birbiriyle tutarlı ilkelerden oluşan tek buyruklar grubudur.⁵⁰⁹ Dedeoğlu’na göre etik; bireylerin tercihlerini ve davranışlarını etkileyen doğru ve yanlış

⁵⁰⁶ Muammer Ketizmen, Çağlar Ülküder, "E-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması", www.inet-tr.org.tr/inetconf12/bildiri/2.pdf, (Erişim Tarihi:05.07.2013).

⁵⁰⁷ "In law a man is guilty when he violates the right of others. In ethics he is guilty if he only thinks of doing so." Immanuel Kant, *Great Thoughts*, George Seldes, 1985, s.222.

⁵⁰⁸ Alain Badiou, *Etik: Kötülük Kavrayışı Üzerine Bir Deneme*, Çev. Tuncay Birkan, Metis Yayınları, İstanbul 1998, s.17.

⁵⁰⁹ Zygmunt Bauman, *Postmodern Etik*, Çev. Alev Türker, Ayrıntı Yayınları, İstanbul, 1998, s.33.

ilişkin ilkeler; doğru ya da iyinin ne olduğunu belirleme sanatı, hayat tarzı, bir dizi eylem kuralı ya da ahlak ilkesidir.⁵¹⁰

Etik, kişiler arası ilişkilerde istem ve eylemlerin ahlaki yönünü inceler ve bu yüzden “ahlak felsefesi” olarak da adlandırılmaktadır. Etik temel olarak insanın eylemlerinin ahlaki açıdan değerli veya değersiz olması ve bunu etkileyen unsurlarla ilgilenmektedir. Bu kapsamda insanın hangi davranışa yola açan nedeninin; yani isteminin veya iradesinin ve aynı zamanda gerçekleştirdiği eylem veya davranışın doğru hangisinin yanlış olduğu etik alanına girmektedir.⁵¹¹ Mesela trafik kazasında yaralanan birisine yardım etmeyi istemek iyidir. Lakin bu kişi ilkyardım kurallarını bilmiyorsa kazazedeye müdahale eylemi yanlış olabilir. Bu kapsamda etik alanında bir eylem veya davranış hem ahlaki açıdan iyi hem de uygulama açısından da doğruysa etik olarak kusursuz bir eylem veya davranış olur.

Gözetim ve gözetim teknolojilerinin oluşturulması ve kullanılması sürecinde hangi istemin/iradenin; yani davranışa yol açan nedenin “iyi” hangi istemin/iradenin “kötü” olduğunu ve aynı zamanda hangi eylemin/davranışın “doğru” hangi eylemin/davranışın “yanlış” olduğunun tespitine yönelik olarak etik kuralların oluşturulması bir gereksinim olarak karşımıza çıkmaktadır. Bu kapsamda Gary T. Marx, gözetim etiğini belirlemeye yönelik sorular oluşturmuş ve bu sorulara verilen cevaplar doğrultusunda bir uygulamanın etik olup olmadığını ispat etme yoluna gitmiştir. Bunu yaparken öncelikle bir takım faktörler belirlemiştir. Öncelikli olarak etik olup olmadığı değerlendirilecek olan gözetim uygulamasının gerekliliği ve bu uygulamanın istenilen hedefe ulaşmak için gerçekten geçerli sonuç verip vermeyeceğidir. Ona göre salt kişisel ya da kurumsal menfaatler için kişisel verilerin kullanılması etik kavramına uygun düşmeyecektir.⁵¹²

Gerekliliği sağlanan bir gözetim yönteminin bireye fiziksel ya da psikolojik zarar verip - vermemesi ve gözetlenenin izni olup - olmaması sorgulanmalıdır. Örneğin, bir bireyin saç, kan ya da parmak izi gibi verilerini toplamak sıradan ve alışık olunan bir durum değildir. Fakat bazı yeni teknolojilerde kullanıcıyı tanıma amaçlı şifre yerine parmak izinin kullanılması ya da havaalanına giren bireyin güvenlik hedefli retinasının eşleştirilmesi gibi teknolojiler hayata sızdıkça, bedene ait tüm veriler gündelik kullanıma açılmaktadır. Burada

⁵¹⁰ Gözde Dedeoğlu, *Etik Düşünce ve Postmodernizm*, Telos Yayınları, İstanbul, 2004, s.113.

⁵¹¹ Server Tanilli, *Yaratıcı Aklın Sentezi: Felsefeye Giriş*, Adam Yayınları, Ankara, 1998, s.233.

⁵¹² Gary T. Marx, “An Ethics For the New Surveillance”; *The Information Society*, <http://www.mit.edu/gtmarx/nicolin5.html>, (Erişim Tarihi: 05.07.2013).

belirtilen tekniklerin böyle bir denetime gerçekten ihtiyaç olduğu için mi kullanıldığının ve bireye zarar verip vermediğinin netleştirilmesi gerekmektedir.⁵¹³

Bireyin DNA'sına kadar sızabilen biyolojik gözetim teknikleri düşünüldüğünde, elde edilen verinin hassasiyeti ve derinliği ortaya çıkmaktadır. Burada bu verilerin kullanımından tedirginlik duymaktan daha doğal bir şey olmayacaktır. Yine biyolojik gözetim uygulamaları üzerinden gidilecek olursa, bireyler güvenlik hedefli bu uygulamalara zaman zaman kendi rızalarıyla katılmaktadırlar. Fakat bu durum bile, gözetleyenlere bu verileri istedikleri gibi kullanma hakkını vermemelidir. Kişisel verilerini paylaşma sunan bireyin en azından kullanım şekli ve sınırları üzerinde insiyatifi olmalıdır. Aksi takdirde Marx'a göre bu durum kişisel hak ve özgürlükleri çiğneme noktasına giden etik olmayan bir yaklaşıma dönüşür.⁵¹⁴

Veri toplama hususunda gereklilik ortaya çıktığında ve bu durumun bireye ciddi bir zarar vermeyeceği temin edildiğinde, sıra veri toplama koşullarının etik kurallara uygun olup olmadığını incelemeye gelecektir. Öncelikle bireylerin kişisel verilerinin kimlerin elinde olduğu ve neden bu kişilerin elinde olduğuna dair fikir sahibi olmaları ve bütün bunlar için izinlerinin olması beklenmektedir.⁵¹⁵ Marx'ın gözetimin zararsızlığı konusunda objektif bir bakış yaratmak için belirlediği faktörlere eklediği bir soru da, gözetleyenlerin bu şekilde bir uygulamaya kendileri maruz kalsa tepkilerinin ne olacağıdır. Çünkü daha önce örneklenen gözetim uygulamalarında, bireyin insiyatiline danışmaksızın gözetleyen iktidarlar, gözetlenenle aynı durumda olmamalarından ötürü, bu tarz bir empatiden uzakta durmaktadırlar. Üstelik iktidarın veri toplamaya yönelik iştahı hep yükselen bir ivmeyle artmakta, asgari düzeyde veri toplamakla yetinmemektedir.⁵¹⁶

Etİge bakan yönüyle bilişimsel gözetim olarak adlandırılan gözetim uygulamalarında, kişisel verilerin çeşitli yazılımlarla toplanıp, veritabanlarında muhafaza edilip, dijital ortamda otomatik olarak gruplanıp bilgi ve istihbarata dönüştürülmesi sürecinde insan faktörünün devreye girip girmediği de önemli bir sorudur. Eğer bu süreç bireylerin müdahalesine açık ise diğer bir soru bu bireylerin kayıtları yorumlama, sorgulama haklarının olup olmadığıdır. Bu durum kişisel verilerin öznel ve objektif olmayan bir değerlendirmeye alındığı anlamına gelecektir ki bu durum etik değildir.⁵¹⁷

⁵¹³ a.k

⁵¹⁴ a.k

⁵¹⁵ a.k

⁵¹⁶ a.k

⁵¹⁷ a.k

Kişisel verilerin o verilere ulaşabilen kişilerin niyetine bağlı olarak kullanılabilceği izlenimi veya gerçeği de etik anlamda sorunlu taraflardan birisidir. Bu durumla ilgili önceki bölümlerde örnekler verilmiş olup, kurumsal yapıların hatta kamu kuruluşlarının bile ellerindeki verileri başka kurumlarla paylaştıklarından bahsedilmiştir. Kişisel veri dolaşımını hızlandıran ve önüne geçilemez bir hale getiren bu husus, bilişim toplumunu gözetim toplumuna iten temel etkindir. Dolayısıyla bu konu etik çerçevesinde atlanmaması gereken bir konu olarak kendini göstermektedir.⁵¹⁸

Kişisel veri toplamaya yönelik uygulamalarda veri toplama yöntemi ile amacı arasındaki bağlantı açığa kavuşturulmalı ve gözetim uygulamasının bütününde temel ilke şeffaflık olmalıdır. Amacı ve kullanım sınırları açıkça belirtildiği ve yapılan işlemlerin denetime tabi tutulduğu, bireylerin izni alınarak oluşturulan veri sistemlerinin genel anlamda etik kurallara uygun olabileceği söylenebilir.⁵¹⁹

Günümüzde gözetim faaliyetlerinin yer aldığı her yerde kendisinden bahsettiren bilgi ve iletişim teknolojilerindeki gelişmeler toplumsal düzen ve toplumda süregelen kurallar üzerinde bazı deformasyonlara yol açmaktadır. Bu bakımdan bilgi ve iletişim teknolojileri kamuda tarafsızlık, maddi çıkar elde etmemek gibi bir takım etik ilkelerin uygulanmasını kolaylaştırırken; dijital eşitsizlik, özel hayatın mahremiyetinin zarar görmesi gibi bir takım yeni etik sorunların ortaya çıkmasına neden olmaktadır.

Bilgi ve iletişim teknolojileri etiği, bilgi ve iletişim teknolojilerinin sosyal etkilerini ve bunlar kullanılarak yapılan eylemlerin uygunluğunu araştırma gayeli etik çalışmalar alanı olarak ifade edilebilir.⁵²⁰ Bilgi ve iletişim teknolojileri etiği kapsamında; bilgi ve iletişim teknolojilerini diğer insanlara zarar vermek için kullanmamak; diğer insanların dijital ortamdaki çalışmalarına karışmamak; başkalarının dijital ortamındaki dosyalarına girmemek; bilgi ve iletişim teknolojilerini veri, para vs. çalmak için kullanmamak; bilgi ve iletişim teknolojilerini yalancı şahitlik yapmak için kullanmamak; bedelini ödemedi bir yazılımı kopyalamamak ve kullanmamak; yetkisiz veya uygun bedelini ödemeksizin başka kişi ya da kuruluşun bilgi ve iletişim teknolojisini, yazılım veya programlarını kullanmamak; bilgi ve iletişim teknolojilerini her zaman diğer insanları düşünerek ve onlara saygı göstererek kullanmak gibi davranışların etik olduğu ifade edilebilir.⁵²¹

⁵¹⁸ a.k

⁵¹⁹ a.k

⁵²⁰ James H. Moor, "What is Computer Ethics?", *Metaphilosophy*, Vol:16(4), 1985, s.226 - 275.

⁵²¹ M. David Ermann vd., *Computers, Ethics and Society*, Oxford University Press, 1997, s.313.

Yukarıda belirtilen etik kurallar aynı zamanda aksiyle düşünüldüğünde bilgi ve iletişim teknolojileri alanındaki etik sorunları da ifade etmektedir. Bunlara ek olarak bilgi ve iletişim teknolojilerinin ve günümüz gözetim dünyasının önemli bir parçası olan elektronik postalarla ilgili olarak ortaya çıkan etik sorunlara, e-posta almayı beklemeyen kişilere ticari amaçla e-posta göndermek, gönderilen bir e-postayı sahibinden izin almadan sanal tartışma grupları gibi genele açık ortamlara göndermek, mesajlaşma listesinden çıkma talebinde bulunan bir kişiyi listeden çıkartmamak, başkalarının e-posta adreslerine dijital izleme virüsleri bulaştırarak onların mesajlarının içeriğini ve kimlerle iletişim kurduğunu takip etmek, dolandırıcılık faaliyetlerinde bulunmak için e-posta mesajı arkasına gizlenen özel virüsler aracılığı ile şahısların bilgisayar ekranlarını izlemek ve bu kapsamda kredi kartı bilgileri gibi özel bilgileri çalmak örnek gösterilebilir.⁵²²

Bilgi ve iletişim teknolojilerinin toplumsal boyutta ayrılmaya yol açabilecek nitelikteki en büyük etik sorunlarından birisi dijital bölünmedir. Dijital bölünme en basit tanımıyla dijital teknolojinin faydalarından yararlananlar ile yararlanamayanlar arasındaki uçurum olarak ifade edilebilir.⁵²³ Dijital bölünmenin aşamalarını ve sebeplerini ekonomik bölünme, kullanılabilirlik bölünmesi ve yetkinlik bölünmesi olarak ayırabiliriz. Buna göre ekonomik bölünme; bilgisayar ve internete erişim sağlayacak ekonomik güce sahip olanlarla olmayanlar arasındaki bölünmedir ve belki de dijital bölünmenin en yaygın ve en temel sebebi olduğu söylenebilir. Kullanılabilirlik bölünmesi; yurttaşlardan teknolojiyi kullanmak için gerekli bilgi, birikim, donanım ve becerilere sahip olan ve olmayanlar arasındaki uçurumu ifade etmektedir.⁵²⁴

Yetkinlik bölünmesi; toplumda ekonomik eşitsizlikler ortadan kaldırılrsa, herkes e-başvuru, e-oylama, e-danışma, e-sorgulama gibi e-devlet uygulamalarını kullanmayı öğrense bile bu uygulamalara herkesin düzenli katılımını sağlamanın olanaklı olmayacağını ifade eder. İşte dijital bölünme bu sebepler üzerinde temellenmektedir ve bu sebepleri ortadan kaldırmak komple yapısal bir sorundur. Bu yapısal sorun devam ettikçe dijital bölünme olacak ve dijital bölünme olduğu sürece de e-devlet uygulamaları bu temelde yükselecektir. Böylece uzun vadede e-devlet ile ilgili mevcut yapısal sorunlar gittikçe derinleşecektir.⁵²⁵

⁵²² Ruhdan Uzun, *İletişim Etiği Sorunlar ve Sorumluluklar*, Gazi Üniversitesi İletişim Fakültesi Basımevi, Ankara, 2007, s.257 - 260.

⁵²³ <http://www.digitaldivide.org/dd/digitaldivide.html>, (Erişim Tarihi: 29.05.2013).

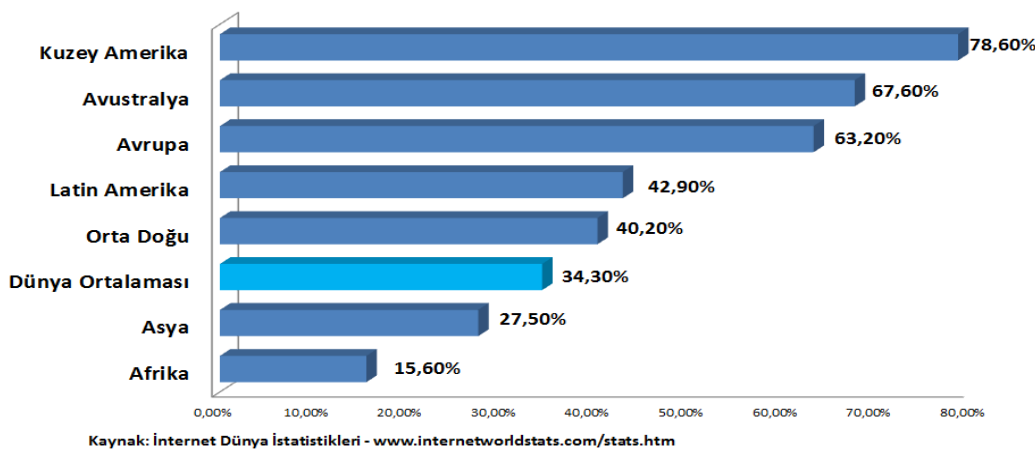
⁵²⁴ Özgür Uçkan, *a.g.k*, s.72.

⁵²⁵ *a.k*

Dijital bölünme ülke içindeki toplumsal kesimler arasında olduğu gibi ülkeler arasında, hatta kıtalar arasında da olmaktadır. Dijital bölünmenin temel sebebi teknolojinin mülkiyetine sahip olan merkez ülkelerin toplumsal ve ekonomik olarak teknolojik gelişmelere hazır iken çevre ülkelerin kapitalizmin eşitsiz gelişme yasası gereği giderek yoksullaşmaları, buna bağlı olarak giderek nüfuslarının artması, salgın hastalıklardan başlarını kaldıramamaları gibi nedenlerle daha Maslow'un "İhtiyaçlar Piramidindeki"⁵²⁶ temel ihtiyaçları karşılayamamışken daha üst basamakları onlardan beklemektir. Bu bakımdan teknolojik gelişmeler kapsamında e-devlet uygulamalarının çevre ülkelerde etkinleşip - yaygınlaşmasını beklemek mantıklı değildir.

Nitekim aşağıdaki Haziran 2012 dönemine ait coğrafi bölgelere göre internet yaygınlık oranlarını gösterir grafik⁵²⁷ bu durumun açık bir resmidir. Grafiğe göre, internet kullanım yaygınlığında Kuzey Amerika %78,6 lık bir orana sahip iken Afrika'nın %15,6 lık bir orana sahip olması ve bu iki kutup arasındaki uçurum olan %63 lük oran aslında dünyadaki dijital bölünmenin yani teknolojik uçurumun boyutları hakkında bize ışık tutmaktadır. Dolayısıyla bilgi ve iletişim teknolojileri ve uygulamalarındaki gelişmeler toplumsal dijital bölünmeyi arttıracığından ve zaten kapitalizm olduğu sürece de bu dijital bölünme var olacağından dolayı dijital bölünmenin bilgi ve iletişim teknolojilerinin kaçınılmaz bir etik sorunu ve sonucu olduğu ifade edilebilir.

Şekil-1. Coğrafi Bölgelere Göre Dünya İnternet Kullanım Yaygınlığı Oranları - 2012



⁵²⁶ Abraham H. Maslow insan ihtiyaçlarını beş temel kategoride incelemiş, ihtiyaçları hiyerarşik olarak ele almış ve insanın en alttaki ihtiyaçların karşılanması ardından bir üstteki ihtiyaçlar kategorisine doğru yöneldiğini söylemiştir. Bu ihtiyaçlar sırasıyla *Fizyolojik ihtiyaçlar*: Temel içgüdüsel ihtiyaçlardır. Yemek, içmek, uyumak, solumak, seks gibi ihtiyaçlar bu kategori için örnek olarak gösterilebilir. *Güvenlik ihtiyaçları*: İnsanlar, can ve mal varlıklarının korunmasına ihtiyaç duyarlar. *Sevgi ve aidiyet ihtiyacı*: Sevmek, sevilme, bir gruba mensup olma, yardımseverlik, şefkat türündeki ihtiyaçlar bu gruba örnek gösterilebilir. *Saygı ihtiyacı*: İnsanlar sevmek, sevilme dışında kendilerine saygı duyulmasını da isterler. Tanınma, sosyal statü sahibi olma, başarı elde etme, takdir edilme gibi ihtiyaçlara yönelirler. *Kendini gerçekleştirme ihtiyacı*: Alt kategorilerdeki ihtiyaçlarını karşılamış olan birey son aşamada ideallerini ve yeteneklerini gerçekleştirme ihtiyacı duyar.

⁵²⁷ <http://www.internetworldstats.com/stats.htm>, (Erişim Tarihi: 11.12.2013).

Bilgi ve iletişim teknolojilerindeki gelişmeler bunları kullananları ve kullanmayanları da kapsayacak şekilde gözetimin nüfuzunun artışına neden olmaktadır. Bu artıştaki yoğunluk günümüzde kaçınılmaz gözüktüğü üzere gözetim faaliyetlerinde bu teknolojileri kullananların; yani kameraların arkasındaki görünmez gözlerin sahiplerinin bu teknolojileri kullanırken uymaları gereken bazı etik kodların varlığını zorunlu kılmaktadır. Bu noktada meslek etiği kavramı ortaya çıkmaktadır. Pehlivan'a göre; meslek etiği, bir meslek grubunun, mesleğe ilişkin olarak oluşturup koruduğu, meslek üyelerine emreden, onları belirli bir şekilde davranmaya zorlayan, kişisel eğilimlerini sınırlayan, yetersiz ve ilkesiz üyeleri meslekten dışlayan, meslek içi rekabeti düzenleyen ve hizmet ideallerini korumayı amaçlayan mesleki ilkeler bütünüdür.⁵²⁸

Her meslek az ya da çok belirgin olan kendi meslek etiğini ya da ait olduğu örgütün etiğini üretir. Pieper'e göre bu etik normlar, bu mesleği seçen kişiler etrafında örgülenir.⁵²⁹ Meslek ya da örgüt onuru bu normlarla sıkı sıkıya bağlıdır ve bunları çiğneyen sadece kendi prestijine değil, mesleğe de zarar verir. Durkheim'a göre meslek etiği, bir grubun ürünüdür. Meslek etiği, grup tarafından korunduğu sürece yürürlükte kalabilen, bireylere emreden, onları belirli bir şekilde davranmaya zorlayan, kişisel eğilimleri sınırlayan kurallardan oluşmuştur.⁵³⁰

Meslek etiği bir anlamda bir mesleğin üyelerinin uyacağı standartları belirten kurallar bütünü olmasından dolayı o meslek üyelerini sınırlar ve yönlendirir. Nasıl ki hipokrat yemininin doktorları sınırlaması, polis meslek etiğinin emniyet örgütü personelini sınırlaması ve yönlendirmesi gibi, her meslek kendi meslek etiğini üretir ve bu etik ilkeler sadece bu mesleği seçenleri bağlar. Bir ülkede iktidar adına denetim ve gözetim faaliyetlerini yerine getiren, hatta güvenliği temin etme gayesiyle bütün bilgi - iletişim teknolojilerini izleyen ve bunlardan elde edilen verileri toplayıp, değerlendiren ve analize tabi tutanlar istihbarat ve güvenlik birimleridir. Güvenlik gayesi çerçevesinin dışına çıkmaması ve bunda da ölçülü hareket etmesi açısından güvenlik birimlerinin kendi meslek etik yapıları önem arz etmektedir.

Polis meslek etiği, kamu düzenini koruma ve suçları önleme, suç oluşuktan sonra faillerin hızlıca bulunarak suçun aydınlatılmasını sağlama, bireysel hak ve özgürlüklere dikkat etme ve onları koruma, hukukun üstünlüğüne uygun davranma davranışları çerçevesinde

⁵²⁸ İnayet Pehlivan, *Yönetmel Mesleki ve Örgütsel Etik*, Pegem Yayınları, Ankara, 1998, s.5.

⁵²⁹ Annemarie Pieper, *Etiğe Giriş*, Çev. Veysel Atayman, Ayrıntı Yayınları, İstanbul, 1999, s.40.

⁵³⁰ a.k, s.85.

güvenlik görevlilerinin görev alanlarına giren konulardaki uygulamalarda davranışlarını standartlaştıran, hizmet ideallerini korumayı amaçlayan ilkeler bütününe ifade etmektedir.⁵³¹

Dünya genelinde kolluk görevlilerinin varlık sebebinin insan hak ve özgürlüklerinin rahatça kullanılabileceği bir ortamı; yani kamu düzenini sağlamak ve korumak olduğu bilinmektedir. Bu noktada kamu görevlileri özel hayatın güvenliğini sağlamak için özel hayatın gizliliğine müdahale edebilme yetkisine sahiptirler. Bazı kolluk görevlileri bu yetkiyi sınır tanımaz bir şekilde kullanabilmektedirler. Halbuki bu yetkinin kullanılabilmemesinin çok ağır şartların gerçekleşmiş olmasına bağlı olması gerekmektedir. Dolayısıyla kolluk görevlilerinin bu yetkileri sınırlıdır.⁵³² Sınırlı olan bu yetkilerin kullanılmasının denetimi çoğu zaman mümkün olmayabileceği için bu noktada devreye meslek etiğinin gruptan dışlama, ötekileştirme, hakir görme gibi yaptırımları devreye girebilmektedir.

1789 tarihli Fransız İnsan ve Yurttaş Hakları Beyannamesi'nin 12. maddesine göre insan ve yurttaşlık haklarının garanti altına alınması mutlaka bir kolluk gücünü gerektirmektedir. “Ancak bu güç kamu yararına kurulmuş olup bu gücü elinde bulunduranların yararına kullanılamaz” denilerek kolluk hizmetinin sınırı ortaya konulmuştur.⁵³³

Kolluk görevlileri eylemlerinde bireysel çıkarları ile kamusal/kurumsal çıkarlar dikatomisi içinde kalabilmektedir. Bu durumu Şen, “çıkar çatışması” olarak ifade etmektedir. Ona göre bir takım kamu görevlileri para, makam, saygınlık gibi kişisel çıkarlarını kamusal çıkarlara tercih edebilmektedirler.⁵³⁴ Bu durumda kamu görevlileri etik olmayan tarzda hareket etmektedirler. Zira gerçekleştirdikleri eylemleri kamu görevlisi olma değerleri ile çelişmektedir.

Yukarıda belirtilen etik olmayan davranışlar bazen kuralların açık ve net olmamasından da kaynaklanabilmektedir. Şen, “Kamu çıkarlarına göre hareket et!”, “Çalışanların ve yurttaşların kişilik haklarını koru!”, “Halka etkili, verimli ve dürüst hizmet sun!” gibi kural ve emirlerin pratikte içeriklerinin semantik olarak bilinemediğini, içeriği açık olan kurallar varken de ilgili kamu görevlisinin yanlış temellendirmeler yaparak kurallara uymayan davranışlar sergileyebildiğini, ya da bazen kuralların kendi içinde ihtilaf halinde olabildiğini ifade etmektedir. Mesela “gizli bilgilerin açıklanmaması” ve “açıklık politikası

⁵³¹ İhsan Bal, Fatih Beren, *Polis Etiği*, Siyasal Kitabevi, Ankara, 2003, s.61.

⁵³² Mustafa L. Şen, “Kamu Yönetiminde Yozlaşmanın Önlenmesinde Yönetimsel Etik Yaklaşımı”, Basılmamış Doktora Tezi, *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı*, İzmir, 1998, s.96.

⁵³³ a.k

⁵³⁴ a.k

gereği şeffaf olunması” genel olarak tüm ülkelerde kamusal kurallardandır. Bu durumda hangi bilgilerin şeffaflık kapsamına gireceği hangi bilgilerin de açıklanmaması gereken grubuna gireceği belli değildir ve bunun net bir sınırını çizmek oldukça zordur.⁵³⁵

Kolluk, görevini yerine getirirken, kişiler ve kurumlar hakkında elde ettiği özel ve gizli bilgileri ve muhbirlerin kimliklerini yasaların belirttiği durumlar dışında saklı tutmak, kendi dahi kullanmamak zorundadır. Kolluk, yasal gerekçeler oluşmadıkça yurttaşın haberleşmesine, konutdokunulmazlığına, aile ve özel hayatına müdahale edemez. Yasalara uygun yapılan müdahalelerde hiçbir zaman yetki sınırlarını aşmaz.⁵³⁶

Güvenlik birimleri, kişilere ait bilgileri toplarken, kaydederken ve kullanırken ancak yasal ve meşru amaçların gerçekleştirilmesini sağlayacak kadar işlem ve eylemde bulunabilir. Bu birimlerin yurttaşların temel hak ve özgürlüklerini kısıtlayıcı yetkilerini kullanırken yasalar çerçevesinde hareket etmesi gerekmektedir.⁵³⁷ Aksi şekilde yapılacak eylemler görevin kötüye kullanılması olacaktır.

Yasal olmayan yollardan elde edilen deliller günümüzde hukuki bir anlam ifade etmemektedir. Örneğin bir bölgede suçun önlenmesi ya da aydınlatılması amacıyla, suç işleyen ya da potansiyel suçlu görülen kişilerin hukuka aykırı yollarla gözetlenerek tespitiyle suç oranları azaltılmış olması o bölgedeki güvenlik hizmetlerinin başarısını göstermemektedir. Etik değerlerin polislik mesleğine uygulanmasının bir sonucu olarak, güvenlik hizmetlerinin başarısı, sadece suçun önlenmesi değil, suçun önlenmesi ya da aydınlatılması aşamasında, şüphelilere hukuk çerçevesinde ve insan haklarına uygun olarak muamelede bulunulmasıyla gerçekleşmektedir.

5. Bilişim Suçları

Bilgi ve iletişim teknolojileri özellikle 2000’li yıllardan sonra çok hızlı bir şekilde sayı, çeşit, kapasite, kullanım oranları gibi konularda gelişme sağlamıştır. Teknolojinin hızla gelişmesiyle bir zamanlar bir odanın içine ancak sığdırılabilen çok düşük kapasiteli bilgisayarların şimdilerde çok daha gelişmiş olanları avuç içinde kullanılabilmektedir. Diğer taraftan özellikle internetin ortaya çıkması ve günümüzde dünya genelinde yaygınlık kazanmasıyla birlikte mekan kavramı bir anlamda ortadan kalkmış, kıtalararası iletişim ve veri transferi çok hızlı ve kolay bir şekilde yapılabilmektedir.

⁵³⁵ a.k

⁵³⁶ Avrupa Polis Etigi Kuralları’nın 41 inci maddesinden yararlanılmıştır.

⁵³⁷ Avrupa Polis Etigi Kuralları’nın 42 nci maddesinden yararlanılmıştır.

Bilişim teknolojilerindeki hızlı gelişme, insanoğluna sunduğu yararlarla beraber birçok olumsuzluk da getirmiştir. Bunlardan belki de en önemlisi bu teknolojilerin birer suç makinesi gibi kullanılabilir olmasıdır. Nitekim günümüzde bu teknolojilerin giderek yaygınlaşmasıyla klasik suçların bu sanal teknolojiler vasıtasıyla işlenmesiyle birlikte daha önce karşılaşılmayan yeni dinamik suç tipleri de ortaya çıkmıştır.⁵³⁸

Bilişim teknolojileri ile suç işlemek klasik suçlara göre daha kolaydır ve fail kimliğini daha rahat gizleyebilmektedir. Bu bakımdan suç işlemeye meyilli olanlar, suç örgütleri de bu teknolojileri takip eder olmuş ve bu teknolojileri suç işlemede nasıl kullanabileceğini, illegal yollarla nasıl para kazanılacağını planlar olmuştur. İşte bu yeni hızla yayılan bilişim teknolojileri ile işlenen suçlara bilişim suçları denilmektedir. Bu suçlar etrafıca incelenmeden önce bilişim ve bilişim suç kavramlarının anlamlarına değinilecektir.

Fransızca “*Informatique*” kelimesinden Türkçeleştirilen ve “Enformatik” olarak da kullanılan, bilişim kavramının birçok tanımlaması bulunmaktadır. Bu tanımlamalardan bazıları şöyledir. Bilişim kavramının sözlük anlamı, Türk Dil Kurumu'nun Bilim ve Sanat Terimleri Ana Sözlüğünde şöyle ifade edilmiştir.⁵³⁹

“İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalı.”

Akbulut’a göre bilişim;⁵⁴⁰

“... İnsanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin temeli olan bilginin elektronik araçlarla özellikle bilgisayarlar aracılığıyla işlenip, ses, görüntü ve veri taşıyan iletişim hatları aracılığıyla aktarılması bilimidir.”

Dülger’e göre bilişim;⁵⁴¹

“İnsanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişimde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir.”

Genel olarak tanımlara bakılacak olursa bilişim; bilgi ve iletişim teknolojilerini kullanarak her türlü verinin, otomatik olarak işlenmesi, saklanması, organize edilmesi, değerlendirilmesi, depolanması ve aktarılması ile ilgili bilim dalı olarak tanımlanabilir. Diğer taraftan bilişim bilgi teknolojilerinin tümünü kapsayan bir üst kavram olarak karşımıza

⁵³⁸ Elektrik Mühendisleri Odası, “Elektronik Gözaltı Dünyası: e-Göz@ltı”, www.emo.org, (Erişim Tarihi: 28.08.2013).

⁵³⁹ Türk Dil Kurumu Bilim ve Sanat Terimleri Ana Sözlüğü.

⁵⁴⁰ Berrin B. Akbulut, “Bilişim Suçları”, *Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı*, S. 1 - 2, C.8, 2000, s.546.

⁵⁴¹ Murat V. Dülger, *Bilişim Suçları*, Seçkin Yayınevi, Ankara, 2004, s.47.

çıkılmaktadır. Nitekim her bilişim sisteminde mutlaka bilgisayar olması gerekmez ancak her bilgisayar mutlaka bir bilişim sistemi olarak kabul edilebilir.

Dönmezer bilişim suçlarını; bilgisayarın kötüye kullanılması, bilgileri otomatik işleme tabi tutulmuş ve verilerin nakline ilişkin kanuna ve meslek ahlakına aykırı davranışlar olarak tanımlamaktadır.⁵⁴² Parker bilişim suçlarını, bilgisayar teknolojisi bilgisi ve kullanımı içeren, faile çıkar sağlayan ve ona bir takım şeyler kazandıran herhangi bir kasıtlı davranış şeklinde ifade etmiştir.⁵⁴³ Yazıcıoğlu ise bilişim suçlarını, ceza kuralları uyarınca, bilgisayar konulu, araçlı suç olgusu içeren fiiller biçiminde tarif etmektedir.⁵⁴⁴

Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun 1983 yılının Mayıs ayında Paris Toplantısı'nda yaptığı tanımlamaya göre bilişim suçları; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır."⁵⁴⁵ Bilişim suçu literatürde bilgisayar suçu, bilişim ihlali, bilişim suçluluğu, bilgisayar vasıta kullanılarak işlenen suç, bilgisayarın kötü niyetli kullanımı, internet suçu, siber suç, dijital suç, yüksek teknoloji suçu, bilgi teknolojileri suçu olarak da ifade edilmektedir.⁵⁴⁶ Bu kavram çalışma boyunca bilişim suçları olarak ifade edilecektir.

Bilişim suçları, tek bir bilgisayar vasıtasıyla işlenebileceği gibi bir ağ, internet, ufak bir elektrik devresi, cep telefonu gibi bilgi ve iletişim teknolojileri araçlarının her türlü ile de işlenebilir.⁵⁴⁷ Esasında bilişim nasıl ki bilgi teknolojilerinin tümünü kapsayan bir üst kavram ise bilişim suçları da bilgi ve iletişim teknolojileri kullanarak veya bunlara karşı işlenen bütün suçları ifade etmektedir.

Bilişim suçlarını, klasik suçlardan ayıran özelliklerden en önemlisi, bu suçların işleniş şekillerinin tespitinin zor oluşudur. Söz konusu suçlar, yepyeni ve çok farklı yollarla işlenebilmektedirler.⁵⁴⁸ Klasik suç olarak tanımlanan adam öldürme, adam yaralama, dolandırıcılık, sahtecilik, hırsızlık vb. gibi suçlarda suçun maddi unsurunu oluşturan eylemler failerin fiziki hareketleridir. Ancak bilişim suçlarında ise fail bir bilişim sistemini kullanarak, suçun etkisinin olduğu yerden kilometrelerce ötede olabilmekte ve buna rağmen suçun

⁵⁴² Sulhi Dönmezer, *Ceza Hukuku El Kitabı*, İstanbul, 1989, s.504.

⁵⁴³ Donn B. Parker, *Computer Crime: Criminal Justice Resource Manual*, 1989., akt., Osman N. Şen, "Polisin Bilişim Suçlarıyla Mücadelede Yapması Gerekenler", *1. Polis Bilişim Sempozyumu*, Ankara, 2003, s.70 - 71.

⁵⁴⁴ Yılmaz Yazıcıoğlu, *a.g.k.*, s.142.

⁵⁴⁵ Şükrü Durmaz, *Bilişim Suçlarının Sosyolojik Analizi*, Ankara, 2006, s.4.

⁵⁴⁶ *a.k.*, s.69.

⁵⁴⁷ Dilek Y. Civelek, "Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi", *Uzmanlık Tezi*, Bilgi Toplumu Dairesi Başkanlığı, Yayın No: 2821, Ankara, 2011, s.25.

⁵⁴⁸ *a.k.*, s.36.

neticesinde çok büyük zararlar verebilmektedir. Dolayısıyla suçun maddi unsurunu dijital hareketler oluşturmaktadır.⁵⁴⁹

Klasik suçların işlenmesinde tasarlama, hazırlık, keşif, icra gibi farklı aşamalardan oluşan bir süreç söz konusu iken bilişim suçlarında buna gerek kalmamaktadır. Örneğin basit bir hırsızlık suçunu işlemede bile suçlu suç öncesinde hırsızlık yapacağı mekana giderek araştırma vs. çalışmaları yaparken, bilişim suçları saniyelerle ifade edilebilecek kısa sürede işlenebilmektedir. Kimlik hırsızlığı suçunun işlenmesiyle ilgili olarak tüm Türkiye'deki yurttaşların kimlik ve adres bilgilerinin, bulunduğu kaynaktan kopyalanması ancak bir kaç dakika sürebilir ve belki çoğu zaman sistemin başındaki teknik personel de bu saldırıyı günler sonra farkedebilir. Bilişim suçlarının bu kadar kısa süre içinde işlenebilmesi de delillerin tespiti ve toplanmasını zorlaştırmaktadır ve bu açıdan klasik suç tiplerinden ayrılmaktadır.⁵⁵⁰ Bilişim suçlarının diğer bir ayırt edici özelliği de bu sistemlerde işlenen suçun tipine göre mağdurun belli olmamasıdır. Fail kimin malını aldığını bilmemekte, mağdur sistem olarak gözükmektedir. Bu durumda güvenlik güçleri için hem failin hem de mağdurun tespiti oldukça zorlaşmaktadır.⁵⁵¹

Bilişim suçlarında karşımıza çıkan önemli bir unsur da, suçluların kimliklerini gizleyebilme kolaylığının bulunmasıdır. Kendi kimliğini gizlemek isteyen suçlular, daha sonra ayrıntılarına gireceğimiz çeşitli tekniklerle, başka kullanıcıların bilgisayarlarını ele geçirip, gerçek kullanıcıların haberleri bile olmadan bu bilgisayarları kendi işleyecekleri suçlarda kullanabilmektedirler. Hatta başkasının bilgisayarından işlenen bu suçlarda da IP değiştirici kullanarak örneğin bilgisayar Türkiye'de ise sanki Japonya'daymış gibi bir izlenim verilebilmektedir. Bu durumda da failin tespiti imkansızlaşmaktadır. Bu noktada genel kullanıma açık olan internet kafelerin, kablosuz internet erişim noktalarının artması, bluetooth, GPRS gibi teknolojilerin ortaya çıkmasıyla beraber, suçlunun izini takip etmek neredeyse imkansız bir hale gelmiştir.

Bilişim suçlarını işleyen suçluların diğer klasik suçları işleyenlerin geneline nazaran bilgi ve eğitim seviyeleri daha yüksektir. Hatta genelde bunlar iyi bir üniversite mezunu veya öğrencisidir. Nitekim bilişim suçlarını işlerken arkada iz bırakmama, kendisinin tespit

⁵⁴⁹ Murat V. Dülger, *a.g.k.*, s.69.

⁵⁵⁰ *a.k.*

⁵⁵¹ Dilek Y. Civelek, *a.g.k.*, s.20.

edilmemesini sağlamak için gelişmiş yazılımları ve ileri teknoloji ürünlerini kullanabilme kabiliyeti gerekir ki bu da örneğin bir inşaat işçisinin yapabileceği bir şey değildir.⁵⁵²

Doktrinde bilişim suçları çeşitli şekillerde sınıflandırılabilir. Ancak bunların sınıflandırılmasında ortaya çıkan karışıklık bu sınıflandırmanın suçların işlenme şekillerine göre mi yoksa neticede elde edilmek istenilen amaçlara göre mi olacaktır. Doktrinde suç tipleri arasındaki farkı oluşturan esas etkenin “suçun işlenmesindeki amaç” olduğu kabul edilmektedir. Dolayısıyla bilişim suçları hangi yöntemle işlenirse işlensin, hangi amaca hizmet ettiğine bakmak gerekir. Mesela bir bilgisayar sistemine girmek için birçok yöntem bulunabilir; bir virüs veya trojan kullanarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Burada önemli olan suçlunun amacının “sisteme izinsiz girme” eylemi olmasıdır.⁵⁵³ Avrupa Ekonomik Topluluğu (AET), bir tavsiye kararında bilişim suçlarını beşe ayırmıştır:⁵⁵⁴

“Bilgisayarda mevcut olan kaynağa veya herhangi bir değere gayri meşru şekilde ulaşarak transferini sağlamak için kasten bilgisayar verilerine girmek, bunları bozmak, silmek, yok etmek; bir sahtekarlık yapmak için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek; bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek; ticari manada yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmak; bilgisayar sistemi sorumlusunun izni olmaksızın, konulmuş olan emniyet tedbirlerini aşmak suretiyle sisteme kasten girerek müdahalede bulunmaktır.”

Yukarıda AET tavsiye kararında bilişim suçlarının ayrımında net bir tavır sergilense de esasında böyle bir sınırlandırma yapmanın doğru olmadığı söylenebilir. Çünkü gelişen teknolojiyle birlikte her geçen gün yeni bilişim suç tipleri ortaya çıkmaktadır. Dolayısıyla birkaç sene sonra, yapılan bu sınıflandırma bilişim suçlarını kategorize etmede yetersiz hale gelebilir. Bu bakımdan günümüzde karşılaşılan bazı bilişim suç tiplerinden bahsedilecektir. Bilgisayar sistemlerine ve servislerine yetkisiz erişim olarak ifade edilen kişinin bir bilgisayar sistemine ya da bilgisayar ağına yetkisi olmadan illegal yollarla ve çeşitli bilişim kurnazlıklarıyla sistemin zayıf bir noktasını bularak ulaşması en çok karşılaşılan bilişim suçlarından. Burada suçun hedefi bir bilgisayar sistemi ya da ağıdır ve erişim, sistemin bir kısmına ya da bütününe, programlara veya içerdiği verilere ulaşma şeklinde olabilmektedir.⁵⁵⁵

Bilgisayar sabotajı; bilgi ve iletişim teknolojileri kullanılarak bilgisayar ve bilgisayar ağlarına izinsiz erişerek buralardaki verilerin silinmesi, değiştirilmesi veya yok edilmesi şeklinde olabileceği gibi bilgi ve iletişim teknolojileri kullanılmadan doğrudan fiziksel olarak

⁵⁵² Murat V. Dülger, *a.g.k.*, s.69.

⁵⁵³ Semih Dokur, “Adli Bilişim”, www.logyonetimi.com/doc/adlibilisim.pdf, (Erişim Tarihi: 11.03.2013).

⁵⁵⁴ Dilek Y. Civelek, *a.g.k.*, s.20.

⁵⁵⁵ Interpol Siber Suçlar Birimi Notları, <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>, (Erişim Tarihi: 11.03.2013).

bu sistemlere ulaşılarak bilgisayar veya bilgisayar ağlarındaki verilerle ilgili izinsiz yapılan işlemleri ifade etmektedir.⁵⁵⁶ Kimlik hırsızlığı; gerçek veya tüzel kişilere ait kişisel verilerin yetkisiz kişilerce, dolandırıcılık veya diğer suçların işlenmesinde kullanılmak üzere ele geçirilmesi, iletilmesi, depolanması veya kullanılması olarak tanımlanabilir.⁵⁵⁷ Örnek olarak internet üzerinden kişilerin kimlik bilgilerinin temin edilerek, sahte nüfus cüzdanı, sahte pasaport, sahte sürücü belgesi yapılmasını gösterebiliriz.

Bilgisayar yoluyla dolandırıcılık; kendisine veya başkasına yasal olmayan ekonomik fayda temin etme veya mağdura mali açıdan zarar verme amacıyla bilgi ve iletişim teknolojileri kullanılarak başkalarının verilerine izinsiz ulaşım ve bu verileri kullanmayı ifade etmektedir. Bilgisayar yoluyla dolandırıcılık en çok internet üzerinden başkalarına ait kredi kartı bilgilerinin kullanılarak internet bankacılığı yoluyla bu hesaplardaki paraların başka hesaplara geçirilmesi şeklinde işlenmektedir. Bunun için üretilmiş birçok sanal kredi kartı oluşturucu programlar bulunmaktadır.⁵⁵⁸ Bu tip program ve sistemler sayesinde internet üzerinden bankacılık veya elektronik alışveriş işlemlerinde kredi kartının sahibi banka için mantıksal olarak muhtemel kredi kartı kullanıcı bilgileri oluşturulmakta ve kredi kartının hamilinin haberi olmadan bu kart içerisindeki paralar kullanılabilir.

Banka kartı dolandırıcılığı; başkalarına ait bankamatik veya kredi kartlarının fiziksel olarak kopyalanması ve çoğaltılması şeklinde olabilmektedir.⁵⁵⁹ Örnek olarak bankamatik sistemlerine (*İng; ATM - Automated Teller Machine*) gizli kart okuyucu sistemleri yerleştirilerek kart bilgilerinin bu okuyucularda toplanmasını, daha sonra da suçluların bu bilgileri kullanarak sahte kredi kartı veya bankamatik kartı oluşturmalarını gösterebiliriz. Kanunla korunmuş bir yazılımın izinsiz kullanımı; çeşitli telif sözleşme ve kanunlarıyla lisans hakkı korunan bilgi ve iletişim teknolojileri yazılımlarının izinsiz olarak kopyalanması, çoğaltılması, satılmasını ifade etmektedir.⁵⁶⁰ Günümüzde örneğin Türkiye’de resmi kurumlar dışında Microsoft vb. ana bilgisayar yazılımlarını lisanslı olarak kullanan sayısının çok az olduğu bilinmektedir.

Kişisel verilerin kötüye kullanılması; kişisel verilerin, ticari ya da mesleki sırlarının ya da değerli diğer verilerin kendisine veya başkasına menfaat sağlamak ya da zarar vermek amacıyla kişi veya kurumların rızası ve izni olmadan temin edilerek kullanılması, satılması

⁵⁵⁶ a.k

⁵⁵⁷ OECD, “OECD Policy Guidance on Online Identity Theft”, Haziran 2008.

⁵⁵⁸ Interpol Siber Suçlar Birimi Notları, <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>, (Erişim Tarihi: 11.03.2013).

⁵⁵⁹ a.k

⁵⁶⁰ a.k

veya başkalarına dağıtılmasını ifade etmektedir.⁵⁶¹ Bu veriler kişilerin kimlik, adres, telefon, e-posta bilgileri veya kurumların halka açık olmayan istatistikleri, raporları, bilgi edinme başvuruları, ihbarları gibi çok çeşitli olabilir.

Yetkisiz dinleme; bir bilgisayar veya ağ sistemi aracılığıyla yapılan iletişimin veya sinyal bilgilerinin hukuka aykırı ve izinsiz olarak teknik anlamda dinlenmesi ve takip edilmesini ifade etmektedir.⁵⁶² Burada suçun hedefi her türlü bilgisayar ve telekomünikasyon iletişimidir. Bunlar kişilerin *Msn, Facebook, Google Talk, Skype* gibi kapalı mesaj trafiği yapan programlar üzerindeki mesajlaşmalarını başkasının görmesi ve takip etmesi şeklinde olabileceği gibi, gelişmiş bilişim cihazlarıyla hukuka aykırı olarak başkasının telefon görüşmelerini dinleme veya ortam dinlemesi yapma şeklinde de olabilmektedir.

Terör örgütlerinin, örgütsel propaganda faaliyetlerini, örgüt üyelerinin birbirleri arasındaki haberleşmelerini, taraftar kazanma ve toplumda infial oluşturma faaliyetlerini yapmak için oluşturdukları internet siteleri, gönderdikleri elektronik postalar terörist saldırılar olarak kategorize edilebilir.⁵⁶³ Hem suç faillerinin bulunmasının zorluğu, hem de dinamik bir suç alanı olması nedeniyle bilişim suçlarıyla mücadele oldukça zordur. Durum böyleyken bilişim suçları sayı ve çeşit olarak da her geçen gün artış göstermektedir. Bu suçlarla mücadelenin en kolay yolu bunlara karşı gerekli tedbirlerin alınması, sistemlerin güvenlik açıklarının tespit edilerek onarılmasıdır.

Bu bölümde bilişim suçlarıyla mücadelede alınabilecek tedbirlerden bahsedilecektir. Bu suçlarla mücadelede öncelikle bilişim sistemlerinin fiziksel güvenliğinin sağlanması gerekir. Fiziksel güvenlik anlamında; bilgileri çoğaltmak, taşımak veya arşivlemek amacıyla kullanılan disket, CD, harici bellek ve diğer harici hafıza birimleri mutlaka emniyetli bir yerde muhafaza edilmeli⁵⁶⁴, özellikle kurumlarda sistem odaları oluşturulmalı ve bu sistem odaları kamera, görevli personel tarafından yedi gün yirmi dört saat gözlem altında tutulmalıdır.⁵⁶⁵

Veri güvenliği, kurumsal bir politika çerçevesinde belirlenmeli ve çeşitli standartlar oluşturulmalı, tüm kurum çalışanları için uymaları gereken kurallar bu politika çerçevesinde tanımlanmalıdır. Bilişim sistemlerinde görevli personel eğitilmiş, teknik yetenekleri en az

⁵⁶¹ İsmail Tulum, “Bilişim Suçları ile Mücadele”, *Yüksek Lisans Tezi*, Süleyman Demirel Üniversitesi, Isparta, 2006, s.36.

⁵⁶² Interpol Siber Suçlar Birimi Notları, <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>, (Erişim Tarihi: 11.03.2013).

⁵⁶³ İsmail Tulum, *a.g.k.*, s.36.

⁵⁶⁴ Berrin B. Akbulut, *a.g.k.*, s.545 - 555.

⁵⁶⁵ www.rtuk.org.tr, (Erişim Tarihi: 17.07.2013).

sisteme saldırmak isteyenler kadar yüksek olmalıdır. Sistemlerde bütün kullanıcıların yetkileri şifrelerle tespit edilmeli ve düzenli olarak işlem kayıtları (*log* kayıtları) görevli sistem yöneticisi tarafından kontrol edilmelidir.⁵⁶⁶ Örneğin, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü sistem odasında çalışan bir teknik personelin tüm Türkiye’deki yurttaşların kimlik, adres ve telefon bilgilerini çalma ihtimali sürekli gözönünde bulundurulmalı ve teknik personelin işlemlerini de denetleyecek güvenilir personelin olması gerekmektedir.

Bilişim sistemlerinden sorumlu sistem yöneticileri, sisteme yabancı kaynaklardan gelebilecek sızmaları fark edebilecek ve sistemin açıklarının neler olduğunu tespit edebilecek kadar teknik bilgi seviyesine sahip olmalı, dışarıdan yapılabilecek müdahalelere karşı koyabilecek kapasitede olmalıdırlar.⁵⁶⁷ Ayrıca bilgisayarlarda lisanslı olarak anti virüs programları kullanılmalı, bunlar düzenli olarak güncellenmelidir.⁵⁶⁸

Bilişim suçlarına karşı yukarıda belirtilen veya benzeri tedbirler ne kadar yoğunlukta alınıralsa alınsın, mutlaka sistem içerisinde güvenlik açıkları olacaktır. Zira bilişim sistemleri esasında barındırdıkları bu güvenlik tehditleri dolayısıyla suç işlenmesine müsait sistemlerdir. Çünkü bir sonraki teknolojik gelişme bir önceki teknolojik gelişmenin ne kadar güvenilmez olduğunu göstermektedir ve bu böyle sürecelecektir. Bilişim güvenliği olarak, bilgi ve iletişim sistemlerinin üreticisi olmalarından dolayı en üst seviyede görülen Amerika Birleşik Devletleri Savunma Bakanlığı (Pentagon), NATO, NASA, CIA gibi kurumların bilişim sistemlerine bile bilgisayar korsanları tarafından sızılabilmiş, birçok önemli veri çalınabilmiştir.⁵⁶⁹ Bilgisayar korsanları tarafından bu teknolojiye başat rol alan Microsoft’un bile ana sunucularına girilerek kullanıcıların iki gün boyunca Microsoft’un sitelerine girememesine yol açılmıştır.⁵⁷⁰

Bütün bunlar şunu göstermektedir ki bilişim sistemleri kamusal ve günlük hayat anlamında sağlamış olduğu çoğu faydaya rağmen tehlikeli ve güvenilmezdir. İşin kötü tarafı ise bilişim güvenliğini temin edecek olan güvenlik birimlerinin bu tehlike ve güvenilmezliği esas alarak fiziksel alandaki gözetim faaliyetlerini bilişim alanına da kaydırmasıdır. Bu bakımdan güvenlik birimleri için bütün bilişim sistemi kullanıcıları güvenilmez ve riskli

⁵⁶⁶ İsmail Tulum, *a.g.k.*, s.81.

⁵⁶⁷ *a.k*

⁵⁶⁸ Yılmaz Yazıcıoğlu, *a.g.k.*, s.86.

⁵⁶⁹ Council of Europe, “Organised Crime Situation Report: Focus on The Threat of Cybercrime”, *Strasbourg*, 10 Eylül 2004.

⁵⁷⁰ Ercan Kurt, “Hacker’lığın Kısa Tarihçesi”, <http://www.olympus.org/article/articleview/283/1/10>, 2004, (Erişim Tarihi: 17.07.2013).

olarak değeriendirilecek ve bundan dolayı tüm bilişim ağlarındaki her dokunuşun incelenmesi ve izlenmesi makul görülecektir.

ÜÇÜNCÜ BÖLÜM

TÜRKİYE'DE GÖZETİM VE GÜVENLİK: TÜRKİYE EMNİYET TEŞKİLATI

Günümüzde içinde bulunduğumuz dönem; teknoloji çağı, bilgisayar ve elektronik çağı, uzay çağı gibi yakıştırmalarla ifade edilmektedir. Bilgi ve iletişim teknolojileriyle birlikte günümüzde bu yakıştırmaları hak edecek gelişmeler yaşanmaktadır. Yurttaşların bilgi ve iletişim teknolojilerini kullanma oranının her geçen gün artış gösterdiği gözlenmektedir. Dolayısıyla bilgiye dair olanla bir iç içelik durumu söz konusudur. İnternetin yaygın bir şekilde kullanılması, akıllı cep telefonlarının satışlarının artış göstermesi⁵⁷¹, *Twitter* ve *Facebook* sosyal paylaşım sitelerinin kullanıcı sayılarındaki müthiş yükseliş, kamu hizmetlerinin e-devlet üzerinden verilmeye başlanması buna örnek gösterilebilir.

Türkiye'nin de içinde bulunduğu bilgi toplumu sürecinin en önemli lokomotif olan bilgi ve iletişim teknolojilerinin gelişimi kapitalist süreçte olduğu gibi eşit ve adil değildir. Kapitalist sistemin eşitsiz gelişiminin neden olduğu eşitsizlikler bilgi ve iletişim teknolojilerinin dünya bazında genişleme ve derinleşme süreci için de geçerlidir. Teknolojinin mülkiyeti merkez ülkelerde olduğu sürece, çevre ülkelerde bilgi ve iletişim teknolojilerinde meydana gelecek olan gelişmeler yukarıdan inme ve yapay bir eğilimde olacaktır; dolayısıyla bu süreç çevre ülkelerde verimlilik, kalite, hızlilik, etkinlik gibi sistemin avantajlarında başat rol oynayan etkilerin kendini göstermesinden ziyade çevre ülkelerin merkez ülkelere daha çok bağlanmasına neden olacak, bir bakıma merkez ülkelerin sömürü gücü daha çok artacaktır. Bilgi ve iletişim teknolojileriyle birlikte geçmişe göre merkez ülkelerin çevre ülkeler üzerindeki sömürü metot ve tekniklerinin şekil değiştirdiği ifade edilebilir.⁵⁷²

Türkiye'deki bilgi toplumuna evriliş süreci de merkez ülkelerin etkisiyle şekillenmiştir. Sürecin başlama düdüğünü toplumun kendi özgür iradesi değil Dünya Bankası, AB, GATT, uluslararası diğer kuruluşlar çalmıştır. Dolayısıyla süreç ülkenin her yerinde adil koşullarda, bütün yurttaşların sürece dahil olabileceği metodu yerine yukarıdan dayatma, mecbur kılma şeklinde ilerlemiştir.

⁵⁷¹ Gartner Uluslararası Araştırma Şirketi'nin yaptığı çalışma neticesinde 2012 yılında dünyada toplam 1,75 milyar akıllı cep telefonu satıldığı ortaya çıkmıştır. <http://www.gartner.com>, (Erişim Tarihi: 20.12.2013).

⁵⁷² Nurcan Törenli, *a.g.k.*, s.193.

Türkiye’de bu gelişmeler özellikle 2000’li yıllardan itibaren kamuda, devlet kurumlarında hayata geçmiş; e-devlet projeleri birer kurtuluş reçetesi olarak görülmeye başlanmıştır. Bu elektronik kamu hizmet unsur ve bileşenlerinin kırtasiyeciliği kaldırmak, hızlılık - etkinlik gibi avantajlarının olduğu bir gerçektir. Ancak toplumsal altyapıyı hazırlamadan, kamu hizmetlerindeki yapısal sorunlara çözüm bulmadan Alaaddin’in sihirli lambası gibi bu değişim sürecine ön kabul ile sorgulamaksızın bağlanmak da doğru değildir. Zira kamu hizmetlerinde yapısal sorunlar devam etmektedir ve elektronik devlet bu sorunları çözecek değildir, çünkü sadece hizmetlerin veriliş biçimini değiştirme orijinlidir.

Günümüzde Türkiye’de meydana gelen e-devlet sürecinin Emniyet Teşkilatı da bir parçasıdır. Bu kapsamda e-devlet sürecinin yansımaları olarak kendi bünyesinde Polnet, Mobese ve diğer kurumsal intranet ağlarını oluşturmuştur. Bu projelerin aktif olarak uygulanmasıyla suç oranlarında ve aydınlatılamayan suç olaylarında düşüş olduğu, bombalı saldırılar gibi büyük tehlikelerin önlenmesinde büyük başarılar sağlandığı ifade edilmektedir. Kurumsal olarak da kırtasiyecilik, iş yükü, zaman kaybı azaltılarak hizmet verimliliğinin arttırıldığına yönelik çeşitli tespitler bulunmaktadır. Ancak bilgi ve iletişim teknolojilerinin toplumsal dönüşümde meydana getireceği çıkmazlar, olumsuz döngüler, yapısal hastalıklar bu teknolojileri giderek artan oranda kullanan Emniyet Teşkilatı için de geçerlidir.

Bireyler bilgi ve iletişim teknolojilerini ne kadar çok kullanırsa o kadar çok gözetim teknolojilerini kullanıyor ya da hedefine oturuyor demektir. Neticede bilgi ve iletişim teknolojilerinin gelişimiyle doğru orantılı olarak her geçen gün artan oranda iktidar güçlerine bilerek veya bilmeyerek kendisi hakkındaki bilgiyi teslim etmektedir. Bu bakımdan iktidarın her şeyi bilmek, her şeye hakim olmak için teknolojik gelişmeleri fırsat bildiği ifade edilebilir. Bu durum ülkemiz için de geçerlidir. Gerek toplumsal anlamda başta internet olmak üzere bilgi ve iletişim teknolojilerini yoğun kullanarak, gerek e-devlet bilgi toplama araçlarına her geçen gün daha çok bilgi vererek günümüz gözetim dünyasında iktidar tarafından öngörülebilir varlıklara dönüştürülmeye bilerek veya bilmeyerek icazet verilmektedir. Bu gözetim faaliyetlerini meşrulaştırıcı araç olarak güvenlik kartı da bireye karşı çekildiğinde birey bu faaliyetlere olan direncini de kaybetmekte, kendisini iktidarın gözetim araçlarının kollarına bırakıvermektedir. Çalışmanın bu kısmında temel olarak Emniyet Teşkilatı’nın iktidarın gözetim aracı olma fonksiyonu eleştirilecektir.

Bu bölümde önceki bölümlerde anlatılanların genelde Türkiye özelde Emniyet Teşkilatı yansıması incelenecektir. Öncelikle Türkiye’nin bilgi toplumuna evriliş süreci ve bu bağlamda gerçekleştirilen e-devlet projeleri ile meydana gelen gözetim toplumu tehlikesi

ortaya konulacaktır. Sonrasında Emniyet Teşkilatı'nda bilgi toplumu sürecinde ortaya çıkan Polnet, Mobese gözetim teknolojileri değerlendirilecektir. Son olarak da bu teknolojilerin ortaya çıkardıkları tehditler çevresinde eleştirisi yapılarak, Emniyet Teşkilatı'nda gözetimin yönetimine yönelik bazı önerilerde bulunulacaktır.

I. TÜRKİYE'DE DENETİMİN VE GÖZETİMİN ARKAPLANI

Türkiye'de gözetim faaliyetlerinin gelişimi, dünyadaki diğer ülkelerde olduğu gibi bilgi ve iletişim teknolojilerindeki gelişim ile doğru orantılı olmuştur. 1993 yılında internetin kullanılmaya başlanması, bilgi toplumu stratejisi kapsamında yapılan Mernis, Takbis, Gimop, Uyap gibi e-devlet çalışmaları, 2008 yılında tüm e-devlet projelerinin tek bir çatı altında birleştirildiği “<http://edevlet.turksat.com.tr>” internet adresinin halka açılması, 2013 yılında uygulanmaya başlanan “Avuç İçi Damar İzi Biometrik Tanımlama Sistemi” gibi biometrik veritabanı oluşturma çalışmaları Türkiye'nin gözetim toplumuna yürüyüşünde attığı adımlar olarak sıralanabilir. Bu bakımdan Türkiye'de gözetim faaliyetleri bilgi toplumu olma çatısında kamu hizmetleri yoluyla yurttaşların verilerinin toplanması, dijitalleştirilmesi, depolanması şeklinde süregelmiştir.

Türkiye uluslararası alanda bilgi ve iletişim teknolojilerinde meydana gelen gelişmelere kendini adapte etmek için hızlı bir dönüşüm sürecine girmiştir. Bu dönüşüm sürecinin çıkış noktasında ve omurgasında da devlet eliyle özellikle kamu kurumlarının hizmetlerinin dijitalleştirilmesi yer almıştır. Bu dijitalleşme süreci oldukça hızlı ve düzensiz bir şekilde gerçekleşmiştir. Dolayısıyla dijitalleşme sürecinde yapılan çalışmalar kontrolsüz, gerçek manada yasal düzenlemeden mahrum, orantısız olarak inşa edilmiştir.

Hızlı dijitalleşme neticesinde bir takım kamu hizmetlerinin sunum şekline kolaylık geldiği aşıkardır. Fakat bu kolaylık için yurttaşların özel hayatlarına özgü kişisel verilerin korunması ve gizliliği adeta yok sayılmıştır. Günümüzde Türkiye'de yaşayan herkesin kişisel verilerinin kurumlar, siyasi partiler, veri hırsızları elinde dolaştığı bir gerçektir.

27 Kasım 2013 tarihinde Cumhurbaşkanlığı Devlet Denetleme Kurulu tarafından kişisel verilerin korunması ve veri güvenliği bakımından kamu kurumlarında yapılan incelemeler neticesindeki tespitleri durumun vahametini gözler önüne sermektedir. Mesela bu rapor sonucunda ortaya çıkan gerçeklerden birisi şöyledir. Türkiye'de her seçim döneminde Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü tarafından seçmen niteliğine sahip olan 18 yaş ve üzerindeki yurttaşların nüfus ve adres bilgileri Yüksek Seçim Kurulu (YSK) ile paylaşılmakta; YSK da bu verilerin hepsini toplu halde dijital ortamda siyasi partilere teslim

etmektedir. Dolayısıyla seçmen niteliğine sahip 50 milyonun üzerindeki yurttaşın adı, soyadı, ana - baba adı, doğum yeri, adres bilgisi onlarca partiyle paylaşılmaktadır. Bu verileri alan siyasi partilerin onları koruyup koruyamadığı, başka şahıs veya tüzel kişilere verip vermediğine yönelik hiçbir denetim mekanizması da bulunmamaktadır.⁵⁷³

Yukarıdaki örnekte görüldüğü üzere ülkemizde tüm yurttaşların şahsına özgü bilgileri elden ele dolaşabilmektedir. Devlet veya kamu kurumları henüz böyle önemli verileri kütük halinde koruyamazken, e-dönüşüm süreci neticesinde oluşturdukları dijital sistemlerin güvenliğini sağladıklarını düşünmek mantıklı olmayacaktır. Zaten aynı denetleme raporunda bu sistemlerde yer alan güvenlik açıklarına yönelik birçok tespit bulunmaktadır. Diğer taraftan yukarıdaki örnek kamu kurumlarının kişisel verilere, kişinin mahremiyetine olan saygısının da seviyesini açıkça ortaya koymaktadır. Böyle bir durumda güvenlik birimlerinin varoluş gayeleri olan güvenliği sağlamak için yapabileceklerinden taviz vererek bireylerin özel alanlarına saygı duymalarını beklemek çok gerçekçi durmamaktadır.

Kişisel verilerin mahremiyetine değer verilmediği, güvenlik endişesinin zirvede olduğu ve bu kapsamda gelişmiş teknolojik cihaz ve yazılımlarla yurttaşların telefonlarının dinlenebildiği, e-posta yazışmalarının takip edilebildiği, irtibatlı olduğu şahısların tespit edilebildiği, kameralarla 7 gün 24 saat izlenebildiği bir toplum için gözetim toplumu kavramından daha hafif bir kavram kullanmanın yetersiz kalacağı düşünülmektedir. Bu kapsamda Türkiye’de gözetim toplumu endekslerinin topyekün varolduğu değerlendirilmektedir.

Türkiye özelinde gözetim faaliyetlerinin ve gözetim teknolojilerinin gelişimi e-devlet projeleri kapsamında kamu hizmetlerinin sunumunun şekil değiştirmesi, giderek artan güvenlik kaygıları nedeniyle güvenliği sağlamak için istihbarat birimlerinin gelişimi, özel sektörde elde edilen karı arttırma odaklı müşteri bilgisine ulaşarak onların profillerini çıkarma girişimleri olmak üzere üç ana kolda ilerlediği ifade edilebilir. Bu bölümde Türkiye’deki bu gelişim seyri ifade edilmiş, gözetim toplumu tehlikesine dikkat çekilmiştir. Türkiye’nin gözetim toplumuna evrilme sürecini anlatmak için öncelikle Türkiye’deki bilgi toplumu oluşturma çalışmaları ve bu kapsamda kamu kurumlarındaki e-devlet çalışmalarından bahsedilecek sonrasında da Türkiye’nin bir gözetim toplumu olduğu düşüncesi savunulacaktır.

⁵⁷³ TC. Cumhurbaşkanlığı Devlet Denetleme Kurulu, *a.g.k*

1. Türkiye’de Bilgi Toplumu Süreci

Bilgi ve iletişim teknolojilerindeki gelişmeler ile bunların kullanımının yaygınlaşması neticesinde yeni bir toplum yapısı olarak bilgi toplumu oluşmaya başlamıştır. Bu toplumsal yapıda diğer toplum türlerindeki üretim biçimlerinden farklı olarak, bilgiye dayalı teknoloji ve bu teknolojinin getirdiği destek ile güçlenen yeni bir anlayış hakim olmuştur. Bu süreçte teknolojik bilgi eğitimden üretime, sanayiden tıp bilimine kadar her alanda kullanılabilen, alınıp satılabilen, tüketimin konusu olabilen bir değere dönüşmüştür. Daha önce de ifade edildiği üzere bu dönüşüm sürecinde kilit kavram “bilgi” ve “bilgi - iletişim teknolojileri” olmuştur. Türkiye de merkez ülkelerde meydana gelen bilgi toplumuna dönüşüm sürecine fazla direnemeyerek dahil olmuştur. Bu bölümde Türkiye’nin bilgi toplumuna evrilişi tarihsel zemin üzerinde anlatılmaya çalışılacaktır.

Yirmi birinci yüzyılda başta batı ülkeleri olmak üzere birçok ülke sanayi toplumundan bilgi toplumuna geçişi bir gaye olarak benimsemiş ve bu kapsamda çeşitli eylem planları hazırlamıştır. Örneğin Avrupa Birliği üyesi ülkeler kapsamında bilgi toplumuna geçiş ile ilgili e-Avrupa eylem planları hazırlanarak yürürlüğe konulmuştur. Bu kapsamda internet kullanımı ve internete erişiminin yaygınlaştırılması, ticari işlemlerin e-ticaret başlığı altında internet ortamına kaydırılması, e-iş, e-sağlık, e-devlet gibi birçok yeni alanların açılarak bunların geliştirilmesi ve bu alanlara katılımın sağlanması, bilgi toplumu müktesebatı oluşturulması gibi adımlar atılmıştır.⁵⁷⁴ Bu kapsamda günümüzdeki anlamda bilgi toplumuna dönüşümün en önemli başlangıç adımı olarak kamu hizmetlerinin elektronik ortamda verilmeye başlanması gösterilebilir. Aynı durum Türkiye için de söz konusu olmuş ve bilgi toplumuna evrilme e-devlet projeleri güdümlü süregelmiştir. Türkiye’de elektronik devlet uygulamalarına yönelik çalışmalar kurumsal anlamda ilk olarak 1990’lı yıllarda başlamış ve bu kapsamda başlangıç olarak kurumsal bilgi havuzlarının oluşturulması, bilgi işlem merkezlerinin kurulması, kamu kurumlarının kurumsal internet adresi alması gibi çeşitli adımlar atılmıştır. Türkiye’nin internetle ilk teması 12 Nisan 1993 tarihinde ODTÜ’den Ankara - Washington arasında kurulan kiralık hat sayesinde olmuştur.⁵⁷⁵

Türkiye’de yönetim ve kamu hizmeti alanlarında bilgi ve iletişim teknolojilerini kullanmasını ifade eden bilgi toplumu süreci, gerçekleştirilen çoğu değişim ve dönüşümde

⁵⁷⁴ Avrupa Birliği, *2003 E-Avrupa Eylem Planı*, Haziran 2001, s.3.

http://www.bilgitoplamu.gov.tr/Documents/3/Diger/010600_eAvrupa+EylemPlani.pdf, (Erişim Tarihi: 15.09.2012).

⁵⁷⁵ TC Sayıştay Başkanlığı, *Performans Denetimi Raporu: E-Dönüşüm Türkiye Projesi Çerçevesinde Yürütülen Faaliyetler*, 2006, s.24.,<http://www.sayistay.gov.tr/rapor/perdenrap/2006/2006-3eDTR/2006-eDTR.pdf>, (Erişim Tarihi: 02.09.2013).

olduğu gibi yine dış dayatmalı - destekli başlamış, halkın kendi istekleri doğrultusunda ülkenin kendi iç dinamiklerinden yükselen bir sesle olmamıştır. Nitekim Dünya Bankası'nın 1993 yılında yayımladığı *Türkiye, Bilişim ve Ekonomik Modernizasyon Raporu* ile Türkiye'de bilgi toplumu sürecinin başladığı söylenebilir.⁵⁷⁶

Dünya Bankası'nın bu çalışmasından sonra 1998 yılında başlayıp Ekim 1999'da sonuç raporu yayımlanan, Ulaştırma Bakanlığı koordinasyonunda, TÜBİTAK tarafından Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA) hazırlanmıştır. Bu oldukça kapsamlı olan ve ülkedeki önemli bilim adamları, gazeteciler, teknik uzmanlar, kamu görevlilerinden oluşan bir ar-ge grubu tarafından 2010 yılına kadar Türkiye'nin bilgi ve iletişim teknolojilerine adaptasyonu ve bilgi toplumuna dönüşümünün temellerinin atıldığı önemli bir rapordur. Günümüzde Milli Eğitim Bakanlığı e-devlet uygulaması olan MEBBİS'in ve e-sağlık uygulamalarının altyapısının 14 yıl önce bu çalışmada hazırlanmış olduğu bilinmektedir.⁵⁷⁷

Kamu hizmetlerinde gittikçe yaygınlaşan bilgisayar ağ projelerinin ayrı ayrı planlanması veya aynı bakanlıkta birden fazla bilgisayar ağı kurulması yerine, kamuya yönelik ağları bir ulusal kamu bilgisayar ağında birleştirilmesi amacıyla 1998/13 sayılı Başbakanlık Genelgesi ile "TC Başbakanlık Kamu-Net Üst Kurulu" oluşturulmuştur.⁵⁷⁸ E-Dönüşüm Türkiye Projesi kapsamında belirlenen amaçları gerçekleştirmek üzere 2003 yılının Mart ayında DPT Müsteşarlığı bünyesinde doğrudan bir müsteşar yardımcısına bağlı olarak "Bilgi Toplumu Dairesi Başkanlığı" kurulmuştur.⁵⁷⁹ 641 Sayılı Kanun Hükmünde Kararnameye göre Bilgi Toplumu Dairesi Başkanlığı'nın görevleri; bilgi toplumuna ilişkin politika, hedef ve stratejileri hazırlamak, bu alanda kamu kurum ve kuruluşları, sivil toplum örgütleri ve özel sektör arasındaki koordinasyonu - iletişimi temin etmek ve uygulamayı etkin bir biçimde yönlendirmek olarak belirlenmiştir.⁵⁸⁰

Türkiye'nin bilgi toplumuna dönüşümü için 2006 - 2010 yıllarını kapsayan *Bilgi Toplumu Stratejisi* oluşturulmuştur. Bu Türkiye'nin ilk bilgi toplumu stratejisi olmasından dolayı önem arz etmektedir. Stratejinin vizyonu şu şekilde ifade edilmiştir:⁵⁸¹

⁵⁷⁶ Dilek Y. Civelek, *a.g.k.*, s.12.

⁵⁷⁷ Tubitak, *Tuena Sonuç Raporu*, Ekim 1999, s.13 - 14.

⁵⁷⁸ Engin Hepaksaz, Betül Hayrullahoğlu, "E-Devlet Kapsamında Vedop Uygulamaları ve E-Haciz", *Sosyal ve Beşeri Bilimler Dergisi*, Cilt 3, No 2, 2011, s.112.

⁵⁷⁹ *a.k*

⁵⁸⁰ www.tbmm.gov.tr/arastirma.../bilisim.../kalkinma_bakanligi.pptx (Erişim Tarihi: 02.09.2013).

⁵⁸¹ Yüksek Planlama Kurulu, *Bilgi Toplumu Stratejisi 2006-2010*, 28 Temmuz 2006., www.bilgitoplumu.gov.tr, (Erişim Tarihi: 02.09.2013).

"Bilim ve teknoloji üretiminde odak noktası haline gelmiş, bilgi ve teknolojiyi etkin bir araç olarak kullanan, bilgiye dayalı karar alma süreçleriyle daha fazla değer üreten, küresel rekabette başarılı ve refah düzeyi yüksek bir ülke olmak."

Bu strateji belgesinde aynı zamanda yedi temel stratejik öncelik belirlenmiştir. Birincisi herkes için bilgi ve iletişim teknolojileri fırsatının temin edilmesi odaklı sosyal dönüşümün sağlanması, ikincisi bilgi ve iletişim teknolojilerinin iş dünyasına nüfuzunun sağlanarak işletmeler arasında bu alanda rekabetin oluşturulması, üçüncüsü yüksek standartlarda kamu hizmeti sunumunun gerçekleştirilmesi, dördüncüsü bilgi ve iletişim teknolojileriyle desteklenen bir kamu yönetimi modernizasyonu ve reformunun başlatılması, beşincisi ülkede küresel rekabetçi bilgi teknolojileri sektörünün oluşturulması, altıncısı toplumun her kesimine yüksek kalitede ve ucuz iletişimin sunulması amaçlı iletişim altyapı ve hizmetlerinin yenilenmesi ve büyütülmesi, yedincisi küresel pazarın taleplerine uygun olacak şekilde araştırma geliştirme faaliyetlerinin organize edilmesidir.⁵⁸²

Bilgi Toplumu Stratejisinin çıkış noktasında bilgiye dayalı iktisadi hayatın, sürdürülebilir ekonomik kalkınma ve rekabetçilik bakımından gittikçe önem kazanması yer almaktadır. Bu bakımdan yukarıdaki hedefler de göz önünde bulundurulduğunda bu strateji ve anlayış küresel, rekabetçi ve iş dünyası orijinli olarak gözükmektedir. Diğer taraftan Dünya Bankası'nın 1993 yılında yayımladığı rapordan sonra bilgi ve iletişim teknolojilerine yönelimin olması ve *Tuena Sonuç Raporunda* belirtilen genişleme hedeflerinden olan *GATT* (*İng; General Agreement on Tariffs and Trade*) anlaşmaları ve Dünya Ticaret Örgütü temelli yaklaşım, Türkiye'de bilgi toplumu dönüşümünün ve e-devlet sürecinin küresel sermayenin yeni pazarlar arayışı içinde olması dürtülü başladığını ve geliştiğini göstermektedir.

"GATT anlaşmaları ve bu anlaşmalardan kaynaklanan WTO (Dünya Ticaret Örgütü) tarafından uygulanmakta olan yeni ticaret rejimi geleneksel malların ötesinde her türlü hizmetler ve iletişim hizmetlerinin de derece derece serbestleşmesini içermektedir. Bu yöndeki gelişmeler de enformasyon altyapılarına yönelik olarak genişlemeyi gerektiren diğer faktörler arasındadır."⁵⁸³

Türkiye'de e-devlet kapısı "<http://devlet.turksat.com.tr>" internet adresi olarak 18 Aralık 2008 tarihinde yapılan resmi bir törenle, Başbakan tarafından açılmıştır. Amaç olarak da kamu hizmetlerinin tek bir internet sitesi üzerinden muhatapları yurttaşlara ve kamu görevlilerine sunmak olmuştur. Böylece devlet organları tarafından sunulan birçok hizmete internetin olduğu her yerden muhataplarının hızlı ve kolay bir şekilde ulaşması hedeflenmiştir. 2008 yılında e-devlet kapısı 28 proje ile açılmıştır. 2010 yılı sonunda bu sayı 246'ya ulaşmıştır.⁵⁸⁴ 2010 yılında yapılan *AB Dokuzuncu E-Devlet Ölçme ve Kıyaslama*

⁵⁸² a.k

⁵⁸³ Tubitak, a.g.k, s.24.

⁵⁸⁴ Devlet Planlama Teşkilatı, *Bilgi Toplumu İstatistikleri 2011*, s.76.

Çalışmasına göre Türkiye’de temel kamu hizmetlerinin elektronik ortama taşınması oranı %89’luk bir seviyedeysen, 27 Avrupa Birliği üyesi ülkesinin ortalama oranı %82 seviyesinde kalmıştır.⁵⁸⁵ DPT Bilgi Toplumu Dairesi Başkanlığı’nca Haziran 2011’de yapılan istatistik çalışması neticesinde Türkiye, hizmetlerin elektronik ortamda sunumu sıralamasında, ölçümü yapılan 32 ülke arasında 17. sırada yer almıştır.⁵⁸⁶

Bilgi toplumu süreci sadece kamu hizmetlerinin dijital sunumu ile sınırlandırılmaz. Zira toplumsal anlamda topyekün bir dönüşümü ifade etmektedir. Bu bakımdan toplumdaki diğer bilgi ve iletişim teknolojilerinin kullanımına yönelik göstergeler de önem arz etmektedir. Bu bakış açısında Türkiye’de gelişen internet teknolojileri sayesinde yurttaşlar internet tabanlı uygulamaları yoğun bir şekilde kullanmaktadırlar. Akıllı telefon kullanıcı sayısı her geçen gün daha da artmaktadır. Evde, işyerinde, alışveriş merkezinde, otobüste hemen hemen her yerde internet bağlantısı bulunmaktadır. İnternet kullanıcı sayısı nüfusun yarısı kadar bir miktarda 36.455.000 civarındadır.⁵⁸⁷ *Twitter, Facebook, Instagram, Linkedn* gibi sosyal medya uygulamaları çok sayıda yurttaş tarafından kullanılmaktadır. Örneğin ülkemizde *Twitter* kullanıcı sayısı 11.337.505 civarındadır.⁵⁸⁸ Dolayısıyla her üç internet kullanıcılarından birisi *Twitter* kullanmaktadır. Diğer taraftan *Whatsapp, Line, Skype, Google Talk* gibi internet bağlantılı olan ücretsiz ve görüntülü görüşme programlarının kullanım oranı her geçen gün artış göstermektedir. Bütün bu göstergeler Türkiye’nin bilgi toplumu sürecinde geri dönülmez bir hızla ilerlediğini göstermektedir. Nüfusunun büyük kısmı genç olması nedeniyle de bilgi ve iletişim teknolojilerinin kullanımının adaptasyonunda ciddi bir sorun ile karşılaşmadığını ifade edebiliriz.

Günümüzde Türkiye’de verilen birçok kamu hizmetinin e-devletleşmesi⁵⁸⁹ yukarıda ifade edilen bilgi ve iletişim araçlarının toplum tarafından hızla benimsenebilmesi bilgi toplumu sürecinin göstergeleri olarak gözükse de aynı zamanda daha önceki bölümlerde ifade

⁵⁸⁵ a.k, s.92.

⁵⁸⁶ a.k, s.193.

⁵⁸⁷ 2013 Yılı’nın Ekim Ayında E-Marketer İsimli Araştırma Şirketi Tarafından Hazırlanan Rapor, www.emarketer.com, (Erişim Tarihi: 12.01.2013).

⁵⁸⁸ a.k

⁵⁸⁹ Türkiye İş Kurumu’nun internet sayfasından kamu ve özel sektör iş ve işçi arama ve başvuru işlemleri yapılabilmektedir. Bu internet sayfasından işsizlik ödeneği için çevrimiçi başvuru da yapılabilmektedir. Sağlık sigortasına ilişkin işlemler Sosyal Güvenlik Kurumunun uygulamaları üzerinden çevrimiçi gerçekleştirilebilmektedir. Sigorta primleriyle ilgili bildirimler internet üzerinden gönderilebilmekte; borç, tahakkuk ve tahsilat bilgilerine ulaşılabilen ve çevrimiçi ödeme yapılabilmektedir. Yüksek Öğrenim Kredi ve Yurtlar Kurumu internet sayfasından öğrenci burs, kredi ve yurt başvuruları çevrimiçi yapılabilmekte; sonuçlar ve borç durumlarına ilişkin bilgilere ulaşılabilir. Elektronik imza kullanılarak Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü internet sayfası üzerinden adres değişikliği işlemi gerçekleştirilebilmektedir. İnternet üzerinden Merkezi Hastane ve Randevu Sisteminden hastane randevu işlemleri yapılabilmektedir. Yeni şirket tescili, değişiklikleri ve ticaret sicili işlemleri elektronik ortamda gerçekleştirilebilmektedir. Gümrük bildirimleriyle ilgili beyannameler elektronik ortamda verilebilmektedir.

edildiği gibi gözetim toplumunun da emaresi hükmündedir. Zira bu iki süreç birbirine eklenmiştir. Ülkemizde bilgi toplumu araçlarının yüksek oranda kullanılması iktidar güçlerini hoşnut etmektedir. Zira Lyon'un “bireylerden özellikle soyutlanmış hakikat parçacıklarını arayıp bulma faaliyeti”⁵⁹⁰ olarak ifade ettiği bireye ait veriye ulaşma bilgi toplumu araçlarıyla mümkün hale gelmiştir. Dolayısıyla bilgi ve iletişim teknolojilerine sahip olan, takip eden ve yönetenler bilgiye hakim olanlar olmaktadır. Bu sahip oldukları bilgi genişliği de bir anlamda üstünlük aracına dönüşmektedir.⁵⁹¹ Sadece üstünlük aracı değil aynı zamanda birey ve örgütler üzerinde birer kontrol aracı da olmaktadır.⁵⁹² İktidarın varlığını devam ettirebilme gücü başkasına ait olanı bilme gücü ile paralellik arz etmektedir. İşte iktidar, başkasına ait olanı bilme gücünü de korumak ve arttırmak için gözetim teknolojilerine başvurmaktadır. Dolayısıyla ülkemiz için de günümüzde bilgi ve iletişim teknolojilerinin gelişimiyle paralellik gösteren gözetim teknolojilerinin iktidarın varlığının garantörü bilgi toplama araçları olduğu söylenebilir.⁵⁹³

2. Türkiye’de E-Devlet Uygulamaları

Kamu hizmetlerinin daha kolay ve basit bir şekilde yerine getirilmesi saikiyle bilgi ve iletişim teknolojileri çatısında şekillenen e-devletin, sosyal ve kurumsal özellikleri olan çok boyutlu bir dönüşüm sürecini ifade ettiği söylenebilir.⁵⁹⁴ Bu süreç genel anlamda bilgi toplumu olarak ifade edilen toplumsal boyuta evrilmenin göstergesi niteliğindedir. Türkiye de merkez ülkelerde başlayan bu evrilme sürecine dahil olmuş ve bilgi - iletişim teknolojilerindeki gelişmeler paralelinde e-devlet projelerine ağırlık vermiştir. Dolayısıyla Türkiye’de e-devlet uygulamalarının bilgi toplumuna geçiş amaçlı olarak başlatıldığı ifade edilebilir. Sürecin e-devlet odaklı olarak yürütülmesinin, bilgi ve iletişim teknolojileriyle paralellik arz eden gözetim faaliyetlerinin de e-devlet odaklı gelişim göstermesine yol açtığı söylenebilir. Bu bakımdan çalışmada Türkiye’deki e-devlet projeleri gözetim faaliyetlerinin bir aracı olarak görülmüştür.

Türkiye’de e-dönüşüm olarak ifade edilebilecek olan e-devletleşme politikaları eğitim, sağlık, işgücü piyasası, yurttaşlık, adalet ve güvenlik olmak üzere altı ana başlıkta incelenebilir. Gerçekleştirilen e-devlet çalışmalarının altyapısal olarak temelini yurttaşlık alanında yapılan dijital faaliyetler oluşturmuştur. Bu faaliyetler genel olarak yurttaşlara ait

⁵⁹⁰ David Lyon, *a.g.k*, 2006, s.13.

⁵⁹¹ Daniel Bell, *a.g.k*, 1973, s.xiii.

⁵⁹² Haluk Geray, *a.g.k*, 1998, s.1416.

⁵⁹³ Michel Foucault, *a.g.k*, 2003, s.35.

⁵⁹⁴ Nurcan Törenli, *a.g.k*, s.192 - 193.

olan kimlik, adres, soy gibi temel verilerin toplanması, tektipleştirilmesi, kategorize edilmesi ve tek bir veritabanında toplanmasını ifade etmektedir. Nitekim buna yönelik olarak Merkezi Nüfus İdaresi Sistemi (Mernis)⁵⁹⁵ adında bir proje geliştirilmiştir. Bu proje ilk defa 1974 yılında gündeme gelmiş ve 1976 yılında ihaleye açılmıştır. İhaleyi kazanan Ortadoğu Teknik Üniversitesi ile anlaşma yapılmış ve çalışmalara başlanmıştır.⁵⁹⁶

Mernis çok uzun yıllar sürmüş olan ve bundan dolayı maliyetinin bile rasyonel olarak ortaya konulamadığı bir projedir. Zira 1976 yılında ihale sürecinin bitmesinden sonra 1996 yılına kadar ancak 600 ilçenin nüfus bilgileri dijital ortama aktarılabilmektedir. Bugünkü anlamda Mernis 2000’li yıllardan sonra ortaya çıkmaya başlamıştır. Bu kapsamda ilk aşamada Mart 2001 sonunda herkese bir kimlik numarası verilmesi ve nüfus müdürlüklerinin çevrimiçi olarak birbirlerine bağlanması sağlanmıştır. Sonraki süreçte Kimlik Paylaşım Sistemiyle yurttaş bilgileri belli kurallar ve kriterler çerçevesinde diğer kamu kurum - kuruluşlarının ve yurttaşların hizmetine açılmıştır. 2003 - 2007 yılları arasında da projenin altyapısal olarak bilgi ve iletişim teknolojilerine uyumlu olması sağlanmış, mevzuat anlamında gerekli adımlar atılmış ve TC kimlik nolu nüfus cüzdanları yurttaşlara dağıtılmıştır.⁵⁹⁷

Mernis ile sağ ve ölü 130 milyon Türkiye Cumhuriyeti yurttaşına veri tabanlarında kullanmak üzere birer TC kimlik numarası verilmiş, bütün nüfus kayıtları elektronik ortama geçirilerek bir “Nüfus Bilgi Bankası” oluşturulmuştur. Günümüzde yurttaşlar, elektronik ortamdaki yegane kimlikleri olan bu numaralar sayesinde işlemlerini yapabilmektedirler. Ayrıca her yurttaşla birer numara verilmesi neticesinde kamu hizmetlerinde kullanılan diğer veritabanları ile Mernis veritabanı ilişkilendirilerek veri yeknesaklığı sağlanmıştır. Bu anlamda diğer kamu hizmetlerinde kullanılan veritabanları ile Mernis arasında bir eşgüdüm sağlanmış ve diğer veri tabanlarının da veri altyapısı oluşturulmuştur.⁵⁹⁸ Bu bakımdan Mernis diğer tüm e-devlet projelerinin gelişimi için önemli bir adım olarak değerlendirilebilir. Kamu kurumları arasında temin edilen bu eşgüdüm sayesinde kamu kurumlarının veri sistemlerindeki bilgi dağınıklığı ve karmaşasının önlendiği iddia edilmektedir. Bu bağlamda Mernisin elektronik alanda hizmet sunan devlet yapısının, yani e-Türkiye’nin merkezi bir unsuru haline geldiği ifade edilebilir.

⁵⁹⁵ Mernis projesinin resmi internet sitesi: www.nvi.gov.tr

⁵⁹⁶ Kemal Atmaca, “E-Devletten Olgun Devlete ya da E-Devlet’in Olgunlaştırılması”, s.8., www.mfa.gov.tr, (Erişim Tarihi: 25.08.2013).

⁵⁹⁷ *a.k*

⁵⁹⁸ Serhat Baştan, *a.g.k*, s.83 - 84.

Mernisin oluřum srecinde amaları nfus mevzuatına uygun olarak merkez ve ile birimlerinde nfus iřlemelerinin bilgisayar ortamında yapılması ve merkezi veritabanının oluřturulması, oluřturulan veritabanındaki bilgilerin Kimlik Paylařım Sistemi erevesinde kamu kurum ve kuruluřları iin paylařıma aılması, Trkiye Cumhuriyeti kimlik numarasının verilmesi, kolay tařınabilir - taklit edilemez modern nfus kimlik kartlarının verilmesi, nfus ve aile istatistiklerinin hızlı ve saėlıklı alınması, kamu kuruluřlarına ve yurttařa elektronik ortamda bilgi hizmetinin verilmesi olarak belirlenmiřtir.⁵⁹⁹ Gncel olarak bakıldıėında sistemin bu amalarına byk oranda ulařtıėı grlmektedir.

Tm yurttաřların kimlik verilerinin dijitalleřtirilmesiyle oluřan Mernisin gnmz dnyasında zellikle kamu hizmetlerinin sunumunda saėladıėı imkan ve kolaylıklar yadsınamaz. Bu imkan ve kolaylıklar mali, gvenlik, askerlik, saėlık, sosyal gvenlik, eėitim, adalet, nfus yurttաřlık iřleri konularında incelenebilir. Mali aıdan vergi tahsilatı ve denetimi kolaylařmıř, kayıt dıřı ekonominin kontrol altına alınmasına ynelik nemli bir altyapı oluřturulmuřtur. Ayrıca noter, tapu, posta ve banka iřlemlerinde grevli personel bu sisteme girebildiėinden dolayı sahte evrak ile iřlem byk oranda engellenmiřtir. Gvenlik ynnden, kolluk kuvvetleri Mernis zerinden aradıėı kiřilerin gerek kimliklerine ulařmak suretiyle hızlı hareket kabiliyetine sahip olmuř, kendi sahip oldukları veritabanlarında sululara iliřkin veriler Mernis veritabanı ile iliřkilendirilebildiėinden dolayı sulu řaхіslara ynelik stratejik ve operasyonel analiz alıřmaları yapabilecek kapasiteye ulařmıřlardır.⁶⁰⁰

Askerlik ynnden, askerlik aėına gelen kiřilerin listeleri doėru ve hızlı bir řekilde Mernis veritabanından alınarak askere alma ve asker kaaklarının takibi kolaylařmıřtır. Ayrıca, yař gruplarına gre erkek nfus bilgileri de bu veritabanından elde edilerek, orta ve uzun vadede asker ihtiyaının planlanması kolaylařmıřtır. Saėlık ynnden her yurttաř iin saėlık kuruluřlarında aılan dosyalar, TC kimlik numarası esasına gre oluřturulduėundan dolayı kiřinin birden fazla saėlık dosyasının olmasının nne geilmiř ve saėlık bilgilerinin birleřtirilmesi kolaylařmıřtır. Sosyal gvenlik ynnden, yurttաř Emekli Sandıėı, SSK veya Baė-Kur’lu olduėunda, tek numara tařıdıėından dolayı bunların takibi kolaylařmıřtır. Sosyal Gvenlik Kurumu alıřanları bu veritabanına baėlanarak, elektronik ortamda kiřiye iliřkin bilgileri hızlı ve saėlıklı bir řekilde alabilir hale gelmiř ve bylece kiřilere iliřkin bilgi eksikliėinden dolayı yurttաřın maėduriyetinin nne geilmiřtir.⁶⁰¹

⁵⁹⁹ DPT Bilgi Toplumu Dairesi Bařkanlıėı, *E-Devlet Proje ve Uygulamaları*, Nisan 2004, s.52 - 53.

⁶⁰⁰ Ali Arifoėlu, *E-Dnřm: Yol Haritası*, Sas Biliřim Yayınları, Ankara, 2004, s.20.

⁶⁰¹ a.k

Eğitim yönünden, eğitim çağına gelen öğrenciler ile ilgili olarak her türlü istatistiki bilgiler alınabilmekte, planlamalar ve politikalar daha sağlıklı bir biçimde belirlenebilmektedir. Adalet yönünden, davaların mahkemelerde görülmesi sırasında yapılan kimlik tespitleri Mernis veritabanından alınabilmekte, böylece davaların hızlı bir şekilde görülmesinin önündeki yapısal engeller ortadan kaldırılabilir. Nüfus yurttaşlık işleri yönünden en sık yapılan işlemlerden birisi olan ve ortalama 20 gün süren “doğum ve nüfus cüzdanı verme” işlemi çevrimiçi sisteme geçilmesi ile birlikte 8 dakika gibi kısa bir süreye kadar düşürülmüştür.⁶⁰²

E-devlet çalışmalarında en önemli projelerden birisi olarak değerlendirilebilecek olan Mernisin sağladığı kolaylıklar onu hatasız ve zararsız kılmamaktadır. Bu hataların ve zararların başında kişisel verilerin güvenliğinin sağlanamaması gelmektedir. Nitekim projenin kişisel bilgilerin korunması konusunda yetersiz olduğu da ispatlanmıştır. İstanbul Emniyet Müdürlüğü tarafından 26 Temmuz 2010 tarihinde yedi ilde yapılan operasyonda tüm Türkiye yurttaşlarının kimlik bilgilerinin bir örgüt tarafından çalındığı ve 70 milyon kişinin kimlik, adres ve telefon bilgilerinin yakalanan şahısların elinde olduğu anlaşılmıştır. Örgüt üyelerinin belli bir ücret karşılığında bu verileri sattığı tespit edilmiştir.⁶⁰³

Yurttaşların nüfus bilgilerine diğer kurum personelinin ulaşabilir olması, kamu görevlilerinin tüm yurttaşların adres, nüfus, ulaşım bilgilerine rahatlıkla ulaşabileceği anlamına gelmektedir ki bu durum yolsuzluk oranının yüksek olduğu ülkemizde kamu görevlilerinin yurttaşlara ait bilgileri üçüncü şahıslara satması yüksek ihtimalini de barındırmaktadır. Kimlik Paylaşım Sisteminin uygulamaya girdiği 2005 yılından Mayıs 2011’e kadar kamu görevlileri tarafından toplamda 14,2 milyar adet kimlik ve adres sorgulaması/paylaşımı yapılmıştır.⁶⁰⁴ Bu tespit de herkese dair bilgiye ne kadar çok kamu görevlisinin ulaşabildiğinin açık bir göstergesidir.

Mernisin sağladığı iddia edilen imkanlara rağmen halen eski bürokrasi ve kırtasiyecilik faaliyetlerine devam edilmesi ortaya çıktığı iddia edilen faydaları hükümsüz kılmaktadır. Örneğin her ne kadar Mernis ile birlikte diğer kamu kurumlarında yer alan personelin Kimlik Paylaşım Sistemine ulaşarak yurttaşların işlerini hızlandıracağı ifade edilse

⁶⁰² a.k

⁶⁰³ 27.07.2010 Tarihli “Tüm Kimlik Bilgilerimiz Ellerin” Başlıklı Haber, http://www.aktifhaber.com/news_detail.php?id=309190, (Erişim Tarihi: 25.01.2013).

⁶⁰⁴ Devlet Planlama Teşkilatı, a.g.k, 2011, s.79.

de güncel olarak kamu kurumlarınca yapılan işlemlerde nüfus cüzdanı örneği, ikametgah ilmühaberi, adli sicil kaydı gibi belgelerin isteniyor olmaya devam edilmesi gösterilebilir.⁶⁰⁵

Türkiye’de e-devlet sürecinin ikinci ayağını eğitim alanında yapılan faaliyetler oluşturmaktadır. Milli Eğitim Bakanlığı 2011 - 2012 eğitim öğretim yılı istatistiklerine göre Türkiye’de 60 bin 165 okulda toplam 25 milyon 429 bin 670 öğrenci eğitim görmekte, 880 bin 317 öğretmen de eğitim hizmeti vermektedir.⁶⁰⁶ Belirtilen sayı göz önüne alındığında Türkiye nüfusunun yarısına yakın oranda bir nüfusun eğitim alanında faaliyet gösterdiği anlaşılmaktadır. Bilgi ve iletişim teknolojilerindeki gelişmelerin nüfusun özellikle genç kesimini oluşturan bu eğitim alanında faaliyet gösterenleri etkilememesi düşünülemez. Bu paralelde ortaya çıkan e-devlet çalışmalarından ilk payını alanlardan birisi de eğitim alanı olmuştur.

Eğitim alanında eğitim - öğretim hizmetlerinin bilgi ve iletişim teknolojilerine entegre edilmesine kurumsal faaliyetlerin dijitalleştirilmesine yönelik çeşitli çalışmalar gerçekleştirilmiştir. Bu kapsamda bünyesinde Milli Eğitimi Bakanlığı ile ilgili farklı e-devlet projeleri yer alan Milli Eğitim Bakanlığı Bütünleşik Yönetim Bilgi Sistemi (MEBBİS) oluşturulmuştur.⁶⁰⁷ MEBBİS bünyesinde öğrencilere, çalışanlara, velilere, halka açık farklı birçok projeler ve modüller bulunmaktadır. İlk adımları 1987 yılında Personel Bilgi Sistemi Projesi ile başlasa da günümüzde geldiği noktada eğitime dair birçok faaliyetin yapıldığı büyük bir sisteme dönüşmüştür.⁶⁰⁸ Eğitim alanında e-devlet faaliyetleri sadece MEB bünyesinde değil diğer eğitim kurumlarında da gerçekleşmiştir. Örneğin günümüzde üniversiteler internet sitelerinde uzaktan yüksek lisans eğitimi gibi farklı hizmetleri sunacak seviyeye ulaşmıştır.

Sağlık alanında yapılan e-devlet çalışmaları 1990’lı yılların başlarına kadar götürülebilir. Nitekim ilk olarak 1992 - 1993 yıllarında Sağlık Enformasyon Sistemleri Planlama Çalışmaları yürütülmeye başlanmıştır. Bu çalışmaların bir sonucu olarak günümüzde kullanılan Sağlık Bakanlığı Sağlık Enformasyon Sistemleri (SES) ortaya çıkmıştır. Bu sistem günümüz e-sağlık hizmetlerinin altyapısını oluşturmaktadır. Sistemin içerisinde Temel Sağlık İstatistikleri Modülü, Çekirdek Kaynak Yönetimi Sistemi, Hastane

⁶⁰⁵ Hakan Yıldırım, *a.g.k*, s.146.

⁶⁰⁶ <http://www.egitimedair.net> (Erişim Tarihi: 25.01.2013).

⁶⁰⁷ TC. Cumhurbaşkanlığı Devlet Denetleme Kurulu, *a.g.k*

⁶⁰⁸ <http://www.meb.gov.tr>, (Erişim Tarihi: 25.01.2013).

Bilgi Sistemleri, Birinci Basamak Sağlık Hizmetleri Bilgi Sistemi modülleri yer almaktadır.⁶⁰⁹ Ayrıca sağlık alanında oluşturulmuş olan sisteme entegre birçok yeni proje de bulunmaktadır.⁶¹⁰ E-devlet politikaları çerçevesinde sağlık alanında gerçekleştirilen projeler kendi öz kaynaklarımızla değil, Dünya Bankası güdümlü ve teşvikli başlamış ve projelendirilmiştir. Nitekim 22 Aralık 1994 ve 7 Ekim 1997 tarihlerinde bu konuyla ilgili Dünya Bankası - Türkiye arasında anlaşmalar yapılmıştır.⁶¹¹

Adalet alanındaki e-devlet faaliyetlerini Ulusal Yargı Ağı Projesi (Uyap) ifade etmektedir. Bu proje diğer e-devlet projelerine göre daha genç durmaktadır. Zira hazırlık çalışmaları 2000 yılında başlamış ve günümüzdeki haline 2005 yılı sonrasında ulaşmıştır. Adalet Bakanlığı merkez ve taşra teşkilatının, bağlı ve ilgili kuruluşlarının, adli ve idari tüm yargı birimlerinin (Cumhuriyet Başsavcılıkları, mahkemeler, icra ve iflas daireleri, ceza infaz ve ıslah kurumları, adli tıp birimleri, denetimli serbestlik birimleri) adli ve idari bütün işlemlerinin evrak sirkülasyonu olmadan dijital ortamda gerçekleştiği bir projedir.⁶¹² Uyapın kendi resmi internet sitesindeki bilgilere göre bugün itibariyle bu projenin ülkemizdeki yargı birimlerinin %100'ünde işletimde olduğu, her türlü yargısal ve idari faaliyetlerin bu sistemle elektronik ortamda yürütüldüğü anlaşılmaktadır. Proje; Yurttaş Bilgi Sistemi, Avukat Bilgi Sistemi, Mevzuat Programı, Kurum Bilgi Sistemi, SMS Bilgi Sistemi, Sesli ve Görüntülü Kayıt ve Video Konferans Sistemi, Karar Destek Sistemlerinden oluşmaktadır.⁶¹³

Uyap sayesinde yargı organları ve görevliler kişilere yönelik bütün işlem geçmişini görebilmekte ve tekrar tekrar aynı verileri oluşturmak zorunda kalmamaktadırlar. Örneğin, sanığın kimlik ve adres bilgilerinin savcılık aşamasında sisteme girilmesi yeterli olup, artık mahkeme aşamasında, Yargıtay'da temyiz aşamasında, kararın infazı aşamasında, dosyanın Türkiye'de başka yer yargı mercilerine gönderilmesi halinde bu merciler tarafından yeniden söz konusu bilgilerin sisteme girilmesine gerek kalmamaktadır.⁶¹⁴ Bu bağlamda yargı sürecinin konusu olan bir şahıs ile ilgili olarak Mernis Projesinden otomatik olarak şahsın

⁶⁰⁹ Haluk Özşarı, "Türkiye'de Sağlık Reformu Süreci ve Sağlık Enformasyon Sistemleri İle İlişkisi", www.sbu.saglik.gov.tr, (Erişim Tarihi: 25.01.2013).

⁶¹⁰ Çekirdek Kaynak Yönetimi Sistemi (ÇKYS - TSİM), Elektronik Belge Yönetim Sistemi, Elektronik Tüberküloz Yönetim Sistemi(e-TYS), Doktor Bilgi Bankası, Döner Sermaye Bütçe Uygulaması, Hasta Hakları , Hastane Enfeksiyonları, İşçi Sayısı Tespit Sistemi, Karar Destek Sistemleri (İş-Zekası), Karar Destek Sistemleri (Sağlık.NET 2) , Özürlüler Veri Bankası, Personel Bilgi Sistemi (PBS), Programları İzleme Değerlendirme Sistemi, Tek Düzen Muhasebe Sistemi (TDMS), Türkiye Diyaliz Bilgi Yönetim Sistemi, Türkiye Yoğun Bakım İzleme Sistemi, Türkiye Organ ve Doku Bağıışı Bilgi Sistemi, Ulusal Organ Bilgi Sistemi, Yeni Doğan İşitme Taraması, Yeşil Kart Bilgi Sistemi, Sosyal Tesis Muhasebe Takip Sistemi. www.sbu.saglik.gov.tr, (Erişim Tarihi: 05.02.2013).

⁶¹¹ Haluk Özşarı, *a.g.k*

⁶¹² www.uyap.gov.tr, (Erişim Tarihi: 26.01.2013).

⁶¹³ *a.k*

⁶¹⁴ *a.k*

kimlik ve adres bilgileri alınabilmekte, Uyap veritabanına varsa şahısla ilgili önceden girilmiş kovuşturma ve soruşturma sürecine ilişkin bütün bilgiler tek ekranda kullanıcının karşısına gelebilmektedir. Bunların yanı sıra itiraz edilen dosyaların üst dereceli mahkemeye, temyiz edilenlerin ise Yargıtay'a sevk edilmesi elektronik ortamda hızlı ve kolay bir şekilde olmaktadır. Yakalama ve gözaltı süreleri de Uyap üzerinden canlı olarak takip edilebilmektedir.⁶¹⁵

Uyapın barındırdığı en büyük tehlike yürütülen soruşturmanın gizliliğinin ihlal edilmesine ve gizli tanıkların deşifre edilmesine imkan sağlamasıdır. Her ne kadar sistem içinde kullanıcı yetki kategorizasyonu ve sınırlandırması olsa da sistemin yöneticisi, teknik görevlisi bilişim personeli bütün veriyi görebilmektedir. Tüm yürüyen soruşturma verilerinin sisteme girilmek zorunda olduğu göz önüne alındığında bütün soruşturmanın büyük bir tehlike altında olduğu düşünülmektedir.

Mevcut durumda güvenlik alanında söz konusu olan en büyük proje Emniyet Genel Müdürlüğü'nün yürüttüğü Polis Network (Polnet) Projesidir. Bu projenin diğer e-devlet uygulamalarından en önemli farkı yurttaşla iletişime giren açık bir sistem değil, yurttaş ilgilendiren işlemleri barındıran; fakat kurum içine dönük bir sistem olmasıdır. Sonraki bölümlerde bu proje ayrıntılı olarak incelenecektir.

Yukarıda Türkiye'de e-devlet pratikleri anlamında genel bir kategorizasyon yapılarak yürütülen projelerden bahsedilmiştir. Ancak bunların dışında da birçok e-devlet projesinin yürütüldüğünün veya hazırlandığının bilinmesi gerekir. Bu bağlamda Gümrük ve Ticaret Bakanlığı Merkezi Sicil Kayıt Sistemi (Mersis)⁶¹⁶, Maliye Bakanlığı Gelirler Genel Müdürlüğü Bilgisayar Otomasyonu (Vedop)⁶¹⁷, İçişleri Bakanlığı İl Envanteri

⁶¹⁵ a.k

⁶¹⁶ Bu proje 2006 yılındaki Bilgi Toplumu Stratejisinde belirlenen projelerdendir. Proje 08 Ekim 2010 tarihinde tamamlanmıştır. Sistem içerisinde tüm tüzel kişilikler ile ilgili ayrıntılı veriler ve bu tüzel kişiliklerin ortak ve kurucusu olan gerçek kişiler yer almaktadır. Yeni şirket tescili, tescil değişiklikleri ve ticaret sicili işlemleri bu proje üzerinden gerçekleştirilebilmektedir. İnternet üzerinden "<http://mersis.gumrukticaret.gov.tr>" adresinden sisteme girilebilmektedir. Ayrıca Gümrük Müsteşarlığı bünyesinde yasadışı eşya, taşıt trafiğini izleme ve bu kapsamda kaçakçılık ile yasa dışı emtia akışını engellemeye yönelik faaliyetleri kapsayan Gümrük Kapıları Güvenlik Sistemleri Projesiyle (GÜMSİS), dış ticaret verilerinin tümünün geçmişiyile birlikte bir veri deposunda tutulacağını belirten Gümrük Veri Ambarı Sistemi Projesi (GÜVAS) yürütülmektedir.

<http://www.gumrukticaret.gov.tr>, (Erişim Tarihi: 12.02.2013).

⁶¹⁷ Maliye Bakanlığı Gelir İdaresi Başkanlığı tarafından yürütülen vergi dairesi işlemlerinin tümünün dijital ortamda gerçekleştirilmesine yönelik bir bilişim projesidir. Vedop ile hedeflenen; vergi dairesi işlemlerinin tümünün bilgisayarlarla yapılmasının sağlanarak iş yükünün azaltılması, vergi dairesi çalışmalarında etkinlik ve verimliliğin artırılarak yurttaşlara ve işletmelere daha iyi hizmet sunulması, vergi yükünün daha adil bir şekilde dağıtılması ve vergi tahsilatının daha verimli bir hale getirilmesi olarak ifade edilmektedir. Vedop, 1995 yılında, vergi dairelerinin otomasyona geçirilmesi amacıyla pilot proje olarak başlatılmıştır. Pilot projenin başarılı olması neticesinde 25 Kasım 1998 tarihinde Vedop - 1 projesi başlamış ve iki yıl içerisinde 22 ildeki 155 vergi dairesinin ve 5 defterdarlığın otomasyonu gerçekleştirilerek proje tamamlanmıştır. 2004 yılında projenin ikinci

Modernizasyonu (İlemod), Tapu Kadastro Genel Müdürlüğü Bilgi Sistemi (Takbis)⁶¹⁸ gibi çeşitli projelerin bulunduğu ifade edilebilir.

Türkiye’de e-devlet süreci neticesinde bir takım kamu hizmetlerinin veriliş şeklinin hızlandığı, kolaylaştığı ifade edilebilir. Ancak bu süreci bütüncül bir bakış açısında incelediğimizde önemli yanlış ve eksikliklerin süregeldiği görülmektedir. E-devlet süreci ile ilgili olumsuzluklardan en dikkat çekici olanı bu teknolojilere yapılan gereksiz ve kontrolsüz kamu harcamalarıdır.⁶¹⁹ E-devlet projeleri ile birlikte hemen hemen bütün kamu kurumları bunların alt kuruluşları veritabanı oluşturma ve verileri dijitalleştirme sürecine girmiştir. Bu süreçte irili - ufaklı birçok bilişim sistemi ve programı ortaya çıkmıştır. Bütün bu sistemlerin her birisi için ayrı ayrı yazılım programları, sunucular, bilgisayar teknolojileri satın alınmış/alınmaktadır. Ayrıca bunların hepsinin kendine özgü işletme maliyetleri de bulunmaktadır. Aynı amaca hizmet eden fakat birbirinden ayrı sistemler oluşturulmuştur. Hatta aynı kurum içinde aynı işlevi görebilecek birden fazla proje hazırlanmış, sonrasında hazırlananlardan hangisi tutulursa o proje uygulanmaya devam edilmiş, diğer projelere yapılan yatırımlar boşa gitmiştir. Neticede yurttaşların vergileriyle dolan devletin kasasından yüklü miktarda para çıkmıştır/çıkmaktadır. Farklı kurumlarda oluşan veritabanlarını tek bir elde, tek bir yönetim altında toplayacak bir mekanizma olmamıştır. Bu bakımdan Türkiye’de eğer bir bilgi toplumu süreci varsa, bu sürecin çok kontrolsüz ve dağınık bir şekilde başladığını ve devam ettiğini söyleyebiliriz.

aşaması olan ve bu otomasyonun tüm ülkedeki vergi dairelerine ve veri işlemi yapan diğer birimlere yaygınlaştırılmasını amaçlayan Vedop - 2 projesi başlatılmış ve tamamlanmıştır. Projenin üçüncü aşaması olan Vedop - 3 ise Temmuz 2007’de başlamıştır. Vedop - 3 projesiyle birlikte son gelinen noktada çevrimiçi olarak hizmet verecek olan vergi dairelerinin e-tahsilat ile vergi, ceza ve gecikme zamlarını, elektronik ortamda tahsil edebilmeleri, mükellef cari hesap uygulaması ile mükelleflerin vergi borçlarının ve alacaklarının banka hesaplarında görülebilmesi, e-haciz uygulaması ile de devletin vadesi geçen vergi alacaklarının tahsili için elektronik ortamda haciz işlemi gerçekleştirebilmesi amaçlanmıştır. Gelir İdaresi Başkanlığı, *2010 Yılı Faaliyet Raporu*, 2011, s.8., http://www.gib.gov.tr/fileadmin/faaliyetraporlari/2010/Faaliyet_raporu_2010.pdf, (Erişim Tarihi: 12.02.2013).

⁶¹⁸ Tapu ve Kadastro Bilgi Sistemi (Takbis): Tapu ve Kadastro Genel Müdürlüğü ve taşra teşkilatları tarafından yürütülen, ülke çapındaki bütün tapu kadastro işlemlerinin coğrafi bilgi sistemleri kullanılarak dijital ortamda gerçekleştirilmesi ve tapu kadastro işlemleri konusunda anlık olarak yerel yönetimler ile diğer ilgili kamu kuruluşlarına yeknesak, doğru güvenilir ve güncel bilgiler sunulmasını amaçlayan bilişim sistemidir. Projenin temel hedefi; konumsal harita bilgilerine dayalı olarak tapu sicilindeki mülkiyet ve kadastro bilgilerini oluşturmaktır. Takbis, 26 Aralık 2000 tarihinde Havelsan A.Ş. tarafından Tapu ve Kadastro Genel Müdürlüğü tarafından belirlenen istek ve ihtiyaçlara göre hazırlanmaya başlanmış, 2005 yılında proje tamamlanmış ve bu tarihten beri bölge müdürlükleri, tapu sicil müdürlükleri, kadastro müdürlükleri ve kadastro şefliklerinde veri girişi ve veri sorgulaması yapılarak kullanılmaktadır. Şaban İnam, Hakan Ayber, “E-devlet İçerisinde E-kadastro ve E-tapu’nun Yeri”, *Selçuk Üniversitesi Jeodezi ve Fotogrametri Mühendisliği Öğretiminde 30. Yıl Sempozyumu*, Konya, 16-18 Ekim 2002.

⁶¹⁹ Banu Salman, “Bilgi ve İletişim Teknolojileri Kullanan mı Üreten mi Olacağız?”, *www.emo.org*, (Erişim Tarihi: 28.12.2012).

Türkiye’de e-devlet süreci ülkenin, kurumların ve yurttaşların ihtiyaçları dikkate alınarak, planlı bir şekilde olmamış, kamu kurumlarındaki yöneticilerin “Haydi biz de bir veritabanı oluşturalım!” söylemleriyle şekillenmiştir. Bu durum da benzer projeler için aynı yatırımların yapılmasına yol açmış ve maliyet yine yurttaşın bütçesinden çıkmıştır/çıkmaktadır. Mesela 2011 Türkiye Yatırım Programında yer alan bilgi ve iletişim teknolojileri proje sayısı 210’dur. Bu projelerin toplam yaklaşık tutarı da 4,9 milyar TL’dir.⁶²⁰

Türkiye’deki e-devlet süreci ile ilgili olumsuzluklardan ikincisi olarak devletin yurttaşlarının özel hayatına ilişkin verileri korumadaki yetersiz oluşu ifade edilebilir. Nitekim daha önce de bahsedilen 2010 yılında 70 milyon Türkiye Cumhuriyeti yurttaşının kimlik ve adres bilgilerinin çalınmış olması da bunu açıkça ortaya koymaktadır. Günümüzde internet ortamında bir kişinin sadece TC kimlik numarasını kullanarak o kişiyle ilgili yüzlerce bilgiye ulaşılabilmesi mümkündür. Örneğin, bir kurumun internet sitesinin ilgili kısmına yazılacak TC kimlik numarası ile o kişinin adı, soyadı, doğum tarihi gibi bilgilere erişilebilmektedir. Doğum tarihi ve ad, soyad bilgilerini bir başka kurumun internet sitesinde kullanarak bu kez o kişinin ikametgah adresi elde edilebilmekte, adres bilgileriyle bir başka kurumun internet sitesinden nüfus cüzdanı, vergi numarası, SGK numarası gibi bilgilere zincirleme şekilde ulaşılabilir. Elde edilen bu bilgilerle de söz konusu kişinin telefon numarasından, aldığı maaşın miktarına, maaşına ne oranda zam yapıldığına, kaç yıldır çalıştığına, diploma notunun kaç olduğuna, su, elektrik ve telefon faturalarına ve ÖSYM sınavlarından aldığı puanlara kadar pek çok bilgiye ulaşmak mümkün hale gelmiştir.⁶²¹ İnternette elde edilen bu bilgilerle sahte kimlik, sahte sürücü belgesi, kredi kartı hırsızlığı, dolandırıcılık yapılabileceği düşünüldüğünde durumun ciddiyeti daha net ortaya çıkmaktadır.

Diğer taraftan internet üzerinde virüs ve spam kurbanı olma, dolandırılma, kimlik bilgisi hırsızlığının konusu olma gibi yurttaşları tehlikeye sokacak çok sayıda ihtimaller bulunmaktadır. Bu ihtimallerin olduğu bir ortamda, kişinin e-Türkiye şifresi alarak bunu internette kullanması riskli gözükmektedir. 2011 yılında yapılan TÜİK Hanehalkı Bilişim Teknolojileri Kullanım Anketine göre bireylerin bilgi ve iletişim teknolojileri kullanımında karşılaştıkları güvenlik problemleri söz konusu teknolojilerden faydalanma düzeylerini

⁶²⁰ Devlet Planlama Teşkilatı, *a.g.k.*, 2011, s.74.

⁶²¹ Örneğin, 24 - 31 Aralık 2012 tarihleri arasında <https://hmbasvuru.hazine.gov.tr/HMBasvuru/> internet adresinden Hazine Müsteşarlığı Uzman Yardımcılığı sınavı başvuruları yapılmıştır. Bu tarihler arasında TC kimlik numarası bilinen her hangi birisinin kimlik numarası giriş yapıldığında sistem, o kişinin KPSS notlarını otomatik olarak vermiştir. Başka bir örnek olarak şunu gösterebiliriz, bir kişinin TC kimlik numarasını biliyorsanız, bununla kişinin Emekli Sandığı numarasına ve <https://ebordro.muhasabat.gov.tr/Bordro/gen/login.htm> adresinden kişinin kamu görevlisi olup olmadığı, kaç yıldır çalıştığı, ne kadar maaş aldığı ve hangi kurumda çalıştığı gibi bilgilere ulaşabilirsiniz.

etkileyen önemli bir faktördür. İnternet kullanıcıları arasında güvenlik sorunu ile karşılaşma oranları 2007, 2008, 2009 ve 2010 yıllarında sırasıyla %31, %29, %28,9 ve %46,8 olarak belirlenmiş olup son yıl oranının yüksekliği dikkat çekmektedir.⁶²² Esasında 2010 yılındaki bu oran, internet üzerinde yapılan her bir işlemde %50’lik bir ihtimalle güvenlik tehlikesi ile karşı karşıya kalındığını ifade etmektedir.

İnternet üzerinden yapılan işlemlerin güvenliği ve bu işlemlerden dolayı ortaya çıkabilecek risklere yönelik bireyleri koruyacak kapsamlı bir yasal düzenleme bulunmamaktadır. Bu kapsamda mesela bankadaki hesabınız internet üzerinden kötü niyetli kişilerce kullanılarak bir terör örgütüne para aktarılırsa, mevcut hukuki boşlukta, muhtemelen paranızı geri alamayabilirsiniz, ama terör örgütüne yardımdan tutuklanabilir, hatta hüküm giyebilirsiniz.⁶²³ Yani mağduriyetinizin telafisi için uğraşırken, daha da mağdur olabilirsiniz. Bu gibi durumları netleştirecek kanuni düzenlemelere ihtiyaç bulunmaktadır.

Türkiye’de e-devlet uygulamalarının gözetime bakan yönünde bu uygulamaların birer veri toplama aracına dönüştüğü bir gerçektir. Gerek istihbarat birimleri gerek diğer kurumlar e-devlet yoluyla toplanıp, sınıflandırılan ve depolanan bu verileri kullanmaktadırlar. Dolayısıyla iktidar ve iktidarın araçları olan bu kurumlar için yurttaşın kendiliğinden gelerek verilerini teslim etmesi bulunmaz bir fırsat olmuştur.

3. Türkiye’de Gözetim Toplumu Tehlikesi

Türkiye’nin bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişmelerle bilgi toplumuna evrilmesi süreci aynı zamanda beraberinde gözetim toplumu tehlikesini getirmiştir. Yeni teknolojiler gözetim potansiyelini sürekli arttırmaktadır.⁶²⁴ Artan gözetim potansiyeli toplumda giderek suç korkusu ve gözetlenme paranoyasını tetiklemektedir. Diğer taraftan toplumun fertleri özellikle güvenlik gerekçesi ile sürekli olarak tanımadıkları gözler tarafından gözetlendiklerinin farkındadırlar. Ancak gözetimin boyutlarını tam olarak kestirememektedirler.⁶²⁵ Bu bilinmezlik ve takibat altında olma kaygısı Türkiye’de de her geçen gün artış göstermektedir. Zira merkez ülkelerde üretilen gözetim teknolojisi kapitalist raylarda Türkiye’ye sürekli olarak transfer edilmektedir. Büyük silah tüccarlarının silah satabilmek için suni savaşlar oluşturması gibi gözetim teknolojisini satan ve satın alanlar da gözetimin gerekliliğini güvenlik çatısı altında meşrulaştırmaktadırlar. Önceki bölümlerde bahsedilen “Echelon” gibi yüksek teknolojiye gözetim güvenlik sistemleriyle gözetimin

⁶²² Devlet Planlama Teşkilatı, *a.g.k.*, 2011, s.31.

⁶²³ Hakan Yıldırım, *a.g.k.*, s.XIX.

⁶²⁴ Veysel Bozkurt, *a.g.k.*, s.3.

⁶²⁵ David Lyon, *a.g.k.*, 2006, s.38 - 41.

büyükluğu takdir edildiğinde Türkiye’de de benzer veya daha ileri gözetim yapılarının olup olmadığı bilinmezliği ülkede oluşan gözetim toplumu tehdidinin boyutlarıyla ilgili korkutucu senaryolara izin vermektedir. Çalışmamızda eldeki veriler ve gözlemler göstergesinde Türkiye’nin bir gözetim toplumu olduğu iddia edilmektedir. Bu bölümde Türkiye’nin gözetim toplumuna evrildiği iddiası somut örneklerle ortaya konulmaya çalışılacaktır.

Toplumsal hayatta kişisel verilerin depolandığı kamusal ve özel geniş veri tabanlarının oluşturulması ve veri toplama araçlarının; yani gözetim araçlarının artış göstermesi gözetim toplumunun en önemli göstergeleri olduğu önceki bölümlerde ifade edilmiştir. Bu bağlamda gözetim toplumu tehlikesini araştırırken sadece devlet eliyle yapılan değil, sivil toplum kuruluşları, bireyler, şirketler, dernekler, vakıflar gibi toplumsal yapıyı oluşturan bütün yapı taşları ekseninde gerçekleştirilen gözetim uygulamalarına bakmak gerektiği düşünülmektedir. Bu bakımdan öncelikle ülkede devlet eliyle yapılanların dışındaki gözetim faaliyetlerinden önemli görülenler incelenecek, sonrasında kamu kurumları bağlantılı olanlarına değinilecektir.

Günümüzde gözetim teknolojileri internet sitelerinde, alışveriş merkezlerinde uygun fiyatlara satılabilmektedir.⁶²⁶ Hatta akıllı telefonlar için bazı takip uygulamaları ücretsiz olarak bile temin edilebilmektedir. Bu gözetim teknolojileri içerisine güvenlik kameraları, kablosuz kameralar, gizli kameralar, casus kameralar, dinleme cihazları, ses kaydediciler, cep telefonu dinleme cihaz ve programları, ortam ses alma cihaz ve programları, GPS takibi cihazları, internet hareket geçmişinin tespitine yönelik yazılımlar girebilmektedir.⁶²⁷ Bu gözetim cihaz ve uygulamalarının rahatlıkla satılabilmesi, bunlar hakkında reklamlar verilebilmesi, insanların gerek internet üzerinden gerek satış dükkanlarından bunları herhangi bir izin belgesi vb. olmadan alabilmesi ülkemizde gözetimin genişleme serbestisini açıkça ispatlamaktadır. Bunların alım - satımına yönelik herhangi bir hukuki düzenleme bulunmamaktadır. Dolayısıyla yurttaşlar satın aldıkları takip cihazları ile komşularının, akrabalarının, arkadaşlarının veya düşmanlarının iletişimlerini kolaylıkla dinleyip, kaydedebilirler. Hatta bu şekilde elde edilen veriler kişilerin aleyhine olarak da kullanılabilir. Örneğin, kişinin ses kayıtları veya cinsel içerikli görüntüleri kullanılarak kendisine şantaj yapılabilir. Buna 2010 yılında eski CHP Genel Başkanı Deniz Baykal’a ve 2011 yılında eski MHP Başkan Yardımcılarına yönelik yapılan ve istifalarıyla sonuçlanan kaset şantajları örnek

⁶²⁶ Örneğin, <http://tr.mspy.com> internet sitesine girerek giden ve gelen çağrıları dinleme, SMS ve e-posta takibi, GPS takibi, internet geçmişinin takibi gözetim faaliyetlerini yapabilen bir programı satın alabilirsiniz.

⁶²⁷ <http://sistembir.com/index.php/cPath/32> internet sitesinden sipariş vererek belirtilen gözetim cihazlarından uygun fiyata satın alabilirsiniz.

gösterilebilir. Örneklerdeki durumlarda hem özel hayatın gizliliği sınır tanımaz bir şekilde ihlal edilmiş hem de siyasetin şekillendirilmesinde bu gözetim verileri kullanılmıştır. Nitekim gözetim toplumlarında bu tür vakaların olması ihtimali yüksektir.

Gözetim toplumunun sokaktaki yansıması güvenlik kameralarıdır. Ülkemizde güvenlik kameralarının sayısı giderek artmaktadır. Alışveriş merkezlerinde, bankalarda, dükkanlarda, apartman girişlerinde, asansörlerde, ibadethanelerde, otoparklarda yani hemen hemen her yerde güvenlik kameralarına rastlamak mümkündür. Yurttaşlar hiçbir engel olmadan kendi güvenlik kamera sistemlerini kurabilmekte ve diğer yurttaşların görüntülerini kaydedebilmektedir. Diğer taraftan birçok il ve ilçe belediyeleri istedikleri alanlara güvenlik veya trafik kameraları yerleştirip, buraların canlı görüntü kayıtlarını internet üzerinden servis edebilmektedir.⁶²⁸

Türkiye'nin gözetim toplumu olduğunun en önemli göstergelerinden birisi olarak özel dedektiflik büroları örnek gösterilebilir. Adli soruşturmalar kapsamında yürütülen gözetim faaliyetleri bir takım hukuki düzenlemelerle hakim kararı ile yapılması şartına bağlanmıştır. Ancak adli birimlere benzer gözetim faaliyetlerinde bulunan özel dedektiflik bürolarına yönelik hiçbir hukuki düzenleme bulunmamaktadır.⁶²⁹ Bu kuruluşlar yasal boşluklardan faydalanarak müşterilerin talepleri doğrultusunda fiziki ve teknik takip, ortam dinlemesi, gizli izleme ve dinleme yapabilmektedirler. Bu kapsamda elde edilen verilerin şantaj, tehdit, casusluk için kullanılma ihtimali de her zaman mümkün gözükmektedir. Diğer taraftan faaliyet alanlarını sınırlayan herhangi bir düzenleme de bulunmamaktadır. Bu bakımdan evli çiftten birisinin diğerini takip ettirmesinden tutun banka patronunun çalışanı personelin internet trafiği ve cep telefonu görüşmelerine kadar her türlü konuda takip, kayıt yapılabilir. Ayrıca dipnotta belirtilen örnekte olduğu gibi buralarda çalışanların eski istihbarat görevlileri ve eski kamu çalışanları olması bunların kamu kurumlarında bulunan gizli verilere bir şekilde ulaşılma ihtimalini de içinde barındırmaktadır.⁶³⁰

⁶²⁸ İstanbul Büyükşehir Belediyesi kamera görüntülerine canlı yayında <http://tkm.ibb.gov.tr/> internet adresinden ulaşılabilir. Ankara Sincan Belediyesi tarafından tüm parklara yakın çekim yapan kameralar yerleştirilmiştir. Bu görüntüler canlı yayında <http://kamera.sincan.bel.tr/> internet adresinden izlenebilmektedir.

⁶²⁹ 07.06.2013 Tarihli "Telekulak Komisyonu: MİT'i Başbakanlık Teftiş Kurulu Denetlesin" Başlıklı Radikal Gazetesi Haberi.

⁶³⁰ 10 Haziran 2011 tarihinde Ankara Organize Suçlarla Mücadele Şube Müdürlüğü tarafından bir özel dedektiflik şirketine yönelik yapılan operasyonda üç emekli astsubay, bir muvazzaf binbaşı, bir nüfus müdürlüğü çalışanı, bir tapu dairesi çalışanı, bir ticaret odası çalışanının da aralarında bulunduğu yirmi kişi yakalanmıştır. Bu operasyonda gizli çekimlerde kullanılan anahtarlık, saat, kalem, rozet şeklinde on altı kamera, bir adet illegal olarak alınan seslerin kayıtlarının bulunduğu cd, üç gprs araç takip cihazı, iki ses ve görüntü kaydı arama dedektörü, bir adet araca monteli ortam dinleme cihazı, yedi mikro kaset, iki dizüstü bilgisayar ele geçirilmiştir. <http://t24.com.tr/haber/ozel-dedektiflik-operasyonu-20-gozalti-ankara-aa/150254>, (Erişim Tarihi: 18.02.2013).

Ülkemizde devlet iradesi ve kamu kurumları ile ilişkili gözetim faaliyetleri de oldukça çeşitlilik göstermektedir. Bu şekilde kameralı gözetim, biometrik gözetim, cep telefonu dinlemesi, ortam dinlemesi, fiziki takip, dijital takip gibi dünyada bu konuda önde olan İngiltere gibi ülkelerin uyguladığı tüm gözetim pratiklerine rastlamak mümkündür.

Günümüzde topluma topyekün yöneltilen gözetim uygulamalarında geline en son noktayı göstermek açısından biometrik kimlik kartları ve Avuçiçi Damar İzi Biometrik Tanımlama Sistemi örnek gösterilebilir. Tübitak UEKAE tarafından Tübitak 1007 programı çerçevesindenüfus cüzdanının yerini alması planlanan Biometrik Kimlik Kartı Projesi yürütülmektedir. Bu projenin hukuki zemini 4 Temmuz 2007 tarihli ve 26572 sayılı Resmi Gazetede yayımlanan Başbakanlık Genelgesi ile oluşturulmuştur.⁶³¹

Biometrik Kimlik Kartı Projesi çerçevesinde tüm yurttaşlara kendi bedenlerine ait tanımlayıcı biometrik verilerin içerisinde bulunacağı tanımlayıcı kimlik kartları dağıtılmak istenmektedir. Bu kapsamda biometrik kimlik kartlarının özel veya kamusal faaliyetler yürütülürken bireye dair kimlik doğrulama işlemlerinde tek araç olarak kullanılması planlanmaktadır.⁶³² Kimlik doğrulama amacıyla bu kartlar içerisinde yurttaşların kimlik bilgileri, parmak izleri (farklı biometrik veriler de eklenebilir) ve kimlik doğrulama sertifikaları bulunacağı ifade edilmektedir. Aynı zamanda bu kartların doğrulamasını yapacak olan, şimdiki pos cihazları gibi kart erişim cihazlarının ilgili kurum ve birimlere dağıtılması öngörülmektedir.⁶³³ Örneğin; yurttaş bankaya veya elektrik idaresine gittiğinde kendisinden yukarıda ifade edilen biometrik kimlik kartı alınıp bu cihazlardan geçirilecek, sonrasında bu cihazlar da merkezdeki kimlik doğrulama sunucusuyla iletişime geçecek ve şahsın kimliğinin doğrulaması gerçekleştirilmiş olacaktır.

Biometrik kimlik kartlarının gözetime bakan boyutunda tehlike arz eden nokta bireyin bedenine ait olan verinin dijital karşılığının kamu kurumlarının veritabanlarında depolanacak olmasıdır. Böylece tüm yurttaşların parmak izi (eğer DNA gibi başka biometrik veri kullanırlarsa bunlar) verileri elde edilecektir. Bu şekilde bireyin her dokunuşunun gözetlenebilmesinin de önü açılmış olacaktır. Biometrik verilerdeki gözetimin bu hakimiyeti

⁶³¹ www.bilgiguvenligi.gov.tr/...tc-kimlik-karti-ve-euygulamalari/download.html, (Erişim Tarihi: 18.02.2013).

⁶³² www.isay.icisleri.gov.tr, (Erişim Tarihi: 28.12.2012).

⁶³³ Bunların yanı sıra kimlik doğrulamada kullanılacak güvenlik seviyesi, geçerlilik süresi vb. kimlik doğrulama politikasını belirleyen merkezi sunucu olan Kimlik Doğrulama Politika Sunucusu ve kart erişim cihazlarındaki güvenlik servislerinin kullanımını sağlayan ara birim yazılımlarından oluşan (GSP, WIA ve OYA) Güvenlik Servisleri Platformu da sistem içinde olacaktır. www.bilgiguvenligi.gov.tr/...tc-kimlik-karti-ve-euygulamalari/download.html, (Erişim Tarihi: 18.02.2013).

yurttaşların bedenini, gözetlemenin alanı olmakla birlikte kaynağı haline de getirecektir.⁶³⁴ Böylece yurttaşlar sayısallaşan bedenleriyle iktidar önünde gittikçe küçülecek ve değerlerini yitirecektir.

Türkiye’de gözetim evrenini anlama açısından ifade edilebilecek olan diğer bir biometrik gözetim projesi 2013 yılında tüm sağlık kuruluşlarında uygulanmaya başlanmış olan *Avuçiçi Damar İzi Biometrik Tanımlama Sistemidir*. 2012 yılında yapılan bir hukuki düzenleme ile 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu’nda yapılan değişiklikle SGK Başkanlığı’na genel sağlık sigortalılarının, sağlık hizmet sunucularına sağlık hizmeti almak amacıyla müracaat etmeleri halinde biometrik yöntemlerle de kimliklerinin tespit edilmesine ilişkin yetki verilmiştir.⁶³⁵ Bu değişiklikle birlikte Sağlık Uygulama Tebliği’nde de, biometrik kimlik doğrulama uygulaması için düzenleme yapılmıştır. Buna göre kimlik tespitini, biometrik kayıt veya biometrik kimlik doğrulama işlemini usulüne uygun yapmayan ve bu nedenle bir başka kişiye sağlık hizmeti sunulmasına yol açarak kurumun zarara uğramasına sebebiyet veren sağlık hizmeti sunucularından ödenen tutarın geri alınacağı hüküm altına alınmıştır. Ayrıca bu tebliğde biometrik kimlik doğrulama işlemlerini zorunlu hale getirecek bir takım düzenlemeler yapılmış olup bir biometrik kimlik doğrulama metodu olarak “*avuç içi damar izi sistemi*” kabul edilmiştir.⁶³⁶

Biometrik kimlik doğrulama sistemi kapsamında ilk planda Türkiye’deki tüm genel sağlık sigortalıların *avuç içi damar izleri* alınarak tek bir veritabanında toplanması hedeflenmektedir. Bu çerçevede *avuçiçi damar izi* kaydı alınan yurttaşlar herhangi bir sağlık kuruluşuna gittiklerinde öncelikle *avuçiçleri* taranacak ve veritabanında kayıtlı olan iz ile karşılaştırılarak kimlik doğrulaması yapılacaktır.⁶³⁷

⁶³⁴ David Lyon, *a.g.k*, 2006, s.139 - 143.

⁶³⁵ 5510 sayılı Kanunun 67. maddesinin üçüncü fıkrasında yer alan hükme göre; sağlık hizmeti almak için sağlık kurumlarına başvuran kişilerin kimlik doğrulamaları nüfus cüzdanı, sürücü belgesi, pasaport veya evlilik cüzdanı gibi kimlik kartları ile yapılmaktaydı. 01 Mart 2012 tarihli ve 6283 sayılı Kanunun 1. maddesiyle 5510 sayılı Kanunun 67. maddesinin 3. fıkrasında yapılan düzenlemelerle yurttaşların TC kimlik numarası bulunan nüfus cüzdanı, sürücü belgesi, pasaport veya evlilik cüzdanı ve/veya biometrik yöntemlerle kimlik tespit işlemleri tamamlandıktan sonra sağlık hizmeti almaları şartı getirilmiştir. Sosyal Güvenlik Kurumu, *Avuç İçi Damar İzi Sistemiyle Kimlik Doğrulama Sistemine Ait Kılavuz*, 2012.

⁶³⁶ *Avuçiçi Damar İzi Biometrik Tanımlama Sistemi*, Sosyal Güvenlik Kurumu tarafından bazı illerde 15 Eylül 2012 tarihinde başlamış olup 81 ile yaygınlaştırılmasının 15 Ocak 2013 tarihine kadar gerçekleştirilmesi öngörülmüştür. Fakat bu öngörülen sürede dahil olmak üzere istenilen seviyeye ulaşılamamıştır. Ancak 01 Aralık 2013 tarihinde tüm sağlık kuruluşlarında topyekün bu sisteme geçilmiştir. *a.k*

⁶³⁷ Buna göre genel sağlık sigortalısının ilk kaydı esnasında, TC kimlik numarası bulunan nüfus cüzdanı, sürücü belgesi, pasaport veya evlilik cüzdanıyla sağlık hizmeti almak amacıyla sağlık hizmeti sunucusu tarafından yapılmaktadır. İlk kayıt işlemi tamamlanan genel sağlık sigortalısının sağlık hizmeti sunucusuna müracaatında MEDULA takip numarası alınması işlemi öncesinde sağlık hizmeti sunucusu tarafından sağ veya sol eline ait *avuç içi damar izi sistemi* ile biometrik kimlik doğrulaması yapılmaktadır.

Mevcut durumda tüm ülkedeki genel sağlık sigortalıların avuçiçi damar izlerinin örnekleri toplanarak siyasal otoritenin elinde tek bir veritabanında depolanmaya başlanmıştır. Ülkemizde gözetim artık Lyon'un ifadesiyle kimlik belirlemek ve sınıflandırmak amacıyla izlemek, denetlemek, test etmek için derinin altına kadar inmiştir.⁶³⁸

Ülkemizde uygulanan gözetim faaliyetlerinde güvenlik tabanlı olanlar ağır basmaktadır. Bu faaliyetler çalışmanın sonraki kısımlarında anlatılacaktır. Ancak burada polisin yurttaşların parmak izi verilerini alabilmesi, bunları kategorize ederek veritabanlarında saklamasından bahsedilmek istenmektedir. Polis Vazife ve Salahiyetleri Hakkındaki Kanunun 5. maddesinin 5. fıkrası polisin parmak izi alma yetkisini düzenlemektedir:

“Polis; a) Gönüllü, b) Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan, c) Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen, ç) Türk yurttaşlığına başvuruda bulunan, d) Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı, e) Gözaltına alınan, kişilerin parmak izini alır.”

Yurttaş, herhangi bir suç şüphesi altında olsun veya olmasın yukarıda belirtilen işlemlerden herhangi birisini gerçekleştirdiğinde polis, onun parmak izini alabilmektedir. Bu bakımdan toplumdaki hemen herkesin parmak izinin polisin veritabanlarında olabileceğini söylemek yanlış olmayacaktır.⁶³⁹ Uygulama neticesinde tüm parmak izleri Otomatik Parmak İzi Teşhis Sistemi (AFİS) olarak adlandırılan merkezi bir veritabanında tutulmaktadır.⁶⁴⁰ Suçluların tespiti aşamasında olay yerinden elde edilen parmak izlerinin bu veritabanından karşılaştırmasının yapılarak suç işleyen şahısların otomatik olarak tespitiyle adaletin hızlı gerçekleşmesi açısından sistemin sağlamış olduğu fayda şüphesiz tartışılmaz. Ancak bütüncül bir yaklaşım açısından yurttaşların parmak izleri bir şekilde bir veritabanında toplanmış olması gözetim toplumu endekslerine uyan bir uygulamadır.

Gözetim toplumu refleksi olarak ülkemizde gözetim arkaplanlı çeşitli projeler ortaya atılabilmekte ve bunlara TBMM’de yapılan oylamalarla bir anda icazet verilebilmektedir. Örneğin henüz Meclis gündemine gelmese de bunlardan birisi de güvenlik güçleri tarafından tüm araçlara GPS/GPRS Entegre Sistemleri yerleştirilmesi ve böylece karayollarında hareket ve seyahat eden bütün araçların sürücü ve hız kontrollerinin uydu vasıtasıyla otomatik olarak

Sağlık hizmeti sunucusu tarafından avuç içi damar izi sistemiyle biometrik kimlik doğrulama işlemi yapılmadan genel sağlık sigortalısı adına MEDULA takip numarası alınmasına MEDULA sistemi tarafından izin verilmemektedir. Sağlık hizmeti sunucusu tarafından genel sağlık sigortalısının, avuç içi damar izi sistemiyle biometrik kimlik doğrulaması yapıldıktan sonra genel sağlık sigortalısı adına MEDULA takip numarası alınarak sağlık hizmeti sunulmaya başlanabilmektedir. Sağlık hizmeti sunucuları tarafından genel sağlık sigortalısı adına alınan her provizyonda belirtilen kimlik doğrulamasının yapılması gerekmektedir. *a.k*

⁶³⁸ David Lyon, *a.g.k*, 2006, s.139 - 143.

⁶³⁹ Hakan Karakehya, *a.g.k*, s. 343 - 344.

⁶⁴⁰ Murat Erdal, *a.g.k*, s.22.

gerçekleştirilip, merkezi bir veri tabanına kaydedilmesidir.⁶⁴¹ Böyle bir sistemde düzenli olarak araçların koordinat sinyal bilgileri kaydedilebilecek ve böylece kimin hangi gün hangi saatte hangi dakikada nerede olduğu bilgisi siyasal otoritenin hizmetinde olacaktır.

Ülkemizde gözetim faaliyetlerinin en korkutucu kısmını Milli İstihbarat Teşkilatı (MİT), Jandarma İstihbarat Kurumu, EGM İstihbarat Dairesi Başkanlığı birimlerinin istihbarat toplama çalışmaları için yaptıkları gözetim uygulamaları oluşturmaktadır. Zira bu birimler tarafından gerçekleştirilen gözetim uygulamalarına yönelik halkın hiçbir farkındalığı bulunmamaktadır. Bu birimlerin hangi teknolojileri kullanarak, özel hayatın hangi alanına kadar sızarak veri topladıklarına dair duyum haricinde bilgi bulunmamaktadır. Dolayısıyla bu birimlerce gerçekleştirilen gözetim evreninin dış sınırları tam olarak kestirilememektedir. Neticede de, sonraki bölümlerde ifade edilecek olan, yurttışta gizli suç korkusu ile gözetim paranoyası oluşmasına yol açılmaktadır.

Ülkemizdeki bu istihbarat birimlerinin gözetim güçlerinin boyutlarının belirsiz olması durumu gözetim toplumlarında gözetime maruz kalan kişi üzerinde iktidar tarafından sürekli bir görülebilirlik hissi oluşturulması etkisiyle açıklanabilir. Gerçekte gözetleme süreci çok kısa olabilir veya hiç gözetleme de yapılmayabilir. Fakat gözetleme yapanın görülmediği ve gözetleme faaliyetinin her an yapılabilir olması hali gözetlenende sürekli gözetime maruz kaldığı düşüncesini oluşturur. Bentham bu durumu “iktidarın varlığının kanıtlanamaz olması ilkesi” ile açıklamaktadır. Ona göre bu ilke yurttışın kendine bakılıp bakılmadığını asla bilmemesi, fakat bunun her an olabileceğinden hiçbir kuşkusunun da bulunmamasını ifade etmektedir. Oluşturulan bu durumu iktidarın varlığının sürekliliğini sağlayan bir garantör olarak açıklamaktadır.⁶⁴²

Yukarıda ifade edilen somut örnekler paralelinde Türkiye’de bilgi toplumu dönüşümüyle girilen sürecin gözetim toplumuna evrilmiş olduğunu ifade edebiliriz. Zira gözetim hem halk nazarında sıradanlaşmış, hem de gözetimin her yerdeliği söz konusu olmuştur. Artık gözetimin öznesi sadece devlet değildir. Gözetim araçlarının herkes tarafından rahatlıkla satılabildiği ve kullanılabildiği toplumsal havada bireyin gözetimin nesnesi olması giderek pekişmiştir. Gözetimin nesnesi olarak birey diğer bireyler, özel kuruluşlar, kamu kurumları tarafından sistematik ve belirsiz bir şekilde izlenmekte, kaydedilmekte, dijitalleştirilmektedir.

⁶⁴¹ Hakan Yıldırım, *a.g.k.*, s.66.

⁶⁴² Yüksel Akaya, *a.g.k.*

II. TÜRKİYE EMNİYET TEŞKİLATI'NDA TEKNOLOJİK DÖNÜŞÜM

İktidar bireye ait olan bilgiyi ele geçirmek için başvurduğu gözetim faaliyetlerini ve gözetim teknolojilerini halk nezdinde meşru gösterebilmek için halkın kendisinden beklediği “güvenliği sağlama” görevini kullanagelmıştır. Özellikle 11 Eylül 2001 tarihinde ABD’de gerçekleşen terörist eylemlerden sonra iktidar güçlerinin eli güvenliği gözetleme faaliyetlerinde meşru araç olarak kullanma konusunda güçlenmiştir. Bu kapsamda tüm dünyada bu terörist eylemlerin sağladığı rüzgarla kapitalist düzenin daha çok kar etme arzusu bütünleşerek gözetim teknolojilerinin geliştirilmesine verilen ağırlık artış göstermiş; neticede gözetim başarıyla küreselleştirilmiştir. Küreselleşen gözetimin etkisiyle iktidar güçlerince Gary T. Marx’ın ifade ettiği “yüksek güvenli topluma” ulaşılması gereken bir toplumsal aşama olarak bakılmaya başlanmıştır.⁶⁴³

Emniyet Teşkilatı’nın da Türkiye’deki bilgi toplumu olma stratejisi kapsamında pasaport, araç alım - satım gibi işlemlerinin internet üzerinden verilmesi gibi kamu hizmetlerini dijitalleştirme yönünde çalışmaları olmuştur. Ancak esas itibariyle Emniyet Teşkilatı’ndaki gelişimin yönü yurttaşa verilen hizmetlerin dijitalleşmesinden ziyade elektronik imza, Genel Bilgi Toplama (GBT), Otomatik Parmakizi Teşhis Sistemi (AFİS), Tahdit Projesi gibi kendi iç işleyişinin dijitalleştirilmesi yönünde olmuştur. Yani yurttaşlardan ve Mernis Projesi gibi diğer e-devlet veri tabanlarından temin edilen verilerin depolanması, kategorize edilmesi, sorguya hazır hale getirilmesi, analitik amaçlı ilişkilendirilmesi gibi çalışmalarla personelin verilere hızlı erişiminin sağlanması; personelin suç şüphesi seviyesini basit, makul ve kuvvetli olarak ayırabilecek güce ulaşabilmesi için mümkün olduğu kadar ona yurttaşa dair her türlü veriyi sunma, personelin suçu ve failleri en kısa zamanda tespit edebilmesi için analiz kabiliyetine ve imkanlarına sahip olması gaye edinilmiştir.

Emniyet Teşkilatı’nda Türkiye’deki bilgi ve iletişim teknolojileri gelişimine uyum, özellikle Polnet ve Mobese gibi projeler ve bunların bileşenleri alt programlarla suçun azaltılması, faillerin tespiti ve yakalanması gibi güvenliğin sağlanması ve adaletin hızlı gerçekleşmesi amaçlı olarak sağlanmıştır. Polnet, Mobese ve diğer alt uygulamaların Emniyet Teşkilatı’ndaki gözetim teknolojileri olduğu ifade edilebilir. Diğer taraftan yürütüldüğü düşünülen çeşitli istihbarat ve analiz projelerinin de Emniyet Teşkilatı’ndaki gözetim faaliyetlerinin başka bir tarafı olduğu söylenebilir. Bu bölümde Emniyet Teşkilatı’nın kurumsal yapısı ve gelişim seyri anlatılacak, sonrasında da Emniyet Teşkilatı özelinde

⁶⁴³ Gary T. Marx, *a.g.k*, 2005, s.1.

gerçekleştirilen gözetim faaliyetlerinden Polnet ve Mobese projeleri gözetime bakan yönleriyle tanıtılacaktır.

1. Emniyet Teşkilatı'nın Örgütsel Yapısı

Emniyet Teşkilatı, rütbeleri polis memurluğundan başlayıp birinci sınıf emniyet müdürlüğüne kadar uzanan, tüm il ve ilçelerde örgütlenmiş, kırsalda görevini jandarmaya bırakmış, kentte ise görevi kendisi yürüten iç güvenlikten sorumlu ve İçişleri Bakanlığı'na bağlı genel müdürlük şeklinde örgütlenmiş bir devlet teşkilatıdır. Emniyet Teşkilatı'nda meydana gelen teknolojik gelişmeler paralelinde gözetim faaliyetlerini konumlandırabilmek için bu bölümde bir güvenlik birimi olarak Emniyet Teşkilatı'nın, güvenlik fonksiyonunun tarihsel süreç içerisinde dönemsel etkiler paralelinde evrimi ve günümüzde aldığı örgütsel yapı ortaya konulmaya çalışılacaktır.

Güvenlik, devletin varoluşundan beri onun en yüce kavramlarından biri olagelmıştır. Zira devletli yaşamla birlikte güvenlik devlet merkezli olmaya başlamıştır. Bireyler güvenliklerini sağlamaları için devlete misyon yüklemişlerdir. Böylece güvenliğin sağlanması devletin meşruiyet kaynaklarından birisi haline gelmiştir. Bu meşruiyet kaynağından aldığı güçle devlet şiddet araçlarına sahip olmuş ve halkı zapt etmeye yönelmiştir.⁶⁴⁴ Güvenlik kavramının kapsama alanı tarihi seyri içerisinde imparatorluğun güvenliğinden, devletin güvenliğine ve oradan da kapitalist devletle birlikte özel mülkiyetin güvenliğine doğru bir evrim izlenmiştir.⁶⁴⁵ Normal bir devletin asıl performansı, devlet içinde ve kendi egemenlik alanında mutlak memnuniyeti, “huzur, güven ve düzeni” sağlamak, bu yolla hukuk normlarının geçerliliği için önkoşul niteliğindeki normal durumu tesis etmek olmuştur.⁶⁴⁶

Emniyet Teşkilatı günümüz örgütsel yapısını kendi evreni içinde anlamak için tarihsel süreçteki evrimini anlamak gerekir. Günümüzdeki yapısı Osmanlı Devleti'ne kadar uzanan bir geçmişe dayanmaktadır. Bu bakımdan kısaca Osmanlı Devleti dönemindeki güvenlik anlayışına ve iç güvenliğin örgütlenme biçimine değinilecektir. Geleneksel devletlerde güvenlik, devletin tebaası altında olanların; yani hükmedilenlerin her türlü yurt dışından gelebilecek tehditlere ve iç isyanlara karşı dolaylı bir koruma altında olması şeklinde olmuştur.⁶⁴⁷ Dolayısıyla birincisi bu yapılarda iç ve dış güvenlik ayrımı net olarak gerçekleşmemiştir. İkincisi devlet padişah ile eşdeğer olduğu için iç ve dış güvenlik daha çok

⁶⁴⁴ Karl Marx, *Yahudi Sorunu*, Çev. Niyazi Berkes, Sol Yayınları, Ankara, 1997, s.35. Akt. Evren Haspolat, *Neoliberalizm ve Baskı Aygıtının Dönüşümü: Türkiye'de Özel Güvenliğin Gelişimi*, Notabene Yayınları, Ankara, 2012, s.85.

⁶⁴⁵ Evren Haspolat, *a.g.k.*, s.86.

⁶⁴⁶ *a.k.*

⁶⁴⁷ *a.k.*, s.47.

padişahın nizamının güvenliğini ifade ettiğinden hükmedilenlere yönelik dolaylı bir güvenlik temini anlayışı oluşmuştur. Dolayısıyla iç güvenlikteki amaç halkın güvenliğinin sağlanması değil, padişahın nizamının korunabilmesidir. Halkın güvenliğini sağlamak padişahın nizamının korunması amacının bir sonucudur. Zira halk da devlet de bir anlamda padişahın mülkü içinde yer almaktadır. Bu durum kendisi de bir geleneksel devlet olan Osmanlı Devleti için de geçerli olmuştur. Osmanlı Devleti'nde de devletin sahibi ve en yüksek yetkilisi olarak padişah yurt içi güvenliğin öncelikle en üst amiri konumunda yer almıştır.⁶⁴⁸

Osmanlı Devleti döneminde iç güvenlik subaşı altında bir örgütlenme ile sağlanmıştır. Ayrıca kadının emrinde bugünün asayiş amiri vazifesini gören şahne veya dizdarlar yer almıştır. Gece bekçiliği görevini yürüten asesler, 16.yy'da yeniçeriliğin ortadan kaldırılmasına kadar olan dönemde bostancıbaşı, yeniçerilerden oluşan kollukçu, başkent dışında subaşı da güvenlik hizmetinden sorumlu olmuştur. Genel olarak güvenlik birimleri; sadrazam, yeniçeri ağası, cebecibaşı, bostancıbaşı, çavuşbaşı, muhsir ağa, asesbaşı olarak kategorize edilmiştir. İstihbarat faaliyetlerini de böcekçibaşı yürütmüştür. Bunların yanı sıra esnaf pasbanları, vezir ve devlet erkanının maiyetinde satır denilen muhafızlar, kırsalda görevli kırserdarı, hapishane ve çevresinden sorumlu tomruk ağaları güvenlik güçlerine örnek olarak ifade edilebilir.⁶⁴⁹

Osmanlı Devleti'nde iç güvenlik hiyerarşik bir omurga üzerine kurulsaydı da oldukça karışık, çok parçalı ve askeri niteliği ağır basan bir yapıda var olmuştur. Bu yapının işleyişinde güvenlik birimleri günümüzdeki yapıda olduğu gibi çok müdahaleci değildir. Yanlış yapanı adaletin önüne çıkarmak ve mahkeme kararlarının uygulanmasını sağlamak mağdur tarafa ya da mağdurun yakınlarına ait bir sorumluluk olduğu için bu birimlerin düzenleyici rolü daha ağır basmıştır.⁶⁵⁰

Emniyet Teşkilatı'nın kurumsal geçmişi 169 yıl öncesine, 10 Nisan 1845 tarihine kadar götürülebilmektedir. Bu tarihte hazırlanan Polis Nizamnamesi ile ilk Polis Teşkilatı kurulmuştur. Böylece devletin güvenlik yapılanması, polis eliyle yürütülen iç güvenlik ve asker eliyle yürütülen dış güvenlik olarak ayrılmaya başlamıştır. 1879'da iç güvenlik görevi Seraskerliğe (Genelkurmay Başkanlığı) verilmiş olsa da, çok geçmeden Zabtiye Müşürlüğü kurulmuştur. Düşünce alanında batı etkisinin görüldüğü Tanzimat'tan sonra, batılı anlamda devlet düzeyinde teşkilatlanmanın görüldüğü dönem II. Abdülhamid dönemidir. II. Abdülhamit'in iç güvenliğe önem verdiği önceliklerle, mülki idare ve polis teşkilatı da

⁶⁴⁸ a.k, s.155 - 156.

⁶⁴⁹ Kemal Çiçek, "Osmanlı Devletinde Asayiş ve Emniyet Hizmetleri", *Avrupa Birliği Sürecinde Türk Polisi Uluslararası Sempozyumu*, EGM Basım, Ankara, 1997, s.123.

⁶⁵⁰ Evren Haspolat, a.g.k, s.45-46.

gelişmiştir. Ancak bu gelişme modern şekliyle özerk bir güvenlik teşkilatı değil, saraya ve bizzat sultana bağlı hafiye sistemi şeklinde olmuştur.⁶⁵¹ 1907’de iç güvenlikle ilgili olarak bir İç Güvenlik Nizamnamesi yayımlanmıştır. Bu nizamnameden iç güvenliğin önleyici zabıta görevleri, siyasi zabıta görevleri, adli zabıta görevleri şeklinde örgütlendiği anlaşılmaktadır. 22 Mayıs 1911 tarihli kanunla diğer illerden ayrı olarak İstanbul Polis Umumi Müdürlüğü kurulmuştur.⁶⁵² 1. Paylaşım Savaşı ve Kurtuluş Savaşı sürecinde Osmanlı Devleti’nde oluşturulmaya çalışılan merkezileşme yolundaki güvenlik yapısı etkinliğini kaybetmiştir. Bu paralelde iç güvenlik anlamında ortaya çıkan kaotik ortam devlet geleneğinde iç güvenliğin önemini arttırmıştır. Emniyet Genel Müdürlüğü’nün Kurtuluş Savaşı sonrasında oluşturulan ilk yapılardan olması ve 1920 yılında kurulması da bunun bir göstergesidir.⁶⁵³

Emniyet Genel Müdürlüğü oluşturulduktan sonra iç güvenliğin merkezi bir yapı altında örgütlenmesine yönelik önemli adımlar atılmıştır. Günümüz polis teşkilatı yapısı ve faaliyetlerini oluşturmak üzere 04 Temmuz 1934 tarihinde 2559 sayılı Polis Vazife ve Selahiyetleri Hakkındaki Kanun (PVSK) ve 4 Haziran 1937 tarihinde 3201 sayılı Emniyet Teşkilatı Kanunu (ETK) çıkarılmıştır.⁶⁵⁴ Bu kanunun 1. maddesinde, ülkenin genel güvenliğinden ve asayişinden İçişleri Bakanı sorumlu tutulmuş ve İçişleri Bakanının bu işleri kendi yasalarına göre hareket eden Emniyet Genel Müdürlüğü ile Jandarma Genel Komutanlığı ve gerektiğinde diğer bütün zabıta teşkilatları aracılığıyla yerine getireceği ve gerekli görüldüğünde de Bakanlar Kurulu kararıyla silahlı kuvvetlerden de yararlanabileceği hükmü getirilmiştir. Ayrıca Polis Teşkilatı’nın resmi adının Emniyet Genel Müdürlüğü olduğu ve İçişleri Bakanı’na bağlı olduğu da bu kanunda netleştirilmiştir.

Emniyet Genel Müdürlüğü’nün kuruluşundan 1980’lere kadar olan süreçte gerek modern devletin müdahaleciliği gerekse ülke içinde yaşanan iç çekişmeler iç güvenlikle geleneksel devletten kalma baskı ile birleşerek polislik anlayışı ve yapılanması yurttaş hakkında aşırı şüphecilik üzerinde evrilmiştir. Bunun neticesinde Emniyet Teşkilatı yapılanmasının şekillenmesinde istihbari faaliyetler önem kazanmıştır. Bu nedenle 1937 yılında istihbari faaliyetlerde bulunmak üzere kurulan ve taşra birimi olmayan “Önemli İşler Müdürlüğü”, 1951 yılında doğrudan Emniyet Genel Müdürüne bağlı çeşitli illerde de uzantısı

⁶⁵¹ Jacques Gleizal, vd., *Batı Demokrasilerinde Polis*, Çev. Mustafa Kandemir, Temiz Yayınları, Ankara 2000, s.IX.

⁶⁵² a.k

⁶⁵³ Evren Haspolat, *a.g.k.*, s.168.

⁶⁵⁴ a.k

birimleri olan “Özel Büro” şeklinde örgütlenmiştir. 1971 yılında da daire başkanlığı şeklinde örgütlenerek “Önemli İşler Dairesi Başkanlığı”na dönüşmüştür.⁶⁵⁵

1980 sonrasında neoliberalizmin etkileri Emniyet Teşkilatı’nda da görülmeye başlanmıştır. Neoliberalizm ile birlikte devlet görünürde müdahale rejimi açısından küçülme eğiliminde olduğu ve bu noktada pek çok görevi piyasalaştırmak ve özelleştirmek suretiyle yükümlülüğü olmaktan çıkarmış gibi görünse de müdahalenin yerini daha çok denetim almıştır. Devletin denetim faaliyetlerini gerçekleştirmek ve piyasalaştırdığı görevlerin ortaya çıkardığı tehlikeler ile toplumsal düzensizliği kontrol altında tutmak için Emniyet Teşkilatı’na daha çok ihtiyaç duyar hale gelmiştir. Bunun da bir neticesi olarak gerek örgütsel yapı gerek maddi kaynaklar açısından Teşkilat güçlendirilmiştir.⁶⁵⁶ Bu neoliberal etkinin bir sonucu olarak 1989 yılında ETK’da yapılan değişiklikle Emniyet Teşkilatı’nın örgütlenmesinde değişime gidilmiş ve günümüzdeki yapıya kavuşturulmuştur. Bu yapı merkez, taşra ve yurtdışı teşkilatları olmak üzere üç ayak üzerine oturtulmuştur. Merkez teşkilatı; bir Genel Müdür, beş Genel Müdür Yardımcısı, otuz yedi Daire Başkanlığı, Araştırma Merkezi Müdürlüğü, Basın ve Halkla İlişkiler Müdürlüğünden oluşmaktadır.⁶⁵⁷ Taşra teşkilatı; illerde il emniyet müdürlükleri, ilçelerde ilçe emniyet müdürlükleri veya ilçe emniyet amirlikleri şeklinde örgütlenmiştir.⁶⁵⁸ Yurtdışı teşkilatı; yirmi beş kişilik müşavir ve ateşeden oluşmaktadır.⁶⁵⁹

⁶⁵⁵ www.egmidb.gov.tr, (Erişim Tarihi: 18.09.2013).

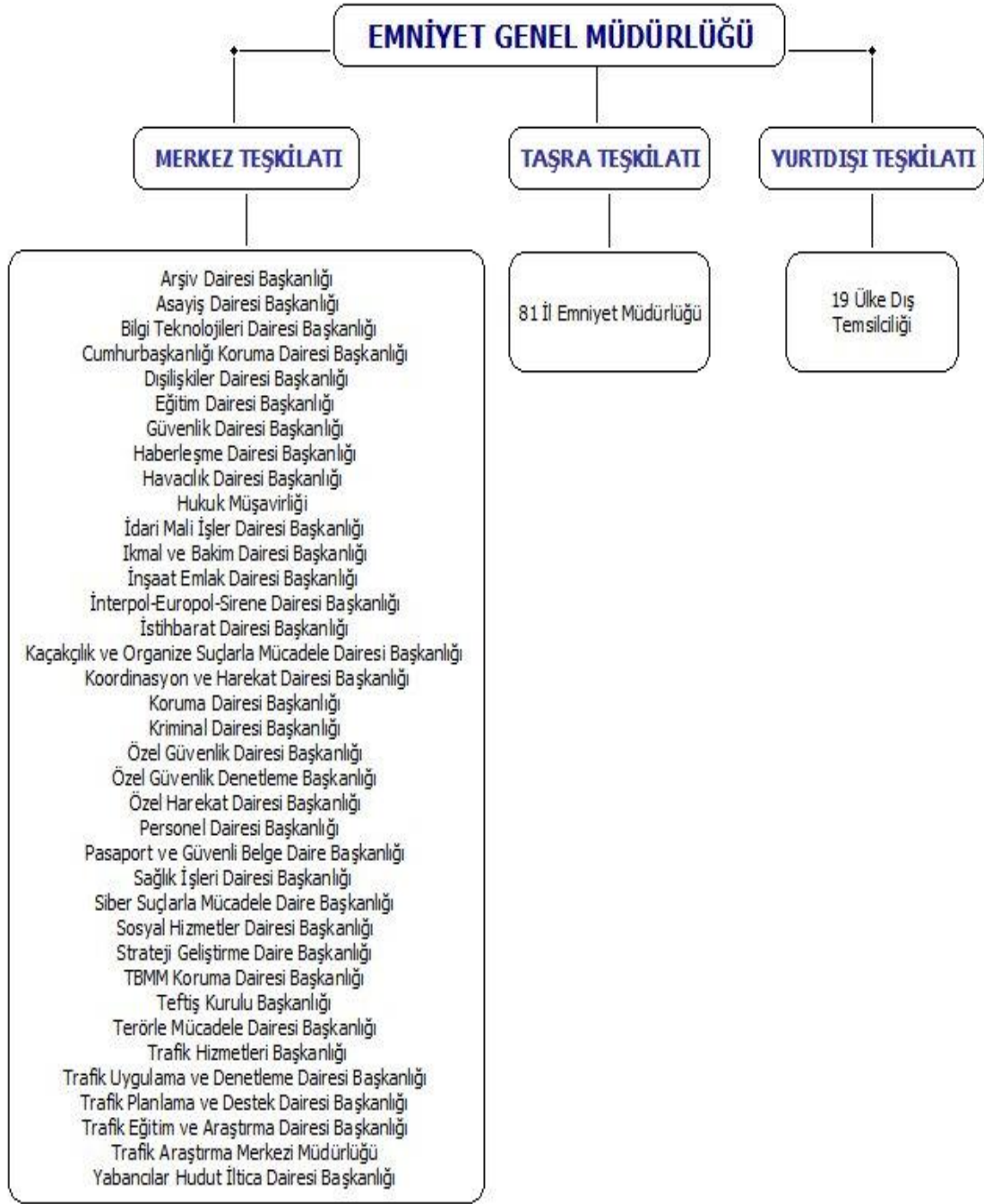
⁶⁵⁶ *a.k.*, s.94 - 95.

⁶⁵⁷ www.egm.gov.tr, (Erişim Tarihi: 18.09.2013).

⁶⁵⁸ 3201 Sayılı Emniyet Teşkilatı Kanunu, Madde 16/B.

⁶⁵⁹ Yılmaz Yaşar, *Polis Meslek Hukuku*, Mustafa Kitabevi, Ankara, 2007, s.120.

Şekil-2.Emniyet Genel Müdürlüğü'nün Örgütsel Yapısı



Kaynak: <http://www.egm.gov.tr>

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler paralelinde içine girilen bilgi toplumu sürecinden Emniyet Teşkilatı da etkilenmiştir. Bu kapsamda gerek bilgi toplumundan kaynaklanan toplumsal beklentileri karşılamak gerek bu teknolojileri kullanan toplumu kontrol altında tutabilmek için örgütsel yapısında yeni birimlere ihtiyaç hasıl olmuştur. Toplumsal sapmaların ve suçların internet gibi bilgi ve iletişim araçları üzerinden gerçekleşebilir hale gelmesi, sınırı gözükmeyen bu alanların kontrol altına alınması

gerekliliğini doğurmuştur. Diğer taraftan bu teknolojiler nedeniyle iktidarın varlığını idame ettirmek için bir gereklilik olan bilgiye hakim olmanın önemi de daha çok artmıştır. Bu nedenle iktidarın bir aygıtı olarak Emniyet Teşkilatı bilgi toplama ve toplanan bu bilgileri güvenlik süzgecinden geçirme ve kategorize etme gibi bir görevle karşı karşıya kalmıştır. Sonuçta Emniyet Teşkilatı'nda bilgi toplumunun örgütsel yapıdaki etkisi bazı daire başkanlıklarının görev stratejisini buna göre değiştirmesi ve yeni daire başkanlıklarının kurulması şeklinde olmuştur. Emniyet Teşkilatı'nda bilgi - iletişim ve gözetim teknolojilerine öncülük eden altyapı, teknik ve teorik çalışmalar Bilgi Teknolojileri Dairesi Başkanlığı tarafından yürütülmektedir. Ayrıca bilişim teknolojileri kullanılarak gerçekleştirilen suçların hızla artış göstermesiyle birlikte Kaçakçılık ve Organize Suçlarla Mücadele Dairesi Başkanlığı bünyesinde bir şube müdürlüğü iken 2011 yılında Daire Başkanlığı şeklinde örgütlenmiş olan Siber Suçlarla Mücadele Dairesi Başkanlığı da bu alanda önemli faaliyetlerde bulunmaktadır.

Bilgi Teknolojileri Dairesi Başkanlığı Emniyet Teşkilatı'ndaki teknolojik değişim ve dönüşümün ana sorumlusudur. Polnet, Mobese, Asbis gibi birçok projeyi gerçekleştirmiştir. Mevcut durumda da çok sayıda hazırlık aşamasında olan e-devlet projeleri bulunmaktadır. Bu daire başkanlığı bünyesinde Yazılım, Sistem, Bilişim Güvenliği, Strateji, Proje Takip, Web Teknolojileri, Eğitim, İnsan Kaynakları Şube Müdürlükleri bulunmaktadır.⁶⁶⁰

Siber Suçlarla Mücadele Dairesi Başkanlığı, bilişim teknolojileri kullanılarak işlenen suçların soruşturulması ve dijital delillerin incelenmesi için destek veren görevli daire başkanlıklarının ve taşra teşkilatındaki birimlerin dağınık yapısının tek bir çatı altında toplanmasını, mükerrer yatırımların önüne geçilmesini, bilişim suçlarıyla mücadelenin etkin ve verimli olarak yürütülmesini sağlamak amacıyla 2011/2025 sayılı Bakanlar Kurulu Kararı ile kurulmuştur.⁶⁶¹ Bu birimin 1980'lerdeki neoliberal etkinin günümüzde internet alanında yeniden kendini göstermesinin bir sonucu olduğu değerlendirilmektedir.

Sonuç olarak Emniyet Teşkilatı'nın gelişimi, güvenlik kavramının tarihsel dönüşümüyle paralellik gösterdiği ve her geçen gün bu kavram çevresinde meydana gelen hızlı dönüşümler nedeniyle görev tanımı ve örgütsel yapısında geçmişe oranla daha hızlı değişim görüleceği düşünülmektedir. Bu değişimin yönünün de gözetim teknolojileri ekseninde olacağı tahmin edilmektedir. Orta ve uzun vadede meydana gelebileceği düşünülen bu değişimlerin geçmişe göre çok daha etkili olacağı ve daha çok yurttaşı ilgilendireceği

⁶⁶⁰ www.egm.gov.tr, (Erişim Tarihi:18.09.2013).

⁶⁶¹ a.k

analiz edilmektedir. Nitekim 1923 yılında 4 bin 250 personelle polisin hizmet götürdüğü alandaki yurttaş sayısı 2 milyon 700 bin kişi⁶⁶² iken bugün 300 bin civarında personelle 50 milyona yakın yurttaşla hizmet götürmektedir.⁶⁶³

2. Emniyet Teşkilatı'nda Bilgi ve İletişim Teknolojileri

Kamu hizmetlerinin yerine getirilmesinde bilgi ve iletişim teknolojilerinin etkin bir şekilde kullanılmaya başlanmasında başat rol oynayan kurumlardan birisinin Emniyet Teşkilatı olduğu önceki bölümlerde vurgulanmıştı. Bu rolün bir sonucu olarak Teşkilat, yeni kurulan veya görev ve işleyiş bakımından bilgi toplumu şartlarında dönüşen birimlerle örgütsel tekamülünü gerçekleştirmiştir. Gerek genişleyen kapasitesiyle bu örgütsel yapıya zemin hazırlaması gerek bu örgütsel yapının bir sonucu olarak birçok bilgi ve iletişim teknolojisi ile donatılmıştır. Teknolojik gelişmelerin ana hattı Polnet sistemi üzerinde oluşturulmuştur. Tüm Teşkilat bilgi ve iletişim teknolojisi bir şekilde bu sistem ile ilişkilidir. Polnet ile ilişkili olmakla birlikte kapasite ve etki olarak Polnet kadar önemli sayılabilecek olan Mobese projesi de bilgi ve iletişim teknoloji çevresinde yer almıştır. Polnet ve Mobese ile ilişkili olmakla birlikte farklı özellikleri olan kendi alanında önemli gizli istihbari projelerin de varlığı bilinmektedir. Emniyet Teşkilatı'nda ifade edilen teknolojik gelişimin gözetime evrilmesini açıklayabilmek için bu bölümde Polnet ve Mobese projeleri anlatılmaya çalışılacaktır.

2.1. Polnet

Emniyet Teşkilatı'nın temel bilgi ve iletişim sistemi "Polnet"tir. Kelime açılımı polis bilgisayar ağını ifade eden "Polis Network"tur. Polnetin neyi ifade ettiği ve kurulum amacı kendi resmi intranet sayfasında şöyle açıklanmıştır:⁶⁶⁴

"Polisin görevinin gerekli kıldığı her türden bilgiye, en hızlı, kolay ve güvenilir bilgi sistemlerini kullanarak ulaşmasını sağlayacak ve ulusal ve uluslararası tüm bilgi ağları ve bilgi bankalarına entegre olabilecek; yeni teknolojilere tamamen açık bilgisayar ve iletişim altyapısı üzerinde tüm teşkilatın bilgi otomasyonunu ve ortak veritabanı kullanımını içeren modern bir bilgi sistemidir.

Emniyet Teşkilatı'nın farklı birimlerince ayrı ayrı kurulması düşünülen görüntü, ses, parmak izi, Kriminal Polis Laboratuvarları uygulamaları ve data iletişim ağlarının müstakil, güvenli ve sağlam bir omurga halinde tek bir polis iletişim altyapısı üzerinde kurularak maliyet, yönetim ve kapasite yönünden tasarruf sağlanmasıdır."

Emniyet Teşkilatı personeli kurumsal olarak bütün resmi faaliyetlerini bu sistem üzerinden gerçekleştirmektedir. Neticede sistemin ülkedeki polis sayısı kadar kullanıcısı var

⁶⁶² Emrah Gürkan, *Ne Kadar Muasırlaşabildik? 80. yılında Cumhuriyet*, Güncel Kitaplar Yayınevi, Ankara, 2003, s.131.

⁶⁶³ <http://www.egm.gov.tr/default.asp>, (Erişim Tarihi:18.09.2013).

⁶⁶⁴ Polnet, (Erişim Tarihi:18.09.2013).

denilse yanlış olmaz. Emniyet Teşkilatı'nın adli işlemler başat olmak üzere resmi işlem görev yoğunluğu ile personel sayısının fazlalığı birleşince sistemin oldukça çok kişi tarafından aktif bir şekilde kullanıldığı ifade edilebilir. Nitekim ülke çapında 2 bin 647 farklı Emniyet Teşkilatı biriminde kullanılan ve 250 bin kullanıcıya sahip olan büyük bir intranet ağıdır.⁶⁶⁵ Bu bağlamda gerek ulusal ölçekte kurumsal örgütlenme anlamında gerek sahip olduğu alt programların büyüklüğü bakımından ülkemizde Uyap gibi önde gelen bilişim altyapılarından.

Polnetin kuruluşu, geliştirilmesi ve günümüzdeki haline ulaşması sürecini incelediğimizde yaklaşık on beş yıllık bir geçmişinin olduğunu görürüz. Daha önceki bölümlerde ifade edilen ülkemizin e-devlet sürecinde başat rol oynayan Mernis, Uyap gibi projeler Polnet ile karşılaştırıldığında hepsinin özellikle günümüzdeki altyapılarının 2000'li yılların başlarında birbirlerine paralel bir şekilde oluşturulduğu söylenebilir. Burada özellikle çalışma boyunca bilgi ve iletişim teknolojileri olarak ifade edilen yeni nesil iletişim teknolojilerinin Türkiye'ye ithal edilmesinin de aynı tarihlerde olması dikkat çekicidir. Zira bu durum hem Polnetin hem diğer projelerin günümüzde kullanılan teknoloji altyapılarının yurt dışı kaynaklı olduğunu da açıklamaktadır.

Polnetin kurulum çalışmalarına “*mainframe*” kapalı sistem altyapılı olarak 1997 yılında başlanmıştır. Sahip olduğu bu kapalı sistem altyapısı nedeniyle Polnet, bu dönemde alt projelerin birbiriyle uyumlu ve entegre olamadığı, teknolojik gelişmelere kapalı olan ve yeni nesil uygulamalara adapte olamayan basit bir sistem olmuştur. Ayrıca çalıştığı süre zarfında oldukça yüksek maliyetli olarak maksimum 2500 sabit kullanıcıya hizmet verdiği bilinmektedir. Bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte “*mainframe*” olarak ifade edilen kapalı sistemler yerini kapasitesi geniş, hızlı, işletim ve kullanım kolaylıkları getiren, başka bilgisayarlar ile entegrasyon kabiliyeti olan, yüksek performanslı, düşük maliyetli, yeniliklere tümüyle açık dijital bilgisayar tabanlı daha küçük açık sistemlere bırakmıştır. Bu duruma Emniyet Teşkilatı da uyum sağlamış ve 2001 yılı sonuna doğru kapalı sistemler tamamen terk edilerek dijital bilgisayar tabanlı açık sistemlere geçilmiştir. 2002 yılının Ocak ayından itibaren sistem bu şekilde kullanılmaya ve geliştirilmeye başlanmıştır.

⁶⁶⁵ Polnet, 1 Merkez, 81 İl Emniyet Müdürlüğü, 874 İlçe Emniyet Müdürlüğü/Amirliği, 939 Merkez/Taşra Ek Hizmet Binası, 543 Karakol/Polis Merkezi, 126 Hudut Kapısı, 41 Polis Evi/Polis Moral Eğitim Merkezi Müdürlüğü, 42 Polis Meslek Yüksek Okulu ve 59 Dış Bağlantı noktasından olmak üzere toplamda 2647 lokasyonda kullanılmaktadır. 10 - 11.10.2013 Tarihlerinde Bilgi Teknolojileri Dairesi Başkanlığı ve Haberleşme Dairesi Başkanlığı'nda Üç Personel ile Yapılan Derinlemesine Görüşme.

2005 yılında iletişim altyapısına yeni güvenlik tedbirleri içeren eklemeler yapılmıştır.⁶⁶⁶ Dolayısıyla günümüzde kullanılan Polnetin, bu dijital bilgisayar tabanlı açık sistemlere geçişin Emniyet Teşkilatı'ndaki sonucu olduğu ifade edilebilir. Dijital bilgisayar tabanlı olarak çalışan günümüz Polnet sisteminde tüm projeler ortak bir veritabanında yer almaktadır. Bu veritabanı görüntü, ses, parmakizi gibi teknolojik gelişmelere açık olmakla birlikte çeşitli bilişim projeleriyle ortak standartlara ve kod tablolarına sahiptir. Bu kapsamda mevcut durumda sistemin sınırsız kullanıcıya hizmet verebilen düşük maliyetli bir yapısı olduğu ifade edilebilir.⁶⁶⁷

Polnetin önemli bir özelliği ve diğer e-devlet uygulamalarından ayrılan tarafı AB destekli fonlar gibi herhangi bir dış kaynak veya destek alınmadan gerçekleştirilmiş olmasıdır. Projenin oluşması ve aktifleşmesi sürecinde personel olarak teknik şartnamelerin hazırlanması, tasarım, muayene ve kabul işlemleri Bilgi İşlem, İstihbarat, Haberleşme ve Asayiş Dairesi Başkanlıklarının rütbeli teknik personeli tarafından gerçekleştirilmiştir. Ayrıca tasarım ve mühendislik için dışarıdan danışmanlık alınmamıştır. Projenin finansmanı ise Emniyet Teşkilatı'nın kendi bütçesi ve Polis Teşkilatı Güçlendirme Vakfı'ndan karşılanmıştır.⁶⁶⁸

Teknolojik gelişmeler paralelinde Polnete farklı şekillerde erişmek mümkün hale gelmiştir. Halihazırda sisteme hem karasal hatlarla hem de uydu yedekleme sistemi ile ulaşılabilmekte, mobil terminaller vasıtasıyla gerekli sorgulamalar ve veri girişleri yapılabilmektedir.⁶⁶⁹ Bir intranet ağı için kullanıcı sayısının oldukça fazla oluşu, farklı teknolojik altyapılarla sisteme ulaşabilme imkanı ile içerdiği verilerin hassasiyeti birleşince sistemin güvenliği en önemli soruna dönüşmektedir. Zira Polnet içinde hem yurttaşların özel hayatlarına ilişkin olan, başkalarının görmemesi gereken veriler olmakla birlikte hem de ulusal güvenlik açısından önem arz eden veriler yer almaktadır. Bu verilerin bir şekilde çalınması, üçüncü şahısların eline geçmesi kurumsal anlamda ve yurttaş açısından büyük bir tehdittir. Bu tehdit algısında Polnetin güvenliğini sağlamaya yönelik birçok güvenlik tedbiri alınmıştır.⁶⁷⁰ Sistemde her personelin kullanıcı profili ile şifresi vardır ve güvenlik açısından

⁶⁶⁶ Ahmet Kocabal, "Polnet ve Transpol", http://www.caginpolicisi.com.tr/v1/yazdir.php?art_id=691, (Erişim Tarihi 12.06.2013).

⁶⁶⁷ Polnet, (Erişim Tarihi 18.09.2013).

⁶⁶⁸ 10 - 11.10.2013 Tarihlerinde Bilgi Teknolojileri Dairesi Başkanlığı ve Haberleşme Dairesi Başkanlığı'nda Üç Personel ile Yapılan Derinlemesine Görüşme.

⁶⁶⁹ a.k

⁶⁷⁰ Polnet kapalı devre (bilgi gizliliği sağlayan devre) sistemi üzerine kurulmuştur. Polnet iletişim altyapısının genel olarak topolojisine bakıldığında, Bilgi Teknolojileri ve Haberleşme Dairesi Başkanlıklarının kurulu bulunduğu Dikmen Ek Hizmet Binasının Bilgi ve İletişim Teknolojileri Merkezi olarak konumlandırıldığı, İl Emniyet Müdürlüklerine bağlı birimlerin öncelikle İl Emniyet Müdürlüğüne ve İl Emniyet Müdürlüklerinin de

kullanıcı seviyeleri belirlenmiştir. Buna göre bazı kullanıcılar sadece okuyabilir, bazı kullanıcılar sadece yazabilir, bazı kullanıcılar da her ikisini yapabilir. Her kullanıcı her bölüme giremez ve kullanıcıların işlemleri kayıt altına alınarak takip edilir; usulsüz uygulamaların hangi personel tarafından yapıldığı tespit edilerek gerekli soruşturma açılır.⁶⁷¹

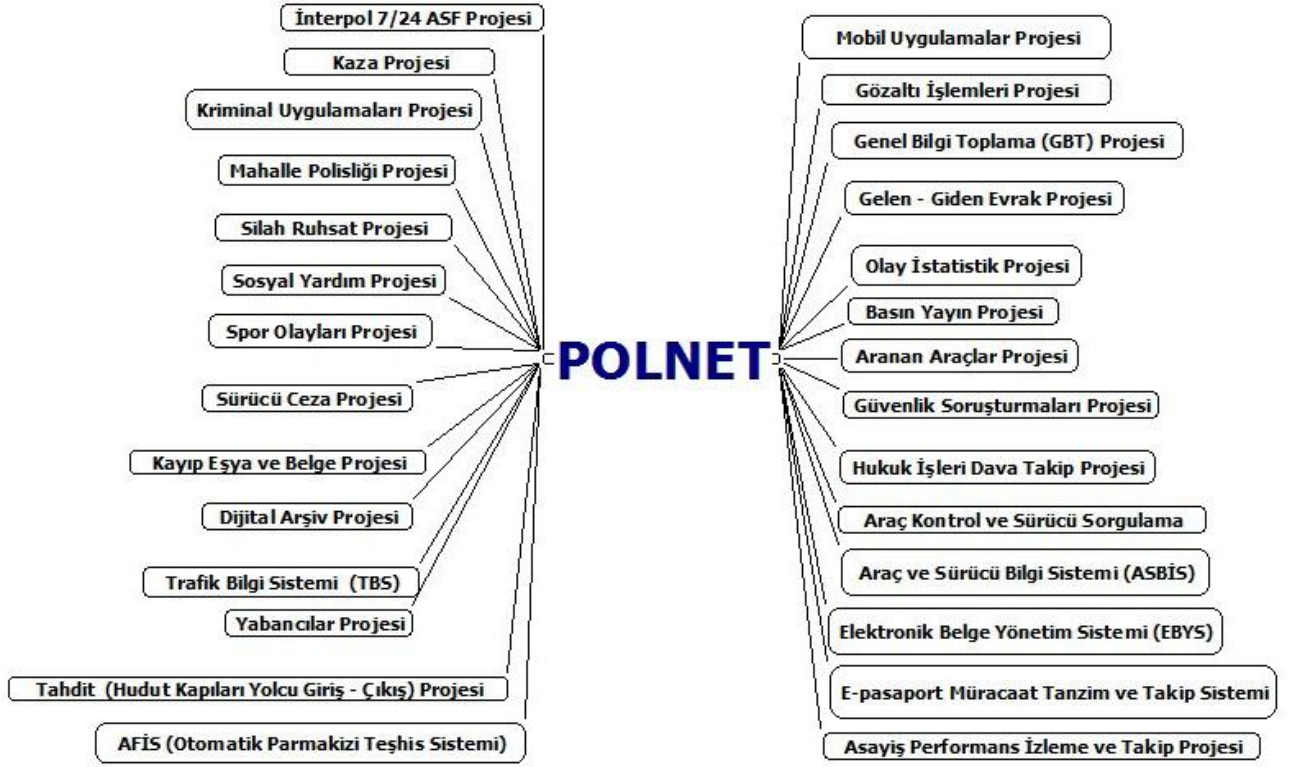
Polnet ilk çıktığı zamanlarda veri transferi amaçlı olarak basit bir şekilde kullanılırken, günümüzdeki haliyle yaklaşık 150 civarında farklı projeyi içeren büyük bir yapıya dönüşmüştür.⁶⁷² Bu yapı içinde Polnet üyesi herkesin ulaşabileceği bazı projeler yer alırken, birimlere özel olanlar da bulunmaktadır. Polnet yapısını anlama açısından bu projelerden önemli olanlar aşağıda şematize edilmiştir. Ayrıca bu projelere ilişkin açıklamalı çizelge de Ek-3'de bulunmaktadır.

Bilgi ve İletişim Teknolojileri Merkezine bağlandığı görülmektedir. Aynı şekilde Merkez yerleşkeler (Daire Başkanlıkları ve Merkez Ek Hizmet Yerleşkeleri) de doğrudan İletişim Merkezine bağlanmaktadır. İl Emniyet Müdürlüklerine bağlı birimler (Şube Müdürlükleri, İlçe Emniyet Müdürlükleri, Ek Hizmet Binaları, Polis Merkezleri-Karakollar, Kara, Deniz, Hava ve Demiryolu hudut kapıları) İl Emniyet Müdürlüğü iletişim merkezine Türk Telekom A.Ş.'den kiralanan noktadan noktaya L2 (OSI Layer 2) hatlar vasıtasıyla bağlanmaktadır. İl Emniyet Müdürlüklerine bağlı birimlerin İl Emniyet Müdürlüğü ile olan veri iletişimi IPSec VPN teknolojisi kullanılarak şifrelenmektedir. Ancak özellikle kritik data trafiği İl Emniyet Müdürlükleri Ana Hizmet Binası ile Emniyet Genel Müdürlüğü arasında akmakta olduğundan burada L2 şifreleme yöntemleri kullanılmaktadır. İletişim cihazlarına erişim ile ilgili katı yönetim kuralları uygulanmakta ve bu konuda ITIL ve ISO 27001 gibi uluslararası standartlara uygun süreç yönetimi yapılmaktadır. Bilgilerin tutulduğu sunucu sistemlere kullanıcılar tarafından direkt erişim sağlanmamakta, DMZ bölgesi içerisindeki proxy IP'lere erişim sağlanmakta ve erişimlere port sınırlaması konmaktadır. Proxy NAT gibi güvenlik yöntemleri kullanılarak kullanıcıların sunucu sistemlere direkt erişimleri engellenmekte ve erişim logları kayıt altına alınmaktadır. Kullanıcı bilgisayarlarının merkezden yönetimini ve güvenliğini sağlamak amacıyla Microsoft firmasının aktif dizin uygulaması kullanılmakta ve IPSec NAP teknolojisi uygulanmaktadır. Sunucu sistemleri ile ilgili fiziksel güvenlik politikalarının yanısıra, erişim politikaları ile de güvenlik seviyesi arttırılmaya çalışılmaktadır. Tüm bunlarla beraber uygulama seviyesinde kullanıcıların yaptıkları bütün işlemler kayıt altına alınmakta, bilgiler disk ortamında şifrelenerek saklanmaktadır. 10 - 11.10.2013 Tarihlerinde Bilgi Teknolojileri Dairesi Başkanlığı ve Haberleşme Dairesi Başkanlığı'nda Üç Personel ile Yapılan Derinlemesine Görüşme.

⁶⁷¹ Ahmet Kocabal, "Polnet ve Emniyet Bilgi Sistemi", <http://www.cagipolisi.com.tr/26/16-17-18-19.htm>, (Erişim Tarihi: 05.06.2013).

⁶⁷² 10 - 11.10.2013 Tarihlerinde Bilgi Teknolojileri Dairesi Başkanlığı ve Haberleşme Dairesi Başkanlığı'nda Üç Personel ile Yapılan Derinlemesine Görüşme.

Şekil-3. Polnet İletişim Altyapısı ve Üzerinde Çalışan Projeler



Kaynak: 10-11.10.2013 Tarihlerinde Bilgi Teknolojileri Dairesi Başkanlığı ve Haberleşme Dairesi Başkanlığı'nda Üç Personel ile Yapılan Derinlemesine Görüşme Sonrasında Oluşturulmuştur. Ayrıntılı Bilgi İçin Ek-3'e Bakınız.

Gözetime bakan yönüyle yukarıdaki projelerden bazılarının ön plana çıktığı görülmektedir. Özellikle Otomatik Parmakizi Teşhis (Afis), Hudut Kapıları Giriş - Çıkış (Tahdit), Genel Bilgi Toplama Projesi (GBT), Araç ve Sürücü Bilgi Sistemi (Asbis), E-Pasaport Müracaat Tanzim ve Takip Sistemi, Kriminal Uygulamaları ve Sürücü Ceza Sistemi projeleri ile yurttaşa yönelik çeşitli veriler toplanıp, depolanmakta ve sorguya açılmaktadır. Örneğin bireyin yurt dışına giriş - çıkış tarihleri, parmak izi gibi biometrik verileri, fotoğraf kayıtları, araç - pasaport bilgileri, silah kayıtları gibi birçok veri sisteme kaydedilebilmektedir. Kurum personelinin gözetimine bakan yönüyle tüm Polnet projeleri gösterilebilir. Zira bütün projelerde personel işlem kayıtları (*log* kayıtları) tutulmakta ve değerlendirilmektedir. Ayrıca Asayiş Performans İzleme ve Takip Projesi gibi doğrudan personelin günlük faaliyetlerini takip etmeye yönelik çeşitli projeler de bulunmaktadır.

Polnet sisteminin yukarıda belirtilen projeler haricinde diğer devlet kurum ve kuruluşları ile arasında dijital veri transferinin düzenlenebildiği bir yapı bulunmaktadır. E-devlet uygulamaları kapsamında Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü (Mernis),

Milli İstihbarat Teşkilatı gibi farklı kurum ve kuruluşların bilgi sistemleri ile elektronik olarak çevrimiçi anlık veri alışverişini sağlayan dış bağlantı servisleri bulunmaktadır.⁶⁷³

Çalışmanın birinci bölümünde e-devlet anlatılırken ifade edildiği üzere kamu hizmetlerinin dijitalleşmesine yönelik olan projelerin bürokrasinin azalması, veriye hızlı erişim gibi sağladığı bir takım imkan ve kolaylıklar bulunmaktadır. Bu durumun Polnet için de geçerli olduğu ifade edilebilir. Polnet doğrultusunda bu imkan ve kolaylıklar göreve, personele ve yurttaşla yönelik olmak üzere üç başlık altında incelenebilir. Göreve yönelik birinci olarak kurum içi kırtasiyeciliğin ortadan kalkması örnek gösterilebilir. Mevcut durumda kurum içi evrak sirkülasyonunda geleneksel yöntemler terk edilip elektronik onay ve e-posta yöntemi kullanılmaya başlanmıştır. Böylece hem kağıt, kalem vs. gibi kırtasiye malzemelerinin harcamasında ciddi azalmalar olmuş, hem de evrakların kurumlararası irtibatını sağlayan personelin zaman, yakıt vs. kaybı engellenmiş ve büyük oranda tasarruf sağlanmıştır. Mesela 2004 yılında posta pulu maliyetinden 147 milyar TL, faks ve teleks maliyetlerinden ise 3 trilyon 316 milyar TL olmak üzere toplam 3 trilyon 463 milyar lira tasarruf sağlanmıştır.⁶⁷⁴ İkinci olarak Polnet üzerinde her birimin kendine ait web sitesinin bulunması ve bütün birimlerin buralarda ilan ve duyuru verebilmesi, mesleki raporlarını buralarda yayımlayabilmesinin sağladığı hızlı erişim ve şeffaflık gösterilebilir.⁶⁷⁵

Üçüncü olarak sistem sayesinde hızlı ve kompleks istatistikler çıkarma kolaylığı ifade edilebilir. Nitekim kamu kurumlarında en çok uğraş gerektiren ve zaman alan uygulamalardan birisi çeşitli kategorilerde istatistik çıkarma işlemidir.⁶⁷⁶ Veriler sistem üzerinde belli bir düzen içinde kategorize edilebildiğinden dolayı istatistik almak oldukça hızlı ve kolaydır. Ayrıca istatistik alma ihtiyaç paralelinde farklı kriterlere göre de yapılabilmektedir. Bu bağlamda tarih, olay, şahıs, eşya, yer ya da daha geniş, çapraz boyutlarda birden fazla değer karşılaştırılarak istatistikler çıkarılıp, analizler yapılabilmektedir.

Dördüncüsü parmak izi, balistik karşılaştırmalar, DNA analizleri, kan ve doku tahlilleri gibi gelişmiş laboratuvar ve uzmanlık gerektiren kriminalistik verilerin Polnet

⁶⁷³ Polnetin dış bağlantı servisi kurduğu kamu kurum ve kuruluşlar şöyledir: Jandarma Genel Komutanlığı, Ulaştırma Bakanlığı Karayolları Ulaştırma Genel Müdürlüğü, PTT Genel Müdürlüğü, Maliye Bakanlığı Gelir İdaresi Başkanlığı, Milli Savunma Bakanlığı Seferberlik Dairesi Başkanlığı, Sosyal Güvenlik Kurumu, TRAMER (Sigorta Bilgi Merkezi), TÜV-TURK, Dışişleri Bakanlığı, Gümrük Müsteşarlığı, Adalet Bakanlığı, Milli Eğitim Bakanlığı, İnterpol Genel Merkezi (Fransa-Lyon), Europol Genel Merkezi (Hollanda), , Bankalar Birliği, Türkiye Noterler Birliği, Sanayi ve Ticaret Bakanlığı, Türk Standartları Enstitüsü. Polnet, (Erişim Tarihi:03.10.2013).

⁶⁷⁴ <http://www.memurlar.net/haber/15517/>, (Erişim Tarihi: 05.06.2013).

⁶⁷⁵ <http://www.egm.gov.tr/egitim/index-17.html>, (Erişim Tarihi: 05.06.2013).

⁶⁷⁶ Ahmet Kocabal, "Cumhuriyet, Türk Polisi ve Bilgi İşlem", <http://www.caginpulisi.com.tr/26/16-17-18-19.htm>, (Erişim Tarihi: 05.06.2013).

iletiřim altyapısı üzerinden Trkiye'deki tm kriminal uzmanlara anında ulařtırılabilmesidir.⁶⁷⁷ Bu kapsamda acil kodlu istihbarat raporları ve analizleri hedef birime anında aktarılabilir. Mesleki aıdan bu řekilde soruřturmaya ynelik verilerin bir ilden bařka bir ile veya merkez birime aktarılabilmesinin saėladıėı birok avantaj bulunmaktadır.

Personele bakan ynyle sistemin en byk avantajı mesleėin niteliėinden kaynaklanan veriye hızlı eriřimin saėlanabilmesidir. Bu řekilde personel zerinde amirlerin psikolojik taciz (*ing; mobbing*) etkisinin bir anlamda azalıėı sylenebilir. Zira Emniyet Teřkilatı'na ihbar geldiėinde, herhangi bir olay olduėunda kendisine ihbar ulařan veya olaya ilk mdahale eden personelden ncelikle hakkında ihbar gelen veya olaya karıřan řahıřlarla ilgili su gemiři, aranıp aranmama durumu gibi temel bilgilere hızlı bir řekilde ulařması beklenmektedir. Sistem sayesinde personel bu verilere 3-5 saniye iinde ulařabilmekte ve amirlerinin baskısından kurtulabilmektedir. Ayrıca psikolojik taciz etkisinden kurtulmanın yanı sıra personel greviyle ilgili bilgilere anında ulařabildiėinden dolayı bunlara ayıracaėı zamanı hizmetin kalitesine ayırdıėı iin kiřiisel iř tatminini de arttırdıėı iddia edilebilir. Polnet sayesinde personel stleriyle veya iřle ilgili řikayetlerini merkeze iletebildiėi gibi tayin durumlarını, maař, taltif, ikramiye gibi mali konularını, yıllık hiyerarřık sıralamalarını buradan takip edebilmektedir. Diėer taraftan aılan kurs, yurtdıřı grevlendirme sınavlarıyla ilgili bilgilere tm personel aynı zamanda ulařabilmektedir.

Polnetin genel kabul grmesinde sistemin yurttařa dnk ynyle saėladıėı imkan ve avantajlar da nem arz etmektedir. Yurttařa ait sicil, arama kaydı gibi bilgiler Polnet iletiřim altyapısında olan Genel Bilgi Toplama (GBT) sistemi vasıtasıyla ok kısa zamanda ėrenilebildiėinden dolayı gzaltı sreleri kısalımıř ve gereksiz gzaltında tutma olayları ortadan kalkmıřtır. İnternette başvuru yapılabilmesi ve kiřiilere ait bilgilere veritabanından ulařılabilmesi nedeniyle pasaport, ara tescil, src belgesi, silah ruhsat iřlemleri brokrasiden arındırılmıř ve hızlı bir řekilde gerekleřtirilmektedir. Ayrıca bu veritabanı sayesinde hudut kapılarında bekleme sresi de azaltılmıřtır.⁶⁷⁸ Trafik denetimlerinde araları plakadan anında sorgulama imkanı sayesinde trafik denetimleri daha hızlı ve daha ok ara zerinde yapılabilir.⁶⁷⁹ Trafik denetimleri neticesinde verilen trafik ceza puanları yurttařlar tarafından internet zerinden ėrenilebilir hale getirilmiřtir. Polis hizmetleri Polnet ile dijitalleřtirildiėinden dolayı hizmeti veren kiřiilerin kltr dzeyinden kaynaklanan

⁶⁷⁷ a.k

⁶⁷⁸ DPT Bilgi Toplumu Dairesi Bařkanlıėı, *a.g.k.*, s.54 - 55 - 56.

⁶⁷⁹ <http://www.hardwarehaber.com/haberbak.php?id=1677>, (Eriřim Tarihi: 06.06.2013).

birimler arası hizmet kalitesi değişikliklerinin en aza indiği, böylece bütün yurttaşlar, her yerden aynı hizmeti aynı hızla ve kalitede alır duruma geldiği iddia edilmektedir.

2.2. Mobese

Mobil Elektronik Sistem Entegrasyon (Mobese), yazılım ve donanım temel bileşenlerinden oluşan, iletişim altyapısı olarak GPRS teknolojisini kullanan, Coğrafi Bilgi Sistemleri ve Bilgi Yönetim Sistemleri ile entegre modern kent bilgi ve güvenlik sistemi olarak tanımlanabilir.⁶⁸⁰ Mobesenin kurulduğu dönemde Bilgi İşlem Dairesi Başkanı olan Ahmet Kocabal Mobese'yi şöyle ifade etmektedir:⁶⁸¹

“Emniyet Genel Müdürlüğü’nün asayişini sağlamak, iç güvenliğe yönelik tehditleri bertaraf etmek ve denetim görevini daha etkin gerçekleştirmek üzere; mevzuata uygun olarak elde edilen görüntü, ses ve konum verilerinin işlenerek anlamlı sonuçlar üretilmesini ve sonuçların Polnet Uygulamaları ile desteklenmesini sağlayan, modüler olarak geliştirilmiş kent güvenlik yönetim bilişim sistemidir.”

Mobese ilk defa İstihbarat Dairesi Başkanlığı tarafından 10 Nisan 2001 tarihinde “Araç Takip ve Suç Analizi Uygulaması” bileşeniyle Diyarbakır’da, sonrasında da en kapsamlı olarak 10 Nisan 2005 tarihinde İstanbul’da uygulanmaya başlanmıştır. Projelerden elde edilen sonuçlar neticesinde 2005 yılında Emniyet Genel Müdürü tarafından Mobese Sisteminin ülke çapında yaygınlaştırılması görevi Bilgi İşlem Daire Başkanlığı’na verilmiştir.⁶⁸² 2005 yılı sonrasında özellikle terör örgütü faaliyetleri kapsamında ülke genelinde araç yakma olaylarının yaşanması, bunları gerçekleştiren bazı failerin Mobese kameralarınca tespit edilmesi ve bu kameraların diğer kamusal olumlu neticeleri çerçevesinde genel olarak faydalı görülmüş ve her yere konulması yönünde kamuoyu desteği oluşmuştur. Hatta Eskişehir ilinde Mobese kurulması için halk tarafından bağış bile toplanmıştır.⁶⁸³ 2014 yılının Şubat ayı itibarıyla Türkiye’de 81 ilde ve 66 ilçede kurulu durumda ve aktif çalışmaktadır.⁶⁸⁴

Mobesenin kendi Polnet intranet ağında amaçları; güvenlik hizmetlerinin verimliliğini arttırmak, güvenlik tehditlerini algılamak, göreve ilişkin koordinasyonu güçlendirmek, kişi hak ve hürriyetlerine dokunulmadan genel asayiş ve huzuru temin edilebilmek olarak ifade

⁶⁸⁰ <http://www.basarsoft.com.tr>, (Erişim Tarihi:07.06.2013).

⁶⁸¹ Egm Bilgi İşlem Daire Başkanı Ahmet Kocabal ile Röportaj, *Konsept*, Meteksan Yayınları, Sayı 9, 2006, s.39.

⁶⁸² Erin Çoban, “Ülkemizin Yeni Bilgi ve Güvenlik Konsepti Mobese”, *Polis Dergisi*, Sayı 43.,http://www.egm.gov.tr/egitim/dergi/eskisayi/45/web/makaleler/Erin_COBAN.htm, (Erişim Tarihi: 22.05.2013).

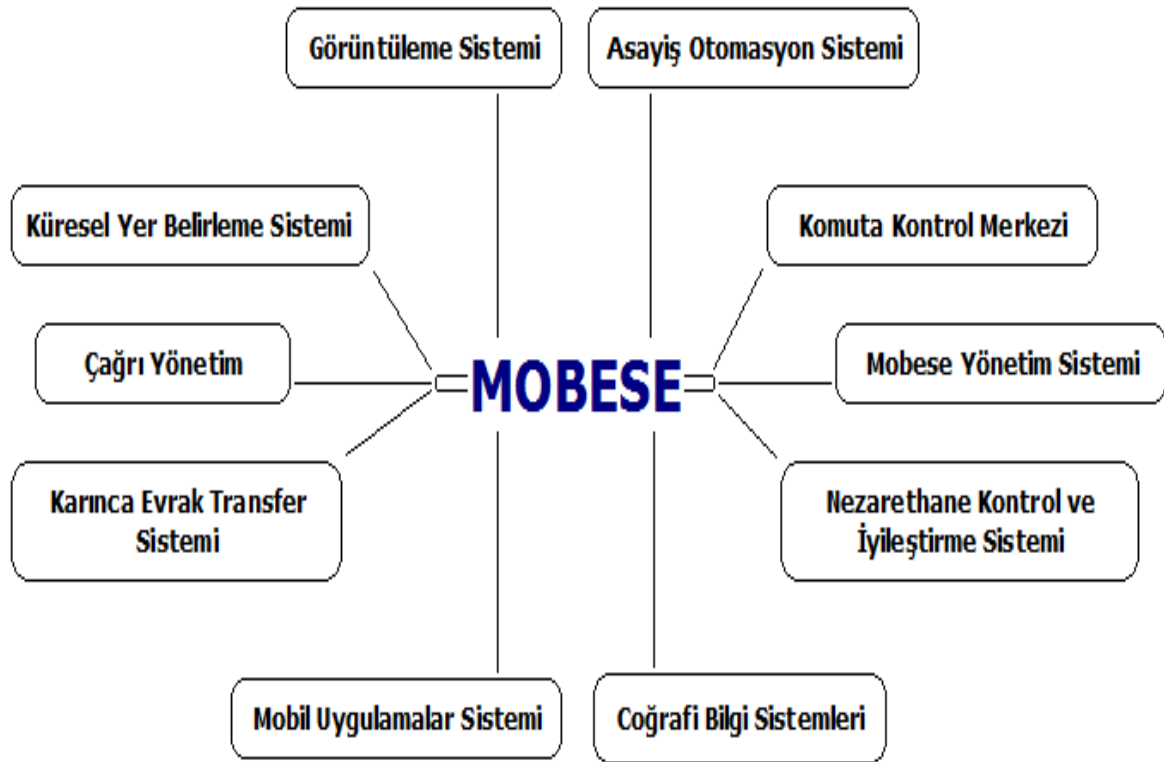
⁶⁸³ Eskişehir’de yerel bir televizyon kanalı Eskişehir’e de Mobese sistemi kurulması için kampanya başlatmış, işadamları ve halkın önemli desteğiyle beklenenin üzerinde bir bağış toplanarak kampanya başarıya ulaşmıştır. http://www.ikiyul.com.tr/yazar_goster.asp?ne=y48&sira=4312, (Erişim Tarihi: 06.06.2013).

⁶⁸⁴ 10 - 11.10.2013 Tarihlerinde Bilgi Teknolojileri Dairesi Başkanlığı ve Haberleşme Dairesi Başkanlığı’nda Üç Personel ile Yapılan Derinlemesine Görüşme.

edilmektedir.⁶⁸⁵ Mobesenin temel altyapısını uygulamaya yönelik sistemler, bu sistemleri faaliyete geçiren yazılımlar, donanımlar üzerindeki çeşitli bilgileri kodlayan, işleyen ve saklayan çeşitli programlar, kameralar, fiber optik kablo sistemleri oluşturmaktadır.⁶⁸⁶

Mobese denilince caddelerde, alışveriş merkezlerinde bulunan kameralar algılsa da esasında arkaplanda kapsamlı bir sistem ve yapı bulunmaktadır. Bu yapının temel bileşenleri aşağıda şematize edilmiştir. Bu bileşenler her il birimi için ayrı ayrıdır. Bütün il birimlerinin Mobese sistemlerinin yönetildiği tek bir merkez bulunmamaktadır.

Şekil-4. Mobese Projesi Bileşenleri



Kaynak: 10-11.10.2013 Tarihlerinde Bilgi Teknolojileri Dairesi Başkanlığı ve Haberleşme Dairesi Başkanlığı'nda Üç Personel ile Yapılan Derinlemesine Görüşme Sonrasında Oluşturulmuştur. Ayrıntılı Bilgi İçin Ek-4'e Bakınız.

Mobese; merkez modülü, mobil araç modülü, polis merkezi modülü olmak üzere üç ana modülden oluşmaktadır. Merkez modülü; tüm kameralardan gelen görüntü kayıtlarının toplandığı ve yönetildiği, Mobese iletişim trafiğinin düzenlenip denetlendiği ana modüldür. Bu modül bünyesinde çalışan personel tüm mobil ve polis merkezi modüllerini gözetleyebilmekte ve acil durumlarda da bu modüllerin birbirini izleyebilmesini sağlayabilmektedir. Ayrıca tüm Mobese kullanıcılarına *GPRS* üzerinden ulusal ve yerel

⁶⁸⁵ Polnet - Mobese İntranet Sayfası, (Erişim Tarihi 28.10.2013).

⁶⁸⁶ Müslüm Sayılı, *a.g.k.*, s.781.

veritabanlarından sorgu (GBT Sorgu gibi) yapabilme, birbirleri arasında sesli ve yazılı iletişim sağlayabilme imkanı vermektedir. Bütün kullanıcıların işlem kayıt verileri (*log* kayıtları) bu modülde tutulmaktadır.⁶⁸⁷

Mobil araç modülü ile sayısal harita üzerinde yer bilgisi, sesli uyarı ve acil durum bilgisi alınabilmekte; diğer mobil ekipler ile haberleşme yapılabilmekte; adres, olay, ihbar ve GBT sorgulama gerçekleştirilebilmektedir. Acil durum halinde tek tuş ile merkez ve diğer terminallere ekibin koordinat bilgisi haber verilebilmektedir. Polis merkezi modülü ile yetkili polisler ulusal ve yerel veritabanlarından sorgu yapabilmekte, olay rapor ve istatistikleri alabilmekte, aynı zamanda olaylara karışan şahıslara ilişkin olarak veri girişi de gerçekleştirebilmektedirler.⁶⁸⁸

Mobesenin temel altyapısı olan kamera sistemleri; hareketli kameralar, termal kameralar, muhafaza kutuları, kamera direkleri bileşenlerinden oluşmaktadır. Hareketli kameralar olarak *IP* tabanlı yakınlaşma kabiliyetine sahip olan görüntü aktarım cihazları; hareketli kameraların gece görüş kabiliyetinin yetersiz kaldığı, özel koruma ve güvenlik gerektiren yerlere yerleştirilen görüntü aktarım cihazları olarak termal kameralar; kameraları dış etkilerden ve çevre şartlarından korumak üzere yerleştirilen, yeterli güç kaynağına sahip muhafaza kutuları olan kamera kutuları ve kamera kutularını kablosuz ağ erişim donanımlarının monte edildiği, diğer şehir uygulamalarından bağımsız alt yapı ürünleri olan kamera direkleri kullanılmaktadır.⁶⁸⁹

Mobese sistemlerinin kurulum maliyeti illerde genel bütçeden veya Valilik, Polis Sandığı, Belediye Başkanlıklarının destekleri ile halk bağışları üzerinden sağlanmaktadır. Bu sistemlerin bileşenlerinin çok olması, kullandığı teknolojinin üretiminin ülkemiz değil merkez ülkeler tarafından gerçekleştirilmesi gibi faktörler nedeniyle maliyetinin yüksek olduğu ifade edilebilir. Düzenli bakım ve kontrol bedelleri de eklenince maliyeti giderek artmaktadır.⁶⁹⁰

⁶⁸⁷ DPT Bilgi Toplumu Dairesi Başkanlığı, *a.g.k.*, s.57.

⁶⁸⁸ 10 - 11.10.2013 Tarihlerinde Bilgi Teknolojileri Dairesi Başkanlığı ve Haberleşme Dairesi Başkanlığı'nda Üç Personel ile Yapılan Derinlemesine Görüşme.

⁶⁸⁹ *a.k.*

⁶⁹⁰ 2011 yılında Antalya bölgesinde yapılmaya başlanan Mobese sistemi 44'ü sabit, 72'si hareketli ve 4'ü de plaka tanıma olmak üzere toplam 120 kamerayla ve diğer bileşenleriyle 3.239.632 TL'lik bir maliyet bedeli ortaya çıkmıştır. <http://kemerhaber.com/gUNCEL/6020-80-gunde-hizmete-girecek.html>, (Erişim Tarihi: 17.12.2013).

Toplumsal algıda kameralı gözetim faaliyetleri öyle bir noktaya gelmiştir ki artık su, gaz, elektrik ve telefondan sonra “beşinci bir kamu hizmeti” olarak değerlendirilmektedir.⁶⁹¹ Bu algının oluşmasında başat rolü kameraların suçları önleme kabiliyeti olduğu düşüncesinin oynadığı önceki bölümlerde belirtilmiştir.⁶⁹² Mobesenin her ne kadar bununla ilgili somut araştırmalar olmasa da genel kanıda birçok suçun aydınlatılmasında, suçun failinin tespit edilmesinde faydası olduğu, proaktif polislik anlamında da suçların işlenmesinde genel caydırıcılık etkisi oluşturduğu ve özellikle asayiş suçlarının işlenmesinde ülke çapında önemli düşüşleri sağladığı iddia edilmektedir. Türkiye’de suçun azalmasına yönelik olan bu algı toplum, siyasetçiler ve güvenlik görevlileri tarafından kabullenilmiştir. Nitekim Mobesenin kuruluşundan itibaren bu kadar hızlı yaygınlaşması da bundan kaynaklanıyor denilebilir. Ancak daha önce belirtildiği gibi suç eğilimi ve riskini ortadan kaldırmak ya da azaltmak kamera kullanımıyla gerçekleşmeyeceği, bunun sadece indirgemeci ve mekanik bir yaklaşım olacağı da bir gerçektir.⁶⁹³

Mobesenin en büyük çıkmazının somut bir hukuki alt yapısının bulunmaması olduğu ifade edilebilir. Anayasanın 13. maddesine göre özel hayatın gizliliği sadece kanuni düzenlemelerle sınırlandırılabilir.⁶⁹⁴ Bu konuyla ilgili farklı tartışmalar olsa da sistematik ve her yerde bir sistem olarak Mobese kameraları bireye ait olan veriyi toplaması, depolaması, bireyin gündelik faaliyetlerini, hareket tarzını ortaya koyabilmesi açısından özel hayatın gizliliğini sınırlandırdığı iddia edilebilir.⁶⁹⁵ Dolayısıyla bu bakış açısında özel hayatın gizliliğini sınırlandıran bir sistem olarak Mobese ile ilgili gerekli hukuki düzenlemelerin yapılmasına ihtiyaç duyulduğu ifade edilebilir. Böyle bir düzenleme olmadığından dolayı günümüzde Mobese kameralarının çekmiş olduğu çeşitli dikkat çekici görüntüler (buzda kayarak düşen yurttaş, kaza yapan araç, başlarına sokakta tuhaf şeyler gelenler vb.) yazılı ve görsel medyada pervasızca yayımlanabilmektedir.

Mobesenin hukuki altyapı eksikliğinden kaynaklanan başka açık noktalar da bulunmaktadır. Örneğin, Mobese kameralarının nerelere kurulabileceği, çekilen görüntülerin nasıl, nerede, kimin tarafından saklanabileceği ve ne zaman imha edileceği gibi hususlara

⁶⁹¹ David Lyon, *a.g.k*, 2003, s.123.

⁶⁹² İpek Görgün, *a.g.k*, s.16.

⁶⁹³ *a.k*

⁶⁹⁴ Anayasa Madde 13: Temel hak ve hürriyetler, Devletin ülkesi ve milletiyle bölünmez bütünlüğünün, milli egemenliğinin, Cumhuriyetin, milli güvenliğinin, kamu düzeninin, genel asayişin, kamu yararının, genel ahlakın ve genel sağlığın korunması amacı ile ve ayrıca Anayasanın ilgili maddelerinde öngörülen özel sebeplerle, Anayasanın sözüne ve ruhuna uygun olarak kanunlarla sınırlandırılabilir.

⁶⁹⁵ Selim Çapar, “Open Street Surveillance in The UK And Turkey”, *Egovshare*, 2009, s.31. www.edem.todaie.gov.tr, (Erişim Tarihi: 22.05.2013).

yönelik herhangi bir düzenleme bulunmamaktadır.⁶⁹⁶ Bu durumda bireye ait olan görüntü verileri yıllarca saklanabilir. Bu verilerin farklı kişilerin eline geçmesinin de önünde herhangi bir engel gözükmemektedir. Ayrıca Mobese kameralarından elde edilen görüntüler mahkemelerde delil olarak da kullanılabilir. Hukuki altyapısı olmayan böyle bir sistemden elde edilen delillerin de hukuka aykırı yollarla elde edilmiş delile dönüşme ihtimali de bulunduğu söylenebilir.⁶⁹⁷

Mobese kameralarının altında bireylerin kendilerini özgür hissedemeyeceklerine yönelik eleştiriler de bulunmaktadır. Karakehya bunu şöyle ifade etmektedir:⁶⁹⁸

“Kamuya açık hemen her alanın gözetlendiği bir çevrede yaşama psikolojisine sahip bireylerin kendilerini ne kadar özgür hissedebilecekleri; bu bireylerin ruhsal durumlarının ne kadar dengeli olacağı ve böyle bir ortamda yetişen bireylerin oluşturduğu toplumun ne kadar sağlıklı gelişebileceği son derece tartışmaya açıktır. Nitekim toplumsal alandaki bu tür müdahaleler belki bir oranda suç işlenmesini engelleyebilir; ancak hiçbir zaman için bireyleri özgürleştirmez ve toplumsal gelişimin önünü açmaz.”

Mobese sisteminin getirdiği kaygılara dikkat çekmek için ve bu sisteme karşı duruş olarak 2005 yılında “Nobese Sivil Toplum Hareketi” oluşturulmuş ve halen faaliyetlerine devam etmektedir. Nobese üyeleri kendi oluşturdukları bu hareketi, “insanların resmi kurumlar tarafından kentin güvenliğine karşı potansiyel tehdit olarak görülüp sürekli olarak gözetim altında tutulma durumuna karşı bir hareket” olarak ifade etmektedirler.⁶⁹⁹ Bu hareketin üyeleri sanal alemde de “www.izleniyoruz.com” internet adresinde seslerini duyurmaktadırlar.

III. EMNİYET TEŞKİLATI’NDA TEKNOLOJİK DÖNÜŞÜMÜN SONUÇLARI: TEHDİTLER, RİSKLER VE ÖNERİLER

Emniyet Teşkilatı’nda Polnet ve Mobese projeleri ile bunlara bağlı alt uygulamalar araçlarında süregelen teknolojik gelişmelerin yönünün gözetim eksenli olduğu ifade edilebilir. Teknolojik gelişimin bu yönde olmasının nedenleri ulusal ve uluslararası faktörlere bağlanabilir. Ulusal anlamda, meydana gelen kapkaç, hırsızlık gibi asayiş ve terör olaylarının artış göstermesi ve bu nedenle Emniyet Teşkilatı üzerinde suçla mücadele konusunda oluşan toplumsal beklentiler ve iktidar baskısı gösterilebilir. Uluslararası boyutta da gözetim teknolojilerinin her geçen gün gelişmesinin, yeni gözetim programlarının kullanılmasının Emniyet Teşkilatı’nın bilişim altyapısını bu programları kullanmaya yönelik değişken ve esnek bir yapıya kavuşturması yönünde etkilemesinden bahsedilebilir.

⁶⁹⁶ a.k

⁶⁹⁷ Hakan Karakehya, *a.g.k*, s.344 - 346.

⁶⁹⁸ a.k

⁶⁹⁹ İpek Görgün, *a.g.k*, s.1.

Günümüzde gözetim teknolojilerini kullanabilir bir bilişim altyapısına sahip olarak Emniyet Teşkilatı'nın suçla mücadelede oldukça başarılı olduğu ifade edilebilir. Suçla mücadelede toplumsal beklentiyi karşılama uğruna gerçekleştirilen uygulamalarla bazı tehditlerin de kendini gösterdiği düşünülmektedir.

Üzerlerinde bir başkasının bakışlarının olduğu korku ve kaygısı insanları itaatkar ve sadık hale getirmiştir. Bu durum, günümüz gözetim teknolojilerinin varoluşlarının altında yatan temel kolonlardan birisidir. Gözetlemeler sonrasında yapılan ani soruşturma, tutuklamalar ve büyük cezalandırmalar toplumda örnek teşkil etmiş ve toplumu bir sessizlik bahçesi haline getirmiştir. Başkaları tarafından izlenme ihtimalini kabul eden yurttaşlar gönüllü olarak uyum içinde hareket etmeye zorlanmıştır. Bu noktada video kameraların veya diğer gözetim araçlarının etkisi, kesin bilgiler elde etme ve şüphelileri tam olarak tespit etme gücü değil bunların toplumda oluşturduğu kronik korkudur.

Bugün iktidar güçleri gözetim araçlarını toplumda sadece kanunlara, temel ilkelere sadakat ve bağlılık sağlanması için kronik korku oluşturma amacıyla kullanmamaktadır. Artık istediği bundan daha ileri seviyede iktidar alanı içinde ve dışında her yerde her zaman olup bitenleri bilmektir. İktidarın bu gücünü geliştirmiş gözetim teknolojileri ve oluşturduğu korku kültürünün sonucu olan muhbirlerden aldığı ifade edilebilir.

Günümüz iktidar sahipleri varlıklarını artık toplum düzenini temin etmek ve güven sağlamak değil; korku, güvensizlik ve şüphecilik üzerine inşa etmektedirler. Tehlike ve suçlara karşı tedbir alma kaygısı onların sürekli bir kırmızı alarm ruhu içerisinde olmalarını gerektirmektedir.⁷⁰⁰ Eğer her şey kontrol altında tutulmak isteniyorsa tehlike her yerde artış gösteriyor olabilir demektir. Dolayısıyla her yerin izlenmesi ve takip edilmesi gerekmektedir. Bu bakış açısında her yer tehlike arz ettiği için takip edildiğine göre, her yerde olan herkes de tehlikelidir. Herkes saldırgan veya terörist olabilir. Herkesi ve her yeri bilmeyi sağlayan güç zamanla öyle bir noktaya gelir ki artık sistem herkesi ve herkesin hareket tarzını bilme ve profillemeye kudretine sahip olur. Eğer bir kimse genel hareket profilinin dışına çıkarsa riskli ve tehlikeli kişi olarak değerlendirilebilir. Ayrıca bir kimse sistem tarafından ne kadar az tanınıyorsa; yani kişi kameralar önünden ne kadar az geçmişse, bilişim sistemlerini ne kadar az kullanmışsa o kadar çok tehlikeli, hatta şüpheli olarak değerlendirilebilir.

İktidarın bilgi dağarcığındaki her boşluk daha çok soruşturma ve araştırma yapılmasını gerektirmektedir. Bu durum toplumu öyle bir hale getirmiştir ki artık toplumdaki her unsur

⁷⁰⁰ Wolfgang Sofsky, *a.g.k.*, s.20 - 22.

ulusal güvenliğin bir ajanına dönüşmüştür. Bu noktada yurttaşlar da doğal ajanlar olarak değerlendirilir ve şüpheli şahısları ulusal güvenlik görevlilerine haber verme yükümlülüğü altına sokulurlar. Toplumda oluşturulan bu algı ve anlayış durumu sadece özgürlükleri sınırlandırmakla kalmamakta ayrıca sosyal bağları koparmakta, komşuluk müessesesini kaldırmakta, insanları birbirine güven duymaz hale getirmektedir. Evinizde otururken, yan dairedesine komşu gözüyle bakmak yerine potansiyel saldırgan veya terörist olarak bakma topluma aşılır hale gelmiştir. Sonuçta toplumda hiçbir yurttaş kendini güven içinde hissetmemektedir.

Gözetim toplumunun tehdit ettiği en büyük hak özel hayatın gizliliği hakkıdır. Zira burası sermaye sahiplerinin ve iktidar odaklarının girmemesi gereken bir alan, adeta bir nefes alma boşluğudur. Ancak günümüzde gerçekleştirilen gözetim faaliyetleri bireyin bu nefes alma boşluğunu her geçen gün daha da daraltmaktadır. Gözetim faaliyetlerini gerçekleştiren güç odaklarının bireyin özel hayatına saygı duyması gerekmektedir. Bu alana normal şartlarda sadece özel hayatın gizliliği hakkından daha öncelikli olan yaşama hakkının tehlikede olması halinde müdahale edilebilir olmalıdır. Günümüzde “yaşama hakkı” kavramı genişletilerek güvenlik kavramıyla örtüştürülmüştür. Bu durumda güvenliği sağlama adına kişilerin mahremiyeti çiğnenebilir hale gelmiştir. Güvenliğin sağlanması ile özel hayatın gizliliğine saygı arasında önemli bir çizgi bulunmaktadır. Bu çizgide prensip olarak ihlal edilen taraf özel hayatın gizliliği olmaması gerekmektedir.

Küreselleşen gözetimin birey ve toplum bazında olumsuz etkilerini yok etmenin mümkün olmadığı düşünülmektedir. Ancak gözetlenenlerin, gözetim faaliyetlerinin sınırını bilmesi açısından gözetleyenlerin hesap verebilirliği gibi bazı mekanizmaların olması gerektiğine inanılmaktadır. Özellikle ileri teknoloji kullanarak yoğun gözetleme yapan birimler muhtemel zararlı sonuçlara karşın hesap verebilir konumda olmalı, hesap verebilirliklerini sağlamak için çeşitli sistemler geliştirilmeli ve kurulmalıdır.⁷⁰¹ İş ortamı gözetlemelerinde bu hesap verebilirlik bazı işyerlerinde dar kapsamda da olsa sağlanmıştır. Zira işçi sendikalarının aktif çalışmalarıyla işverenler işçileri gözetleme faaliyetlerini belirli oranlarda kısıtlamak zorunda kalmıştır. Müşteri gözetlemesi durumu için ise şu ana kadar yapılabilen gelişme kamera görüntülerinin alışveriş yapılan yerde halkın görebileceği şekilde konumlandırılması olmuştur. Bunun dışında küçük dükkanlara girdiğinizde bile karşınızda size yönelmiş duran bir kamera karşılayabilmektedir. Güvenlik boyutuna bakan yönde amir denetimi dışında bir kontrol mekanizması gözükmemektedir. Örneğin, Mobese kamera

⁷⁰¹ David Murakami Wood, *a.g.k*, s.8.

kayıtlarının nerede, ne kadar süre saklandığına dair belirsizlik vardır. Bu noktada gözetim faaliyetlerinin sınırlandırılması veya kontrol altında tutulmasına yönelik olarak elle tutulur düzenlemelerin olmadığı düşünülmektedir.

Polnet ve Mobese projeleri içerisinde yurttaşa ait olan parmak izi gibi biyometrik verilerin, kapsamı geniş olan kamera görüntülerinin, suç kayıtlarının, ihbar bilgilerinin, adres-araç-pasaport-telefon bilgileri gibi birçok verinin toplandığı ifade edilebilir. Bu verilerin tek bir veritabanında toplanarak yurttaşla ilişkilendirilmesi, çeşitli kalıplarda profillerin çıkarılması yurttaşa ait olan birçok şeyin iktidar tarafından bilinmesi anlamına gelecektir. İktidarın gözetim yapan birimlerine MİT, Jandarma, Genelkurmay Başkanlığı gibi diğer güvenlik birimleri de eklendiğinde iktidarın yurttaşa yönelik elindeki bilgi gücünün seviyesinin tahmin edilemeyecek boyutlarda büyük olacağı değerlendirilmektedir. Türkiye'deki bu tablo Mark Poster'ın "süperpanoptikon" kavramıyla açıklanabilir. Yurttaşların ülke içinde kendilerini takip eden gözler gerçekliğinin farkında bile olmadan duvarsız, penceresiz, gözetleme kulesiz bir gözetim çevresinin içine mahkum olduğu düşünülmektedir.⁷⁰²

Emniyet Teşkilatı'nın güvenlik gerekçeleriyle gözetim faaliyetlerinden geri dönüşünün mümkün olmadığı gözükmektedir. Ancak önümüzdeki dönemde yurttaşların kişisel hak ve özgürlüklerini merkeze oturtan bir güvenlik anlayışı içinde ilerlemesi gerektiği değerlendirilmektedir. Eğer bir güvenlik toplumu değil, özgürlüklerin özgürce yaşanabildiği bir toplum olmak istiyorsak başta devletin yönetim kadrosu olmak üzere bu anlayışı benimsemek zorundayız. Emniyet Teşkilatı bu yeni teknolojik gelişmeleri uyguladığı takdirde ortaya çıkacak olan fayda ile zararı ve uygulamadığı takdirde ortaya çıkacak olan zararı ve faydayı ortaya koymalı, bunun sistemsel analizini yapmalı ve seçtiği metotta ortaya çıkan zararları gözardı etmemeli, gerekli adımları atmalı ve önlemleri almalıdır.

Yukarıda ifade edilenler ekseninde bu bölümde Emniyet Teşkilatı'ndaki teknolojik dönüşümün neticesinde yurttaş ve kurumsal yapı açısından ortaya çıktığı veya çıkabileceği değerlendirilen tehditlere dikkat çekilecektir. Ayrıca Emniyet Teşkilatı gözetim faaliyetlerinin içinde barındırabileceği bu tehditlerin gerçekleşme oranlarını minimuma indirmek ve gözetim faaliyetlerinin kontrol altında tutulabilmesi için bazı yapısal önerilerde bulunulacaktır.

⁷⁰² Mark Poster, *a.g.k.*, 2001, s.175 - 192.

1. Kuruma Yönelik Tehditler

Emniyet Teşkilatı bilgi ve iletişim teknolojilerinin gözetim eksenli olarak gelişim göstermesinin kuruma, personele bakan yönüyle ortaya çıkardığı bir takım tehditler bulunmaktadır. Bu tehditler beş başlık altında incelenecektir. Birincisi gözetimin imkanlarının sağladığı güç zehirlenmesi nedeniyle kurumsal ve personel boyutunda oluşabileceği değerlendirilen güvenlik paranoyası olacaktır. İkinci olarak gerek güvenlik paranoyasının etkisiyle gerek gözetimin imkanlarının sınır tanımaz hale gelmesi nedeniyle Emniyet Teşkilatı görevlilerinin suçla mücadele için istihbari amaçlı gerçekleştirecekleri çalışmaların evreninin genişlemesi tehdidi anlatılacaktır. Üçüncü olarak Emniyet Teşkilatı'nda gözetleyenlerin gözetimi eleştirilecektir. Dördüncü olarak yurttaşa ait olan verilerin güvenliğinin sağlanamamasının kuruma bakan yönleri tartışılacaktır. Son olarak da gözetimin uygulamasının doğru davranışlar çevresinde gerçekleştirilmesi amaçlı olarak etik ve meslek etiği kapsamında kurumsal gözetim faaliyetleri değerlendirilecektir.

1.1. Güvenlik Paranoyası

Güvenlik bir iktidar tekniğidir. İktidarın yurttaşlara ulaşmada, ilişki kurmada oluşturduğu bir kanaldır. Devlet, biçimlerine göre doğrudan veya dolaylı olarak meşruiyetinin kaynağını bu kanaldan almaktadır.⁷⁰³ Geleneksel devletlerde halkı zapt altında tutmada bir araç olarak kullanılan güvenlik, günümüzde gözetim teknolojilerinin halka yöneltilmesinde, gözetimi yapan personelin daha çok gözetim faaliyetinde bulunma istek ve arzusunun oluşturulmasında kullanılan bir araca dönüşmüştür.

Yukarıda belirtilen istek ve arzunun oluşmasının altında yatan birinci neden olarak gözetim teknolojisinin sağladığı bilgiye sahip olma gücünün güvenlik güçlerini iktidarlaştırması ifade edilebilir. Başlangıçta iktidarın gücünü pekiştirmek için gözetim araçlarıyla bilgi toplayan güvenlik birimleri zamanla üzerlerinden akan bu güç potansiyelini kendileri de kullanmak isteyebilirler. Bu durumda iktidarın gölgesi gibi hareket etmeye başlayabilirler. Nitekim polis güçlerine yönelik yurttaşların “devletin polisi” değil “hükümetin/iktidarın polisi” olarak eleştirel yaklaşımları da bu şekilde açıklanabilir. İktidarın gölgesi gibi davranmaya başlayan güvenlik güçleri iktidarın bireye hakim olmak ve onu terbiye etmek için daha çok bilgi toplama, her şeyi bilme sınır tanımaz hırsını kendilerinde hissetmeye başlayabilirler.⁷⁰⁴

⁷⁰³ Evren Haspolat, *a.g.k.*, s.42 - 43.

⁷⁰⁴ Hakan Karakehya, *a.g.k.*, s.333 - 335.

Emniyet Teşkilatı'nda Polnet, Mobese, istihbarat birimlerinin gözetim projeleri ile yurttaşa dair veriler toplanmaktadır. Toplanan bu veriler ışığında iktidar kendini daha güvende hissetmektedir. Bu güven ve güvenin oluşturduğu güç gerek kurum gerek personel tarafından sahiplenilebilmektedir. Bu noktada Emniyet Teşkilatı mensupları bilginin toplandığı gözetim araçlarını meşrulaştıran güvenlik görevlerini kutsallaştırabilmektedirler. Kutsallaşan görev ile güvenlik, bir kamu hizmeti olmaktan çıkarak bazen “halka rağmen güvenlik” algısında paranoyak bir hale dönüşebilir.

Suç sayıları ve çeşitlerinde meydana gelen yükseliş veya terörist eylemler, bombalı saldırılar gibi yankı uyandıran olayların meydana gelmesiyle güvenlik güçlerinde “suçların işlenmesine engel olma” görevlerini olması gerektiği gibi yerine getiremedikleri inancı toplumsal baskıyla birleşince ortaya bir güvenlik paranoyası çıkabilmektedir. Bu güvenlik paranoyasının yurttaşa dönük kısmı sonraki bölümde anlatılacaktır. Personele bakan yönünde farklı olumsuzluklar ortaya çıkabilmektedir. Bunlardan birisi şüphesiz Emniyet Teşkilatı gibi dikey hiyerarşik örgütlenmiş bir birimde yukarıdan aşağıya indikçe artan iş baskısı olacaktır. Hem bu baskının hem de güvenlik paranoyasının bir sonucu olarak gözetim faaliyetlerinde bulunan personel “suçların önlenmesi” görevinin arkaplanında yer alan istihbarat faaliyetlerine eskisinden çok daha fazla ağırlık verecektir. Bunun da bir sonucu olarak gözetim araçlarına olan gereksinimi eskisine göre artacaktır. Gelişen gözetim teknolojileri evreninde bu gereksinimini karşılayarak daha çok gözetim yapacaktır. Gözetim teknolojilerinin sağladığı şaşırtıcı bilgi toplama yetenekleri zamanla güvenliğin temin edilmesinde sıfır hata ile hareket etme güdüsüne dönüşebilecektir. Esasında güvenlik paranoyasından gözetim teknolojilerine geçiş ve gözetim teknolojilerinden güvenlik paranoyasına geçiş kendi içinde bir döngüsellığe sahiptir. Aşağıda belirtilen Türkiye ve diğer ülkeler örneklerinde bu durum daha net olarak anlaşılmaktadır.

11 Eylül 2001 terörist saldırılarından sonra ABD’de hızla artan bir güvenlik paranoyası oluşmuştur. Böylece gözetimin önünde bulunan bütün engeller aşılıp tam randımanlı gözetime geçiş gerçekleşmiştir. Bu saldırılardan sonra ABD’de alınan önemli kararlardan birisi insan hakları ve özgürlüklerini tümüyle daraltarak, bireye ait mahremiyetler alanını yok ederek her türlü iletişimin dinlenmesine ve gözetim pratiklerinin maksimum noktaya taşınmasına yönelik bilgi edinimi ve paylaşımının sağlanması kararı olmuştur.⁷⁰⁵ ABD’de Ulusal Güvenlik Birimi (NSA) öncülüğünde gelişmiş gözetim teknolojilerinin

⁷⁰⁵ Uğur Dolgun, “Gözetim Devleti, ‘Penguenler’, ABD ve FBI Örneği”, 20.06.2013 tarihli Taraf Gazetesi Köşe Yazısı.

kullanılması ve tüm dünyayı tehdit olarak görmenin bir yansıması olarak dünya çapında milyonlarca telefon numarasının takip edilmesi de bu güvenlik paranoyasının göstergesi olarak işaret edilebilir.⁷⁰⁶

07 Temmuz 2005 tarihinde İngiltere'nin Londra şehrinde metro istasyonlarında meydana gelen 56 kişinin öldüğü yüzlerce kişinin yaralandığı bombalı terörist saldırılarından sonra ABD'deki 11 Eylül saldırılarından sonraki sürece benzer gelişme yaşanmıştır. İngiltere başta Mobese benzeri güvenlik kameraları olmak üzere gözetim teknolojilerini arttırmış ve geliştirmiştir. Nitekim bugün İngiltere'de 5.9 milyon adet Mobese benzeri güvenlik kamerası bulunması da bunun açık bir neticesidir.⁷⁰⁷

2003 yılında Türkiye'de Sinagog, HSBC Bankası ve İngiliz Konsoloslugu'nda düzenlenen 63 kişinin öldüğü bombalı terörist saldırılar da ABD ve İngiltere'deki saldırılar çerçevesinde değerlendirilebilir. Bu saldırılar sonrasında Türkiye'nin de ABD ve İngiltere'de olduğu gibi gözetim teknolojilerine ağırlık verdiği bilinmektedir. Mobesenin aktif olarak kullanılmaya başlanması 2005 yılı ve sonrasında, Polnet projesinin yeni nesil gözetim teknolojilerine uygun bir şekilde evrilmesi de 2003 ve sonrasında olması Emniyet Teşkilatı yönünde bu iddiayı teyit eder niteliktedir.

Güvenlik paranoyası güvenlik güçleri ve toplum açısından oldukça riskli bir durumdur. Zira böyle bir paranoya ile oluşan “toplumun güvenliği adına gözetim alanında ve ülkedeki teröristleri, suçluları takip etme noktasında sürekli yetersiz olunduğu” düşüncesi, hem toplum hem de güvenlik güçleri nezdinde belli bir süre sonra yersiz bir korku ve endişeye dönüşebilir.⁷⁰⁸ Bu korku ve endişe durumu ile siyasal otoritenin suçların önlenmesi ve terörist eylem oluşumlarının tespitine yönelik şiddetli baskısı birleşince kurumsal ve görevsel açılardan stres unsuru meydana gelebilir. Böyle bir stres, korku, panik ortamında hareket eden güvenlik güçlerinin daha çok gözetlemek isteyecekleri bir gerçektir. Hatta böyle bir durumda yurttaşın mahremiyeti gibi konular çok önemsenmeyebilecektir.

1.2. Proaktif Polislikten Düşünce Polisliğine

Gözetim teknolojilerindeki hızlı gelişimin ve güvenlik paranoyasının yayılmasının Emniyet Teşkilatı'nda oluşturabileceği en büyük tehlikelerden birisi gözetimin derinleşmesidir. Derinleşen gözetim ile istihbarat faaliyetlerinin arkasında yer alan “proaktif

⁷⁰⁶ <https://www.eff.org/nsa-spying>, (Erişim Tarihi: 19.12.2013).

⁷⁰⁷ <http://www.securitynewsdesk.com/2013/07/11/bsia-attempts-to-clarify-question-of-how-many-cctv-cameras-in-the-uk/>, (Erişim Tarihi: 19.12.2013).

⁷⁰⁸ Uğur Dolgun, *a.g.k*, 20.06.2013 Tarihli Taraf Gazetesi Köşe Yazısı.

polislik” uygulamaları haddini aşarak suç oluşmadan önce suçu önleme hedefli olarak George Orwell’ın *Bin Dokuz Yüz Seksen Dört* isimli kitabında belirttiği “düşünce polisliğine” evrilebilir.

Proaktif polislik; suç oluşmadan önce suçun önlenmesine yönelik yapılan polisiye faaliyetleri ifade etmektedir. Proaktif polisliğin iki yönü bulunmaktadır. Bunlardan birincisi farklı kurumlarla, sivil toplum kuruluşlarıyla, halkla polisin iletişim gücünü arttırarak suçun oluşmasına zemin hazırlayan etmenlerin ortadan kaldırılması veya bunlara yönelik tedbir alınmasıdır. Örneğin, mahallede meydana gelen işyerinden hırsızlık olaylarına karşı işyeri sahipleri ile görüşülerek hırsızlığın önlenmesi amaçlı dükkanlara alarm sistemi taktırılması, caydırıcılık için güvenlik kamerası yerleştirilmesi, kepenk kullanılması gibi önleyici tedbirlerin alınmasını gösterebiliriz. Proaktif polisliğin ikinci ve bizi ilgilendiren yönü suçlar oluşmadan önce istihbarat faaliyetleri yoluyla suçla mücadeleye yönelik polisiye faaliyetlerdir.⁷⁰⁹ Dolayısıyla proaktif polisliğin temel özelliği suç henüz oluşmadan önce işlenmesi muhtemel suçlara yönelik gerçekleştirilmesidir. Bu tür polislik faaliyetlerin gerçekleştirildiği ülkelerde istihbarat birimleri kuvvetlidir. Zira bilinmeyen bir suçun bilinmeyen zamanını, bilinmeyen faillerini tespit edebilmek için o birimin gözetim teknolojileriyle donatılması, güvenlik tabanlı olarak sınırsız veriye erişim imkanının olması gerekmektedir. Dolayısıyla gelişen gözetim teknolojileriyle proaktif polisliğin özellikle ikinci ayağının suistimale açık olduğu bir gerçektir.

Emniyet Teşkilatı gibi güvenlik birimlerinde proaktif polislik uygulamalarının kontrolsüz bir şekilde artış göstermesi personelin gözetlemenin cazibesine kapılmasına yol açabilir. Nitekim olan bir suçu ispat etmek kolaydır. Fakat henüz olmayan bir suçu ispat etmek için her taşın altına bakmak gerekir ve oldukça zordur. Bu kadar zor bir işi gerçekleştirmek için bireyin mahremiyetine daha çok müdahale gerekebilir. Hatta durum öyle bir hal alabilir ki bireylerin düşüncelerinde suç işleme kastı olup olmadığını, suça meyilli olup olmadıklarını tespit etme ihtiyacı doğabilir. İşte burada daha önceki bölümlerde vurgulanan Orwell’ın ifade ettiği “Düşünce Polisliği” distopyası bir gerçek olarak karşımıza çıkabilir.

“Düşünce polisliği” Orwell’ın *Bin Dokuz Yüz Seksen Dört* romanında distopik gözetim dünyasının önemli bir denetim mekanizmasını oluşturmaktadır. Görevi, Büyük Birader olarak ifade edilen totaliter otoriteye karşıt düşünceli olan ya da kurallara şüphe ile bakan insanları tespit ederek önce “Sevgi Bakanlığı” olarak ifade edilen işkence merkezlerinde düzeltmek hala devam ediyorsa da buharlaştırarak öldürmektir. Düşünce polisinin düşüncelere ulaşma

⁷⁰⁹ Aytekin Geleri, *Devriye Polisi*, Seçkin Yayınları, Ankara, 2002, s.21 - 25.

araçları herkesin evinde yirmi dört saat açık tutulması zorunluluğu olan ve sahip olduğu kameralarla bireyin hareketlerini, mimiklerini izleyen tele-ekranlar, her yerde olan kameralar, muhbirler ve bireyin olağan dışı aktivitelere girme niyetinde olup olmadığını değerlendirmek için kullanılan uzaktan kalp atışlarını algılayan sensörlerdir. Bu gözetim teknolojileriyle bireyin düşünceleri takip edilmektedir.⁷¹⁰

Her ne kadar Orwell romanında düşünce polisliğini distopik bir kavram olarak kullanmışsa da günümüzde bunun var olduğu gözlemlenebilir. Nitekim Haziran 2013’de meydana gelen “Gezi Parkı Olayları” sonrasında güvenlik güçleri tarafından benzeri toplumsal olaylar henüz başlamadan önce bunların tespit edilmesi hedefli olarak internet ve sosyal medyaya yönelik analiz çalışmalarına ağırlık verildiği bilinmektedir. Mesela *Twitter*, *Facebook* gibi sosyal paylaşım sitelerinde insanların ifade ettikleri düşüncelerinin ve değerlendirmelerinin semantik analizi⁷¹¹ yapılmaya çalışılmaktadır. Örneğin ABD’de “*Topsy Pro*”⁷¹² isimli *Twitter* analiz programı kullanılarak halkın tepkileri ölçülmekte ve toplumsal olayların nerede, ne zaman, nasıl çıkacağına yönelik çalışmalar yapılmaktadır. Hatta alışveriş mağazaları tarafından semantik analiz kullanılarak halkın ürünlere olan tepkisi, beğenileri ölçülebilmektedir. Siyasi partilere yönelik olarak olumlu - olumsuz tepkiler analiz edilerek bir anlamda oy değerlendirmesi yapılabilmektedir. Bu noktada Orwell’ın ifade ettiği düşünce polisliğinin günümüzde zaten yapıldığını söyleyebiliriz. Günümüz itibarıyla ülkemizde de güvenlik paranoyasının bu ve belki daha gelişmiş programlar kullanılarak düşünce polisliğine dönüşmesi tehlikesi bulunmaktadır.

1.3. Gözetleyenlerin Gözetimi

Emniyet Teşkilatı’ndaki teknolojik dönüşümün gözetime evrilmesinin kurumsal anlamda meydana getirebileceği tehlikelerden birisi de gözetleyenlerin gözetiminin yapılması ve bunun ortaya çıkarabileceği olumsuzluklardır. Polnet ve Mobese projeleri sadece yurttaşlara yönelik değildir. Bu projelerde yurttaşlara yönelik olan programları kullanan polisleri kontrol etmek için de gözetim programları bulunmaktadır.

⁷¹⁰ George Orwell, *a.g.k*, s.22 - 23.

⁷¹¹ Semantik analiz; sosyal medya üzerindeki her ifadenin, etkileşimin olumlu veya olumsuz olarak kategorize edilmesi ve sonrasında oransal analiz yapılmasını ifade etmektedir. Örneğin “Mülkiye” ifadesini “semantik analize tabi tut” denildiğinde sistem otomatik olarak içinde Mülkiye kelimesi geçen tüm twitleri tespit eder. Sonrasında bu twitlerde kullanılan olumlu ve olumsuz ifadeler göre bir yorumlama yapar. Bu yorumlama twitlerin anlamsal olumluluk veya olumsuzluk oranına göre şekillenir. Mesela son bir ay içinde Mülkiye ile ilgili olumlu twitler %78, olumsuz twitler %22 gibi. Bu durum Mülkiye’ye sosyal medyada son bir ay içinde pozitif bir yaklaşım sergilendiğini göstermektedir.

⁷¹² <http://topsy.com/analytics>, (Erişim Tarihi: 19.12.2013).

Polnet ve Mobese uygulamaları içerisinde “Küresel Yer Belirleme Sistemi (*İng; GPS, Global Positioning System*)” ve “Çağrı Yönetim Sistemi” yer almaktadır. Bu sistemler, polis birimlerine veya çağrı merkezine bir ihbar geldiğinde olay yerine en yakın ekibi olay mahalline sevk etmek için ekip aracının harita üzerinde noktasal olarak konumunu belirlemek amacıyla kullanılmaktadır.⁷¹³ Ancak aynı sistemi ekip amirleri de kullanabildiğinden dolayı ekip araçlarının gün içindeki tüm hareket tarzı, olay yerine olan uzaklığı, olay yerine ulaşma süresi ya da devriye görevi yapan ekiplerin hareket halinde olup olmadığı, dinlenmek için bekledikleri yerlerde geçirdikleri süre, görev mahalli dışına çıkıp çıkmama durumları ekip amiri tarafından canlı ve geçmişe dönük olarak takip edilebilmektedir.

Polnet projesi bileşenlerinden olan “Asayiş Performans İzleme ve Takip Sistemi” ile okullarda görev yapan polis memurlarının okullara giriş - çıkış saatleri ve günlük faaliyetleri kaydedilmektedir.⁷¹⁴ Görevli polis memurunun faaliyet raporunda ifade ettiği olaylar, müdahaleler ile okul ders ve teneffüs saatleri karşılaştırılarak performansı ölçülmektedir. Bu noktada personelin yaptığı bütün faaliyetlerin takip edilmesi iş verimliliği açısından olumlu karşılanabilse de onun mekanik bir varlık gibi algılanması zamanla personel üzerinde baskı aracına dönüşebilmektedir.

Mobese projesi bileşenlerinden olan “Nezarethane Kontrol ve İyileştirme Sistemi” ile nezarethaneler de dahil olmak üzere tüm polis merkezleri 7 gün 24 saat kameralara sesler de dahil olmak üzere kaydedilmektedir. Bu kayıtlar il içinde tek bir merkezde toplanmaktadır.⁷¹⁵ Polis müfettişleri ve kayıt sisteminin başında görevli amir personel düzenli olarak bu kayıtları izlemekte ve hukuka aykırı veya görevle bağdaşmayan davranışlarda bulunan personel hakkında adli ve idari soruşturma başlatmaktadırlar. Sistemin yurttaşa bakan yönüyle polis merkezlerinde görev yapan personelin işkence, hakaret gibi suçları işlemesini engelleme açısından faydalı olduğu ifade edilebilir. Ancak, görevli personelin tüm hareketlerinin ve konuşmalarının sistematik ve aralıksız kaydedilmesi personel üzerinde psikolojik baskı aracı haline dönüşebilmektedir.⁷¹⁶ Personelin tuvalete giriş - çıkış zamanlarının, arkadaşlarıyla şakalaşmalarının, telefon görüşmelerinin, bilgisayar başında geçirdiği vaktin takip edilip kaydediliyor olması onların üzerinde gizli bir psikolojik taciz (*ing; mobbing*) oluşturabilmektedir.

⁷¹³ 10 - 11.10.2013 Tarihlerinde Bilgi Teknolojileri Dairesi Başkanlığı ve Haberleşme Dairesi Başkanlığı'nda Üç Personel ile Yapılan Derinlemesine Görüşme.

⁷¹⁴ a.k

⁷¹⁵ a.k

⁷¹⁶ David Murakami Wood, a.g.k, 2006, s.8.

Polnet ve Mobese üzerinde yer alan bilişim sistemlerini kullanan personelin tüm işlem kayıtları (*log* kayıtları) depolanmaktadır. Zaman zaman iş performansı açısından bu kayıtlar analize tabi tutularak personel hakkında “en çok çalışan”, “en az çalışan” gibi kategorilendirmeler yapılabilmektedir. Bu şekilde personelin bilgisayar üzerinde programları kullanarak yaptığı tüm klavye ve fare hareketlerinin başkaları tarafından takip edilmesi rahatsızlık verici bir durumdur.⁷¹⁷ Yapılan gözetim faaliyetleri hem yukarıda ifade edilmiş olan personel üzerinde psikolojik tacize dönüşmekte hem de personelin “iş esnasında farkında olmadan hatam olduysa soruşturma geçirebilirim” korkusu içinde işlerini icra etmesine yol açmaktadır. Daha net bir ifadeyle Polnet, Mobese ve bu projelerin bileşenlerini kullanan polislere yönelik daha önceki bölümlerde belirtilen “çalışma yaşamında gözetim” faaliyetlerinin uygulandığı söylenebilir.

Yukarıda belirtilen Emniyet Teşkilatı’ndaki gözetleyenlerin gözetimine dair verilen somut örnekler perspektifinde personele bakan yönüyle iki temel sonuç çıkarılabilir. Birincisi önceki bölümlerde ifade edilmiş olan çalışma yaşamında yapılan gözetim faaliyetlerinin olumsuz etkileri bu şahıslar için de geçerlidir. Günlük rutin içinde yaptıkları faaliyetler gözetim faaliyetleri de olsa, bunların başkaları tarafından izlenmesi, denetlenmesi fabrikadaki işçinin kameralarla izlenmesiyle eşdeğer sonuçları doğurabilir.⁷¹⁸ İkinci sonuç olarak gözetleyenlerin gözetimin olumsuz etkilerini hissetmelerinin sağlanarak empati yapabilmelerini sağlaması ifade edilebilir. Bu noktada Gary T. Marx’ın gözetim konusunda objektif bir bakış oluşturabilmek için sorduğu “gözetleyenlerin, gözetim uygulamasına kendileri maruz kalsa tepkileri ne olacaktır?”⁷¹⁹ sorusu gündeme getirilebilir. Emniyet Teşkilatı’ndaki gözetleyenlere yönelik uygulanan gözetim programlarının Marx’ın sorduğu bu sorunun işlevini tam olarak yerine getirdiği düşünülmektedir. Bu işlev, gözetleyenlerin aynı zamanda gözetlenenler olması sağlanarak gözetim gücünü sahiplenmelerini önlemek suretiyle iktidarlaşmalarına engel olmak olarak ifade edilebilir.

1.4. Veri Güvenliği Sorunu

Polnet, Mobese projeleri ekseninde Emniyet Teşkilatı’nın kurumsal yapısı açısından ortaya çıkabilecek risklerden birisi de bu gözetim teknolojileri vasıtasıyla toplanan verilerin güvenliğinin sağlanamaması ve bunun neticesinde ortaya çıkabilecek tehditler ve kayıplardır. Kamusal anlamda bilgi ve iletişim teknolojilerinin veri güvenliğinin sağlanamamasından

⁷¹⁷ David Lyon, *a.g.k.*, 2006, s.83.

⁷¹⁸ David Lyon, *a.g.k.*, 2001, s.71 - 73.

⁷¹⁹ Gary T. Marx, “An Ethics For the New Surveillance”; *The Information Society*, <http://www.mit.edu/gtmarx/nicolin5.html>, (Erişim Tarihi: 05.07.2013).

doğabilecek tehlikeler iki şekilde görülebilir. Bunlardan birincisi, bu projeler bünyesinde yurttaşa ait “özel” olan verilerin çalınması veya üçüncü şahısların eline geçmesi tehlikesidir. İkincisi, görevli personel tarafından bu verilerin kötüye kullanılması durumudur.⁷²⁰ Bu bölümde, belirtilen iki önemli tehlike açısından veri güvenliği sorunu değerlendirilecektir.

Yurttaşın güvenliğini sağlama amaçlı olarak toplanan verilerin güvenliğinin sağlanamayarak üçüncü şahısların eline geçmesi kurumsal olarak büyük bir itibar zedelenmesine ve yurttaşın özelde Emniyet Teşkilatı’na genelde kamu kurumlarına olan güveninde aşınmaya yol açabilir.⁷²¹ Ayrıca yurttaş açısından da çalınan verilerinin kredi kartı dolandırıcılığından kimlik bilgileri kullanılarak adına paravan şirket açılmasına, kopyalanan parmak izinin cinayet mahallinde bırakılmasından hakkındaki istihbari veriler kullanılarak kendisine şantaj yapılmasına kadar birçok riskli durum oluşabilir.

Yurttaşa ait “özel” olan verilerin çalınması veya üçüncü şahısların eline geçmesi çeşitli şekillerde olabilmektedir. Bunlardan en önemlisi bu verilerin toplanma, kaydedilme, kategorize edilme, depolanma işlemlerinin yapıldığı sistemlerdeki güvenlik zafiyetleridir. Emniyet Teşkilatı Polnet - Mobese ve diğer istihbari projelere yönelik teknik anlamda alınan güvenlik tedbirleri ilgili bölümde ifade edilmiştir. Bu sistemlere yönelik olarak ne kadar güvenlik tedbiri alınırsa alınsın sistem içerisinde mutlaka güvenlik açıkları olacaktır. Bilişim güvenliği alanında, bilgi ve iletişim sistemlerinin üreticisi olmalarından dolayı en üst seviyede görülen ABD Savunma Bakanlığı (Pentagon), NATO, NASA, CIA gibi kurumların bilişim sistemlerine bile bilgisayar korsanları tarafından sızılabilmiş, birçok önemli veri çalınabilmiş olması Polnet - Mobese projelerinin çok güvenli olduğuna yönelik söylemleri boşa düşürebilmektedir.⁷²² Nitekim Kızıl Hackerlar (*RedHack*) tarafından 2012 yılının Şubat ayında Ankara Emniyet Müdürlüğü’nün internet sitesi üzerinden sisteme girilerek ihbar yazışmalarının ve ihbar eden şahısların isimlerinin ele geçirilebilmiş olması bunu doğrular niteliktedir.⁷²³

Sistemdeki açıklar nedeniyle yurttaşın verisini tehlikeye atmamak için öncelikle Emniyet Teşkilatı bünyesindeki tüm sistemler, veritabanları, iletişim altyapıları belirlenmeli, hepsine yönelik alınacak üst düzey güvenlik tedbirleri için protokoller hazırlanmalıdır.⁷²⁴ Bu protokoller çerçevesinde sistemlerin güvenlik riskleri belli periyotlarla uzman personel

⁷²⁰ Mete Yıldız, *a.g.k*, s.318.

⁷²¹ Nigel Gilbert, *a.g.k*, s.25.

⁷²² Council of Europe, “Organised Crime Situation Report: Focus on The Threat of Cybercrime”, *Strasbourg*, 10 Eylül 2004.

⁷²³ - - - , (Erişim Tarihi:15.01.2013).

⁷²⁴ Muammer Ketizmen, *a.k*

tarafından denetlenmelidir. Ayrıca gelişen teknolojiyle tüm güvenlik açıklarının tespit edilemeyebileceği göz önünde bulundurularak sisteme sızmaya çalışan yabancı şahısları anında tespit edebilecek uyarı alarm mekanizmaları oluşturulmalıdır.

Emniyet Teşkilatı bilişim sistemlerinde veritabanını kontrol eden personel her ne kadar güvenilir olduğu değerlendirilen personel olsa da bu verileri tamamen veya kısmen kurum dışına çıkarma ihtimali olabilir. Sisteme girmeye yetkili kimselere rüşvet vermek suretiyle bu bilgilere ulaşım mümkün olabilmektedir.⁷²⁵ Örneğin, günümüzde İzmir’de devletin gizli belgelerini, çeşitli kamusal verileri eskort kızlar aracılığıyla çeşitli bürokratlardan temin ederek başka bir ülkenin istihbarat servisine kaçırdığı iddiasıyla 378 bürokratı da kapsayan bir çeteye yönelik kovuşturma yürütülmektedir.⁷²⁶ Bu somut olayda da görüldüğü üzere kamu görevlilerinin içerisinde de hata yapanlar olabilir. Bu durum Emniyet Teşkilatı personeli için de geçerlidir. Polnet, Mobese veritabanlarında bulunan verilerin çalınmasının kurumsal olarak büyük bir itibar zedelenmesine yol açabileceği ve yurttaşların kuruma olan güvenini zedeleyeceği bir gerçektir.

Bilişim sistemlerinde görevli personel eğitilmiş, teknik yetenekleri en az sisteme saldırmak isteyenler kadar yüksek olmalıdır. Sistemlerde bütün kullanıcıların yetkileri şifrelerle tespit edilmeli ve düzenli olarak işlem kayıtları (*log* kayıtları) görevli sistem yöneticisi tarafından kontrol edilmelidir.⁷²⁷ Bunlara ek olarak mümkün olduğu kadar az personel mümkün olduğu kadar az veriye ulaşabilir olmalıdır. Güvenlik faaliyetlerinin gerektirdiği personelden daha fazlası bu verilere hiçbir şekilde temas edememelidir. Bu standartlar belirlenir ve uygulanırsa personel tarafından kasıtlı olarak veya kişisel hatası nedeniyle veri kayıplarının önüne geçilebilir.

1.5. Etik Sorunlar

Gözetim faaliyetlerinin ve gözetim teknolojilerinin oluşturulmasının ortaya çıkaracağı muhtemel sorunların meydana gelmesini önlemek için hukuki düzenlemelerin yapılması gerektiği önceki bölümlerde ifade edilmiştir. Teknolojik gelişmeler paralelinde değişen ve dönüşen gözetim pratikleri karşısında zamanla bu hukuki düzenlemeler yetersiz hale gelebilmektedir. Bu noktada gözetim faaliyetlerinin ortaya çıkaracağı davranışların hangisinin “doğru” hangisinin “yanlış” ve bu davranışların arkaplanında yer alan istemlerin hangisinin

⁷²⁵ Nigel Gilbert, *a.g.k.*, s.22.

⁷²⁶ <http://www.haberler.com/askeri-casusluk-davasi-nda-yeni-belgeler-5036186-haberi/>, (Erişim Tarihi: 19.12.2013).

⁷²⁷ İsmail Tulum, *a.g.k.*, s.81.

“iyi” hangisinin “kötü” olacağını değerlendirmeyi ifade eden etik kuralların belirlenmesi ve bunların kurumsal anlamda meslek etiğine dönüştürülmesi gerektiği değerlendirilmektedir.⁷²⁸

Önceki bölümlerde de ifade edildiği üzere gözetim dünyasında bir zaruret olduğu düşünülen etik kuralların oluşturulmasına yönelik olarak Gary T. Marx bir takım faktörler belirlemiştir. Öncelikle gözetim uygulamasının gerekliliği ve bu uygulamanın istenilen hedefe ulaşmak için gerçekten geçerli sonuç verip vermeyeceği ortaya konulması gerekmektedir. Sonrasında gerekliliği sağlanan bir gözetim yönteminin bireye fiziksel ya da psikolojik zarar verip - vermeyeceği netleştirilmelidir. Eğer bireye zarar vermeyecek bir yöntemse bununla ilgili gözetlenenin izni olup - olmadığının sorgulanması gerekmektedir. Bütün bunlar tamamsa veri toplama tekniklerinin, teknolojilerinin toplumsal kurallara uygun olup olmadığı kontrol edilecektir.⁷²⁹ Marx’ın ifade ettiği bu adımları uygulama açısından toplumsal şartlar ışığında etik kuralların belirlenmesi doğru olacaktır.

Yukarıda Marx’ın belirlediği etik ilkelerin Emniyet Teşkilatı’nda gözetim faaliyetleri yürütülürken uygulanabileceği düşünülmektedir. Bu bağlamda Mobese, Polnet ve istihbari projeler çerçevesinde gözetim faaliyetleri icra edilirken bireylerin özel alanına müdahalenin istisna olduğu göz önüne alınarak öncelikle bu sistemlerin ve bunlara benzer hazırlanan projelerin varlık sebepleri sorgulanmalıdır. Güvenliği sağlama açısından etkili olmadığı, fakat bireye ait verileri topladığı değerlendirilen programlar kapatılmalı, içlerindeki veriler geri dönüşü olmayacak şekilde imha edilmelidir. Suçla mücadele ve güvenliğin sağlanması açısından gerekli olduğu değerlendirilen programlar bireye fiziksel veya psikolojik olarak zarar verip vermediği açılarından ölçülmelidirler. Bu kapsamda örneğin Polnet bünyesinde bulunan parmak izi ve diğer kriminolojik verilerin bireye zarar verme riski yüksektir. Bu verilerin çalınması, üçüncü kişilerin eline geçmesi durumlarında telafisi olmayacak sonuçlar ortaya çıkabilecektir. Bu bakımdan bir çözüm önerisi olarak kayıtlı parmak izlerine numerik kod verilip, parmak izi verileri imha edilebilir. Böylece suç mahallinden bulunan parmak izleri aynı algorithmada numerik koda çevrilerek karşılaştırma yapılabilir ve bireyin biometrik verisini kaybetme riski de ortadan kaldırılmış olur. Bireye zarar verme ihtimali düşük veriler belirlendikten sonra bu verilerin hukuka uygun olarak bireyin izni ile alınıp alınmadığı sorgulanmalıdır. Mobese kamera görüntülerinin alınmasıyla ilgili net bir hukuki zemin oluşmamış olmasına rağmen kitlesel olarak bu verilerin toplanıp kaydedilmesi etik dışı olarak değerlendirilebilir.

⁷²⁸ Server Tanilli, *a.g.k.*, s.233.

⁷²⁹ Gary T. Marx, “An Ethics For the New Surveillance”; *The Information Society*, <http://www.mit.edu/~gtmarx/nicolin5.html>, (Erişim Tarihi: 05.07.2013).

Kişisel verilerin salt kişisel ya da kurumsal menfaatler için toplanması Marx’a göre etik değildir.⁷³⁰ Bu bakımdan suçla mücadele ve güvenliğin sağlanması amaçları dışında kurumsal işleyişin hızlandırılması, görevli polis memurlarının çeşitli izin mekanizmalarını kullanmadan kendisine verilen parola ile sisteme girerek verilere anında ulaşması gibi amaçların Marx bakışında etik olmadığı gözükmemektedir.

Emniyet Teşkilatı gözetim projeleri yürütülürken yapılan tüm işlemlerin denetime açık olması ve gözetimin konusu olan yurttaşların da hem bu denetim faaliyetleri hem de kendilerine yönelik gerçekleştirilen gözetim konusunda bilgilendirilmesi gerekir.⁷³¹ Dolayısıyla gözetim faaliyetlerinde şeffaflık temel etik ilkelerden biri olmalıdır. Sonraki bölümlerde önerilen “şeffaflık raporlarının” ve “gözetleyenleri gözetlemeye yönelik örgütsel örnek yapının” bu etik ilkenin uygulanmasında önayak olabileceği düşünülmektedir.

Yukarıda ifade edilen gözetimde etik çerçevenin Emniyet Teşkilatı bünyesinde oturtulabilmesi için bunun örgütsel anlamda kabullenilmesi gerektiği düşünülmektedir. Başka bir ifadeyle gözetim faaliyetleri yerine getirilirken uyulması gereken etik kurallar meslek etiğine dönüştürülmelidir. Daha önce de açıklandığı üzere meslek etiği, doğru ve yanlış olarak kategorize edilen faaliyetlerin grup tarafından benimsendiği, bunların grup baskısıyla grup mensubu bireylere emredildiği, onları belirli bir şekilde davranmaya zorladığı, bu çerçevede kişisel eğilimleri sınırladığı kurallar bütünü olarak ifade edilebilir.⁷³²

Gözetim faaliyetleri ile ilgili Emniyet Teşkilatı bünyesinde bir meslek etiği oluşturulmasının önemi, denetim faaliyetlerinin yetersiz olduğu zamanlarda etik kurallara uymayanların grup tarafından dışlama, ötekileştirme, hakir görme gibi yaptırımlarla karşı karşıya kalarak bir anlamda denetim mekanizması rolü üstlenmesidir.⁷³³ Bu bakımdan örneğin, bir personelin Polnet bilgi sistemlerinde suç konusu ile ilgili olmayan, mesela uzun zamandır görüşmediği arkadaşının ev adresini tespit etmeye yönelik bir sorgu yapmak istemesi durumunda çevresindeki personel ona tepki gösterebilirler. Ama öncelikle bu tür davranışların doğru değil yanlış olduğunun örgütsel çevrede genel kabul görmesi gerekmektedir.

⁷³⁰ *a.k*

⁷³¹ *a.k*

⁷³² Annemarie Pieper, *a.g.k*, s.85.

⁷³³ Mustafa L. Şen, *a.g.k*, s.96.

2. Topluma ve Yurttaşla Yönelik Tehditler

“İnsanlar sonunda hapiste olduklarını anlayana kadar çok iyi korunan bir tatil köyünde olduklarını düşünecekler...”
Herbert Prantl

Yurttaş açısından Emniyet Teşkilatı’ndaki teknolojik gelişmelerin suçla mücadele boyutuyla mutlaka sağladığı olumlu tarafları vardır. Ancak yurttaşın her geçen gün Mobese kameraları ya da Polnet üzerindeki veritabanları yoluyla dijital metaya dönüştürüldüğü gerçeği de unutulmamalıdır. Bu bölümde öncelikle Emniyet Teşkilatı gözetim faaliyetlerinin varlık sebebi olarak suçla mücadele, kullanılan gözetim teknolojileri ekseninde eleştirilecektir. Sonrasında bu teknolojilerin uygulamasının toplumsal ve bireysel bazda oluşturduğu korkular, psikolojik ve sosyolojik travmalar ile özel hayatın gizliliğinin yokoluşu değerlendirilmeye çalışılacaktır.

2.1. Mobese, Polnet ve Suçla Mücadele İlişkisi

Suçları toplumsal yapıdaki iyileşmeler azaltabilir, teknoloji değil!⁷³⁴

Suç kavramı, TDK Türkçe Sözlükte yasalara aykırı davranış olarak tanımlanmaktadır. Bu bağlamda bir eylemin suç sayılabilmesi için, o eylemin yasalarca yasaklanmış eylem türlerinden biri olması gerekir. Her suçun bir faili ve failin eyleminden zarar gören mağduru vardır. Mağdur kimi zaman birey, kimi zaman bir topluluk, kimi zaman da kamu olabilir. Suç konusunu oluşturan eylemin zarar verme amacına yönelik olması ve eylem ile doğurduğu sonuç arasında bir illiyet bağı bulunması suçun manevi unsurunu oluşturur. Suç oluşturan eylem o suçu işleyenın kastından ya da kusurlu davranışından doğabileceği gibi, ihmali sonucunda da ortaya çıkmış olabilir.⁷³⁵

Polis bilimlerinde suçlar genel olarak; yaralama, adam öldürme, hırsızlık gibi suçları içine alan asayiş suçları; mafya tipi yapıların işledikleri suçları konu alan organize suçlar; illegal yollardan yurtdışından ülkeye veya ülkeden yurt dışına ürün veya yasaklı malzeme getirip götürmeyi içeren kaçakçılık suçları; uyuşturucu madde ticaretini içeren narkotik suçları; bilgi - iletişim araçlarını kullanarak işlenen bilişim suçları; silahlı olarak devlete veya millete saldıran ideolojik silahlı örgütleri içeren terör suçları olmak üzere ayrılmaktadır.

⁷³⁴ İngiltere’de Kameralı Gözetime Karşı Oluşturulan “ No CCTV” İsimli Platformun Sloganıdır. <http://www.no-cctv.org>, (Erişim Tarihi: 15.12.2013).

⁷³⁵ Ruşen Keleş, “Kente Karşı Suç”, *TMMOB Mimarlar Odası Ankara Şubesi*, Bülten 55, Ankara, Kasım - Aralık 2007, s.45.

Suçun oluşabilmesi için suç konusunu oluşturan eylemden zarar gören mağdur olması gerekir. Bu kapsamda birey - birey veya birey - örgüt ilişkisinin varlığı esasen suçun oluşmasında bir gerekliliktir. Bu ilişki bağlarının sayısı ve çeşitliliği arttıkça suç işleme riski de artış göstermektedir. Nitekim günümüzdeki olay, fail, mağdur, suç örgütü, suç çeşitliliği yükselişinde en büyük etmen; bu ilişki sayı ve türlerinin artış gösterme imkanı bulduğu kentleşme olgusudur.

Ülkemizde 1950’li yıllardan bugüne kadar artarak devam eden kırdan kente göç ile birlikte kent nüfusları hızla artmış buna bağlı olarak kentte mekansal ve sınıfsal ayrımlar, işsizlik, yoksulluk gibi birtakım sosyal ve ekonomik sorunlar baş göstermiştir. Bu sorunlar farklı sosyolojik sorunları doğurmuş ve 1970’li yıllardan sonra özellikle de 1980’lerde suç eğilimi had safhaya ulaşmaya başlamıştır. Bu yıllarda işsizliğin ve yoksulluğun sonucu olarak, işi ve ikamet edeceği bir yer olmayan kişilerin yasa dışı olaylara karıştığı ve suç işlemeye başladıkları görülmektedir. Böylelikle ülkemizde güvenlik kavramının günümüzdeki anlamda gündeme gelmesi bu dönemde olmuştur.⁷³⁶

2000’li yıllarda kent güvenliği tüm dünyada önemli bir sorun haline dönüşmüştür. Kent nüfusundaki hızlı ve kontrolsüz artış ve küreselleşmenin bir etkisi olarak kentlerdeki gelir dağılımlarındaki eşitsizlikler ile birlikte kentlerde sosyal sınıflar ve gettolaşma oluşmuştur. Bu sosyal ve mekansal ayrımlar neticesinde diğer sınıfların ekonomik varlıklarına özenme gibi nedenlerle kentsel suç ve şiddette yıkıcı bir artış gerçekleşmiştir.⁷³⁷ Bunun paralelinde de kamusal zeminde güvenlik ve suçla mücadele konuları ve çalışmaları önem kazanmıştır.

Suç esasında bir çeşit toplumsal sapmadır. TDK Türkçe Sözlükte sapma kavramı, yön değiştirmek; önceden belirlenmiş görüş, düşünüş, amaç veya davranıştan ayrılmak biçiminde tanımlanmaktadır. Toplumun varlığının sürdürülmesi birtakım değerler ve normlar üzerine kuruludur. Bu değerlerin ve normların dışındaki davranışlar norm dışı, yani toplumsal sapma olarak ifade edilmektedir. Bu kapsamda isyan, suç (cinayet, hırsızlık, rüşvet, ırza geçme, dolandırıcılık, vb.), intihar, uyuşturucu alışkanlığı, cinsel sapkınlık toplumsal sapmaya örnek verilebilir.⁷³⁸

Mobese ve Polnet sistemlerinin güvenlik birimlerince oluşturulması ve adeta bir devlet güvenlik politikası haline dönüşmesinin arkaplanını doğru okumak gerekmektedir. Güvenlik

⁷³⁶ Ela Ataç, Davut Gürbüz, “Kentsel Mekanda Gelişen Suça Müdahale Etmede Disiplinlerarası Güvenlik Politikaları”, *Polis Bilimleri Dergisi*, Cilt: 11, 2009, s.28 - 29.

⁷³⁷ a.k

⁷³⁸ Yılmaz Yazıcıoğlu, *a.g.k.*, s.111.

boyutu ile değerlendirildiğinde arkaplanda suçu önleme, suça müdahale etme ve en önemlisi suça meyilli olanların suç işlemek için alması gereken risk oranını arttırma amacı yattığı ifade edilebilir. Bu durumu açıklamak için suçla mücadeleyle yönelik ileri sürülen Rasyonel Tercih Teorisi ve Durumsal Suç Önleme Teorisinden faydalanabiliriz.

Rasyonel Tercih Suç Teorisine göre suçlular faydacıdır ve suç işlemeye karar vermeden önce kar ve zarar hesabı yaparlar. Bu hesaba göre de suçu işleme ya da işlememe noktasında kendilerine göre mantıklı bir tercihte bulunurlar. Bu bağlamda suçu işlemekle elde edecekleri fayda, yakalanma ihtimallerinden veya yakalandıklarında alacakları ceza riskinden daha fazla ise suçu işlerler. Potansiyel suçluların yapacakları kar ve zarar analizlerinde, girecekleri riskin yüksek olduğu algısını oluşturacak önleyici tedbirlerin alınmasının suç işleme güdüsünü azaltacağından dolayı suç oranlarında düşüş olması öngörülür.⁷³⁹

Bu teoriye göre suçla mücadelede suç işleme potansiyeli olan kişiler için suç işleme riskli hale getirilmeli ve suçluları motive eden unsurlara karşı tedbirler alınmalıdır. Mesela hırsızlık olaylarına karşı kamera sistemlerinin kurulması, işyerine kepenk takılması, kapıya sağlam bir kilit takılması, alarm sistemi kurulması, gece bekçileri istihdam edilmesi, polis devriye ekiplerinin arttırılması suçlular için riski arttıran ve suç işlemeye yönelik motivasyonlarını azaltan faktörlerdir. Bu kapsamda hırsızlığa meyilli şahıslar suçu işlediğinde yakalanma riskinin veya kimliğinin tespit edilmesi ihtimalinin yüksek olduğuna inanması halinde suçu işlemekten vazgeçebilirler.⁷⁴⁰

Rasyonel Tercih Teorisinin başka boyutu ise suçluların suç çeşitlerini tercihinde kar zarar hesabı yapmasıdır. Mesela Türkiye şartlarında eroin kaçakçılığı suçunun cezası oldukça ağırdır. Sigara kaçakçılığının cezası oldukça azdır ve bu suçtan dolayı mahkumiyet hemen hemen yok gibidir. Bu kapsamda bir kaçakçı eroin yerine sigara kaçakçılığı yapmayı daha karlı görebilir.

Durumsal Suç Önleme Teorisine göre ise fiziksel ve sosyal çevrede gerçekleştirilecek değişimler yoluyla suçu gerçekleştirme fırsatları azaltılarak suçun, suçlular açısından karlı bir tercih olmaktan çıkarılabileceği ve böylece suçun önlenebileceği iddia edilmektedir.⁷⁴¹ Bu bakımdan bu teori Rasyonel Tercih Teorisi ile iç içe girmiştir. Durumsal Suç Önleme Teorisi, hedef olarak seçilmesi muhtemel mal ve şahısları korumak için kullanılabileceği gibi (örneğin; vitrinde gerçek altın, elmas yerine imitasyonlarının sergilenmesi gibi), olası suçları

⁷³⁹ Halil İ. Doğan, Bilal Sevinç, “Suç Teorileri ve Şehir Güvenliği: Bitlis İliyle İlgili Genel Bir Değerlendirme”, *Polis Bilimleri Dergisi*, Cilt:13 (4), 2011, s.31.

⁷⁴⁰ a.k

⁷⁴¹ a.k, s.33.

önlemek için suç mahallerinde de kullanılabilir. Örneğin, suç işlenmesi muhtemel binaların camlarına demir parmaklıklar takılması, güvenlik kameraları yerleştirilmesi, görünürlüğü sağlayacak iç - dış aydınlatmanın kurulması gibi mekansal düzenlemelerle suça işlemeye meyilli olanların suç işlemekten vazgeçirilmesi sağlanabilir.

Günümüzde kentleşme, kapitalist düzenin hakimiyeti, toplum içinde bireylerin yabancılaşması, hızla gelişen teknoloji, kalabalık ve heterojen toplum yapısı gibi nedenlerle suç tiplerinde ve suç sayılarında geçmişe oranla hızlı bir artış olmuş, suçluların da giderek profesyonelleşmesi ile birlikte suçlar kompleks hale dönüşmüş ve uluslararası suç tipleri oluşmuştur. Bu noktada günümüz suçla mücadele birimleri, bilgi ve iletişim teknolojilerine hakim ve bunları işledikleri suçları örtbas etme aracı veya birer silah olarak kullanabilen, güvenlik güçlerinin suçla mücadele metotlarına karşı güçlü savunma metotları geliştirebilen bir suç güruhu ile karşı karşıya bulunmaktadır. Bu bakımdan güvenlik birimleri böyle profesyonelleşmiş suçlularla mücadele edebilmek, hatta proaktif polislik anlamında suç oluşmadan önce suçu önleyebilmek, suçluların yeni suç işleme metotlarını deşifre edebilmek için bilgi - iletişim teknolojilerini çok iyi bilmeli ve kullanabilmeli, bilgiye hızlı ve analitik olarak ulaşabilmelidir.

Ülkemizde özellikle son on yıllık süreçte terör, kapkaç, gasp, tecavüz gibi günlük yaşamda etkisi derinden hissedilen çok farklı suç tipleri ile özellikle büyük kentlerde sık sık karşılaşılır hale gelmiştir. Diğer taraftan cezaların yetersizliği ve caydırıcılıktan uzak olması da aynı kişilerin aynı suçları defalarca işleyebilir hale gelmesine yol açmıştır.⁷⁴² Bunun neticesinde siyasal otorite ve halk, güvenlik güçlerinin gözetim pratikleri kapsamında suçla mücadelede bilgi ve iletişim teknolojilerini sınır tanımaz şekilde kullanmasına göz yumar hale gelmiştir.

Yukarıda belirtilen süreçte suçla mücadele konusunda Emniyet Teşkilatı'nın bilgi ve iletişim teknolojilerini kullanmada kendi içerisinde adeta bir devrim yaptığı iddia edilebilir. Bu devrim sürecinde kendi rütbeli personelini ABD, İngiltere gibi gözetim teknolojilerini çok iyi kullanan ülke güvenlik teşkilatlarına uzmanlık kurslarına göndermiş; personel alırken bilgisayar mühendisi, elektronik mühendisi olan amir personel adaylarına kontenjan açarak teknik personel ihtiyacını gidermiş; topyekün meslek içi uzmanlık eğitimlerini arttırmıştır. Bu çalışmalar neticesinde Polnet, Mobese gibi profesyonel bilgi - iletişim ve gözetleme

⁷⁴² Ali Koyun, Abdullah S. Öztürk, "Toplumsal Kontrol ve Gözetim Araçlarından Olan Mobese Teknolojisinin İşlevselliği Konusunda Halkın Bilinç Düzeyi", *Sosyoloji Alanı Orta Öğretim Öğrencileri Arası Araştırma Projeleri Yarışması*, Tubitak, Bursa, 2012, s.4 - 5.

teknolojilerine sahip olmuş, ülke çapında bunları yaygınlaştırmıştır. Böylece bir anlamda suçların işlenmesinde kanunlarla sağlanamayan caydırıcılık oluşturulmaya çalışılmıştır.

Emniyet Teşkilatı bünyesinde geliştirilen gözetim teknolojilerinin suçla mücadele ilişkisini anlama açısından ülkemizde halk tarafından en hissedilir olanı olarak değerlendirilebilecek Mobese sistemini inceleyebiliriz. Mobese'nin ilk olarak Diyarbakır ilinde EGM İstihbarat Dairesi Başkanlığı tarafından kurulmuş olması, sistemin somut olarak ilk çıkış noktasının terör eylemleri ile mücadele, PKK terör örgütünün şehir yapılanması olan KCK terör örgütü üyelerinin faaliyetlerini takip etmek olduğunu göstermektedir.⁷⁴³ İlk çıkış noktası böyle olmakla birlikte zamanla tekamülünü tamamlaması kentlerde, ana caddelerde yurttaşların özgürce yürüyebilmesi, arabalarını güven içinde park edebilmesi, evinde hırsızlık korkusu olmadan ikamet etmesi hedefinde gerçekleştirmiştir. Ayrıca suça meyilli olanların içlerindeki suç potansiyelini engellemek hedefi de buna eklenmiştir.

Suç işlendikten sonra “geciken adalet adalet değildir” prensibiyle faillerin en kısa zamanda yakalanmasının sağlanması, demokrasinin ayrılmaz bir parçası olan toplantı ve gösteri yürüyüşlerinde provakatoörlük yaparak amacın dışına çıkılmasına neden olan ve masum yurttaşlara zarar veren gizli suç faillerinin ortaya çıkarılarak mağduriyetin önlenmesi, suç işlenmeden suçun önlenmesi olan proaktif polisliğin gerçekleştirilmesi; topluma, güvenli bir kentte yaşadıklarını, suç ve suçlularla mücadelede güvenlik görevlilerinin etkin çalıştıklarını hissettirerek yoğun psikolojik etki yapan “suç korkusunu” (*ing; fear of crime*) azaltma ve kamera görüş alanına giren yerlerde meydana gelen olayları gözleyerek en yakın ekibi olay yerine yönlendirerek hızlı ulaşımı sağlama gibi hedefleri de bulunmaktadır.⁷⁴⁴

Yukarıda ifade edilen Rasyonel Tercih Suç Teorisi ve Durumsal Suç Önleme Teorisi temel alındığında da Mobese sistemindeki kameraların varlığının suçların önlenmesi ve suç işleme risk grubuna girenler için caydırıcılık sağlanması açısından anlam ifade ettiği söylenebilir. “Suç işlersem polis kameradan beni fark eder ve hemen yakalar”, “polis elinde çok gelişmiş istihbarat teknolojileri var, suç işlediğim anda beni bulur” gibi düşüncelerle Rasyonel Tercih Suç Teorisinde belirtilen kar - zarar dengesinde suça meyilli kişi zararlı çıkacağını düşünebilir ve suç işlemekten vazgeçebilir.

Rasyonel Tercih Teorisinin kar - zarar dengesinde zararın ağır basabilmesi için sadece bu tip gözetleme teknolojilerinin varlığı yeterli olmayabilir. Kişi suç işlediğinde son derece

⁷⁴³ Erin Çoban, *a.g.k*

⁷⁴⁴ İbrahim Cerrah, “Polis”, *Almanak Türkiye: Güvenlik Sektörüne Demokratik Gözetim*, Ed. Ümit Cizre, Tesev Yayınları, İstanbul, 2005, s.94.

gelişmiş olan bu gözetleme teknolojileri ile kısıvrak yakalansa bile yargılamada aldığı ceza yetersiz kalıyorsa bu teknolojiler de bir anlam ifade etmeyebilir.⁷⁴⁵ Örneğin, sigara kaçakçılığı suçunu işleyen kişiler yargılandıklarında genelde para veya çok az hapis cezası almakta, yargılama sürecinde de tutuklanmamaktadırlar. Dolayısıyla bir aylık süre içerisinde aynı şahıslar sigara kaçakçılığından dolayı üç - dört kez yakalanabilmekte ve yine serbest kalıp kaçakçılık yapmaya devam etmektedirler.

Suç soruşturması yürütülürken delilden sanığa ulaşma felsefesi paralelinde hareket eden güvenlik birimleri suç mahallinde bırakılan saç teli, deri kırıntısı, kan, meni, sigara üzerindeki tükürük, kıyafet parçaları, ayakkabı izi, parmak izi gibi biyo-kimyasal delilleri toplamak suretiyle bir inceleme faaliyeti yürütür. İşte bu faaliyet polisin sadece suçu önlemek için değil suç sonrası faillere ulaşmak için de gözetim faaliyetlerinden faydalandığını göstermektedir. Nitekim suç mahallindeki güvenlik kameraları, Mobese kameraları vasıtasıyla olay anındaki görüntüler taranarak suçla ilgisi olabilecek şahıslara ulaşılmaktadır.⁷⁴⁶

Mobese sistemi aslında bir anlamda sokak polisliğinden masabaşı polisliğine geçiş sürecini simgelemektedir. Zira bu sistem kurulmadan önce polisin sorumlu olduğu muhitlere güvenlik açısından hakim olunabilmesi için mahalle bekçiliği, yoğun devriye görevleri, sivil görevli polis memuru gibi farklı uygulamalar kullanılmaktayken; mevcut durumda şehrin her tarafına kurulmuş ve 7 gün 24 saat görevli polis memurlarınca takip edilen Mobese kameraları bu tip uygulamaları gereksiz kılmıştır. Zira hem görevli polis memurunun gözle takibi hem de sistemin alarm verebilme özelliklerinden dolayı bu uygulamalardan kat kat daha fazla oranda şehrin güvenlik hakimiyeti sağlanabilmektedir.⁷⁴⁷

Eskişehir’de yerel bir televizyon kanalı Eskişehir’e Mobese sistemi kurulması için bağış kampanyası başlatmış, işadamları ve halkın önemli desteğiyle beklenenin üzerinde bir bağış toplanarak Mobese sistemi kente kurulmuştur. Yerel bir gazetede kampanyaya ilişkin

⁷⁴⁵ EGM Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, *2009 Faaliyet Raporu*, Ankara, 2010, s.78.

⁷⁴⁶ Julie K. Petersen, *a.g.k.*, s.68.

⁷⁴⁷ Lyon tarafından anlatılan bu olay sokak polisliğinden masabaşı polisliğine geçişe güzel bir örnektir: “Ocak 2001’de, Ontario’nun 401 nolu Otoyolu’nda değişik bir araba kovalamacası oldu. Çalınan araç haber verildiğinde, polis imalatçıyla, aracın üstünde nasıl bir ekipman olduğunu anlamak amacıyla bağlantıya geçti. Arabada küresel yer belirleme uydusu (GPS) dolaşma sistemi olduğunu öğrendiklerinde, aracı izleme görevi kolaylaştı. Polis, arabanın faaliyetlerini ekranlarında gözledi ve hırsız Tim Horton’un Donot Bar’ın otoparkında kayıp aracın yanına park ederek tutuklandı. Elektronik araba kovalamacası, otoyolda yüksek hız aksiyonu içerenlerden daha az riskliydi.” David Lyon, *a.g.k.*, 2006, s.75.

yer alan, “Haydi Eskişehirli Kentine Sahip Çık” başlıklı bir makalede, kampanyanın amacı şöyle ifade edilmektedir:⁷⁴⁸

“Son günlerde şehrimizde meydana gelen araç kundaklama olaylarının artmaması, daha güvenli ve daha huzurlu bir Eskişehir için şehrimizin güvenliği açısından çok büyük önem taşıyan (MOBESE) kameralı takip sistemini şehrimize kazandırmak için... yardım kampanyası başlattık.”

Bu örnekte halkın, Mobese sistemine özel hayatın gizliliğini ihlal ediyor gibi söylemlerle karşı çıkmak şöyle dursun sistemin kurulmasını tıpkı bölgeye bir okul yapılmasını ister gibi desteklediklerini görmekteyiz. Esasında bu durumun gerekçesini “suç korkusu”⁷⁴⁹ kavramı net bir şekilde açıklamaktadır. Suç korkusu, Kenneth Ferraro tarafından “duygusal korku veya endişe reaksiyonu” olarak ifade edilmiştir.⁷⁵⁰ Esasında suç korkusu, yargı birimlerinin suç faillerine yönelik yeterince caydırıcı beceri ve güce sahip olmadığı kanısına halkın sahip olmasından kaynaklanmaktadır. İnsanlar bu psikoloji içerisinde ve korkularının etkisiyle kapılarına fazladan kilit taktırmakta, evlerinde savunma amaçlı silah ve benzeri gereçler bulundurmakta, apartmanlarına kamera ve alarm sistemleri taktırmakta ve hatta 7 gün 24 saat esasına göre çalışan özel güvenlik görevlileri kiralamakta ve bütün bunlar için azımsanmayacak meblağlarda harcamalar yapabilmektedirler. Bu noktada Mobese sistemini desteklemeleri de benzer bir şekilde suç korkusunun halktaki yansıması, hatta çaresizliği olarak ifade edilebilir.

Mobese ile ilgili halkın içerisinde yukarıda belirtilen şekilde düşünenler varken siyasetçilerin de benzer görüşte oldukları görülmektedir. CHP İstanbul Milletvekili Hasan Fehmi Güneş’in 19 Aralık 2006 tarihinde Meclis Kürsüsünde yapmış olduğu aşağıdaki konuşmada suçla mücadeleyi gerekçe göstererek Mobeseyi sorgulamadan kabul ettiğini göstermektedir.⁷⁵¹

“...Suç, bir geçim kaynağı, bir kazanç aracı, bir meslek olma yolundadır. İnsanlıktan çıkmış, hayvanlaşmış, canavarlaşmış acımasız kişiler, mafyalaşmış eli kanlı çeteler şehir sokaklarında bu mesleği adeta icra etmektedirler. Kamu düzeninde bir otorite yitimi söz konusudur, toplumun suç toplumuna sürüklenişi söz konusudur. Önleyici otoritenin silikleşmesi, suç eğilimi üzerindeki caydırıcı baskıyı zayıflatmakta, suç dürtüsünün eyleme yansımaları kolaylaştırmaktadır. Önlenemeyen her eylem, her suç, yeni eylemleri çağırarak, yeni suç işleme eşiğindeki kişileri yüreklendirmektedir. Resmî rakamlar bunu çarpıcı boyutlarda sergilemektedir. Eylem sonrası aşamadaki aydınlatma, yakalama sayıları da caydırıcı düzeyde değildir, caydırıcı olmamıştır...”

...Sayın milletvekilleri, çağımızın en çarpıcı niteliği sayılan hızlı değişim olgusu, yaşamın tüm alanlarını etkilemekte ve yeni boyutlar getirmektedir. Bu arada, ahlak anlayışını, kişinin suçtan sakınmaya yönelik kendini sınırlama disiplinini de aşındırmaktadır. Yeni suç türlerinin, yeni suçlu profillerinin, yeni

⁷⁴⁸ http://www.ikieylul.com.tr/yazar_goster.asp?ne=y48&sira=4312, (Erişim Tarihi: 22.05.2013).

⁷⁴⁹ Kenneth Ferraro, *Fear of Crime: Interpreting Victimization Risk*, State University of New York Press, Albany, 1995, s.23., Akt. Şener Uludağ, “Vatandaşların Suç Korku (Güvenlik Endişesi) Seviyesine Etki Eden Faktörler ve Alınabilecek Önlemler: Malatya Örneği”, *Polis Bilimleri Dergisi*, Cilt:12 (1), 2010, s.3.

⁷⁵⁰ a.k

⁷⁵¹ TBMM Tutanak Dergisi, *CHP Grubu Adına İstanbul Milletvekili Hasan Fehmi Güneş’in Konuşması*, Dönem 22, Cilt 141, Yasama Yılı 5, 37. Birleşim, 19 Aralık 2006.

suç örgütlenmelerinin, sosyal, ekonomik ve diğer nedenlerin yanı sıra, onlardan ayrı olarak, bu sürecin de ürünü olabileceği iddiasının bilimsel bir yaklaşımla ve ciddiyetle araştırılması gerekir. Eğer böyle ise, şikayetçi olduğumuz suç ve suçlu sayısındaki artışın gerçek nedenini anlamak için başkalaşma, hat-ta başkalaştırma dayatan değişimi doğru algılamak ve doğru okumak zorundayız. Koşullar ve öncelikler değişirken, yönetim ve güvenlik alanında eskimiş yöntem ve önlemlerle yetinmeyiz, yeterli sonuçlar alamayız. Değişimin ürünü olan sorunları, değişmemenin ürünü olan eskimiş ve geçersiz yaklaşım ve yöntemlerle çözebileceğimizi sanmak, çözümsüzlüğe tutsaklıkla eş anlamlıdır. Kimi kentlerde kurulan ya da kurulmakta olan MOBESE ve benzeri örgütler, görüntüleme ve izleme ağı, yeni koşullarla ihtiya-cı karşılamaya dönük atılımlar olarak değerlendirilmelidir ve desteklenmelidir...”

Diğer taraftan dönemin İçişleri Bakanı Abdülkadir Aksu’nun aynı oturumda yaptığı aşağıdaki konuşma da suçla mücadele amacıyla Mobesenin tüm ülkede yaygınlaştırılmasına devletin en üst düzeyinde sahip çıkıldığını göstermektedir:⁷⁵²

“...Değerli arkadaşlarım, suç ve suçlulukla mücadelede bilişim ve iletişim teknolojileri kullanılarak alan hakimiyetinin sağlanması da bir zorunluluktur. Bunun bilincinde olan güvenlik teşkilatlarımız da tekno-lojiyi en üst seviyede kullanmayı amaç edinmişlerdir. Bu kapsamda bilişim teknolojileri kullanarak, suç ve suçlunun azaltılması kapsamında da önemli projeleri hayata geçirdik. İstanbul’da uygulamaya başla-dığımız MOBESE Projemiz ve bunu diğer bütün illere yaygınlaştırmaya çalışıyoruz. Bu yıl içerisinde on altı ilimizde bu sistemin kurulması çalışmalarını başlattık...”

Mobesenin kurulduğu tarihten bu yana dördüncü kuvvet olarak nitelenen medya da genel olarak bu kameralı kent güvenlik yönetim sistemlerini desteklemiştir. Günümüzde hemen hemen bütün yazılı ve görsel medyada Mobese, suçla mücadelede bir kurtarıcı olduğu, varlığı olmazsa faillere ulaşılamayacağı ifade edilerek kutsanmaktadır. Nitekim buna 23 Ocak 2007 tarihli Hürriyet Gazetesinde yayımlanan aşağıdaki “Kameralar olmasaydı...” başlıklı makaleden kesit örnek niteliğindedir:⁷⁵³

“İstanbul’un göbeğinde bir cinayet işlendi. Katil, Hrant Dink’i vurup kaçtı. Eğer o bölgede bir banka güvenlik kamerası olmasaydı ve suratı tabak gibi ortaya çıkmasaydı, yakalanması mümkün olacak mıydı?.. Kentlerin ana caddeleri, işyerlerinin ve bankaların yakın çevreleri... Bu gibi yerlerde suç işleyenler kameradan yakalanıyor. Ara sokaklarda, kameralardan uzakta suç işleyenlerin yakalanması genelde mümkün olmuyor. Özellikle büyük kentlerde soyulmayan ev ve işyeri, kapkaça maruz kalmayan yurttaş neredeyse kalmadı. O suçlular niçin yakalanmıyor?.. Çünkü çevrede kamera yok! Polis yılgın, çaresiz. Suçların fazlalığı ve yetkilerinin AB yasalarıyla budanmış olması nedeniyle iş göremiyor. Sonuç: Kameraya yakalanan soyguncu, hırsız vesaire yakalanıyor.”

Halk-medya-siyasetçiler-güvenlik güçleri tarafından varlığı her şeye rağmen kabul edilmiş olan Mobesenin varlık nedenlerinden olan suçların azalması gerçekten söz konusu mudur? Bu soruyu cevaplamak için ayrıntılı bir çalışma yapmak gerekir. Fakat örnek olarak Ankara ilini incelersek, elde edilen istatistikler neticesinde Aralık 2010 tarihinde hizmete giren Mobese sisteminin yapmış olduğu 21 farklı noktadaki denetimler sonucunda; 2010 yılının Aralık ile 2011 yılının Eylül ayları arasındaki zaman periyodu içerisinde, yapılan kırmızı ışık ihlallerinde %61 oranında, hırsızlık olaylarında da %8 oranında azalma olduğu

⁷⁵² TBMM Tutanak Dergisi, İçişleri Bakanı Abdülkadir Aksu’nun Konuşması, Dönem 22, Cilt 141, Yasama Yılı 5, 37. Birleşim, 19 Aralık 2006.

⁷⁵³ <http://hurarsiv.hurriyet.com.tr/goster/haber.aspx?id=5822235&tarih=2007-01-23>, (Erişim Tarihi: 22.05.2013).

ifade edilmektedir.⁷⁵⁴ Ülkemizde bilimsel yazında bu oranları doğrulayacak farklı çalışmalara rastlanmamıştır. Diğer ülkelerde yapılan araştırmalar incelendiğinde aynı başarı oranının dünya genelinde gözükmediği görülmektedir. Örneğin kameraların suçların azalması ve faillerin yakalanması konusundaki etkisiyle ilgili olarak Kanada Özel Yaşamı Koruma Komiseri George Radwanski, Büyük Britanya uygulaması temelinde Türkiye’deki durumun tersine suç oranlarında artış görüldüğünü ifade etmiştir.⁷⁵⁵

“Londra’da 150 bin civarında kamera var. Geçen yıl (2001 yılından söz ediyor E.C.) daha önce görülmemiş sayıda kamera konuldu. Tahmin edin bakalım ne oldu? Londra sokaklarında suçluluk oranı yüzde 40 artış gösterdi. Komiserliğimiz, İngiltere’de, Sheffield Üniversitesi Hukuk Fakültesi Kriminoloji Profesörü Jason Ditton’un bilgisine başvurdu. Prof. Ditton, Açık hava video gözetlemesinin etkinliği konusunda çok geniş biçimde tanınan, belki de dünyanın en büyük uzmanıdır. 1993 yılından beri konuyu incelemektedir. Diyor ki; Kapalı devre televizyonla sokakların gözetlenmesi suretiyle suçluluğun azaltıldığını ya da yok edildiğini gösteren inandırıcı hiçbir kanıt yoktur.”

İngiltere, Amerika, İspanya gibi ülkeler gözetim teknolojilerini zirvede kullanan ülkelerdir. Ancak 11 Eylül 2001’de New-York’ta İkiz Kulelere düzenlenen terörist saldırı, 7 Temmuz 2005 tarihinde Londra Metrosuna yapılan bombalı saldırı, 11 Mart 2004’te Madrid’de tren garına yapılan bombalı saldırılar güvenlik tabanlı gözetim teknolojilerinin çok da güvenliği temin edemediğini göstermektedir. Nitekim bu ülkelerin polis teşkilatları, gizli servisleri mesailerinin yüzde doksanını bu tip terörist eylemlere karşı gözetim yapmak için harcarken, bombalı saldırı gibi birçok hata yapmaya müsait hazırlık gerektiren saldırıları bile bertaraf edemedikleri açık ve net biçimde ortaya çıkmıştır.

Çeşitli polis kaynaklarında “Mobese kamera sisteminin iline kurulduğundan beri suçunun yüzde oranında işlenmesi azaldı.” gibi çıkarımlarda bulunmaktadır. Ancak böyle bir tespit esasında oldukça zordur. Çünkü suçun doğası ve çevresi gereği bir suç faaliyetinin oluşmasında sosyolojik, ekonomik, çevresel, demografik, psikolojik gibi birçok faktörün etkisi bulunmaktadır. Bütün bu faktörlerdeki gelişim ve değişim oranlarını (tespit etmek çok zor) saptamadan salt Mobese sisteminin şehre kurulmasından sonraki dönem ile önceki dönemin suç oranlarının karşılaştırılması doğrudan gerçekleri yansıtmamaktadır.

Daha önce de ifade edildiği üzere suç, esasında toplumsal sapmanın türlerinden birisidir. Mobese bu tip toplumsal sapmalarla mücadele amacıyla oluşturulmuş iken, kendi varlığı toplumsal sapmaların kaynağını oluşturabilecek niteliktedir. Bu bakımdan sistem ontolojik olarak amacına aykırıdır. Nitekim insanların sürekli kameralar altında yaşamaya zorlanması, evinden çıktığı andan itibaren kendisini “Biri Bizi Gözetliyor Evinde” gibi

⁷⁵⁴ <http://ankara.pol.tr/kgys/index.php>, (Erişim Tarihi: 22.09.2013).

⁷⁵⁵ Enis Coşkun, “Amaç Gözetleme mi, Güvenlik mi?”, <http://izleniyoruz.50webs.com/oku8.html>, (Erişim Tarihi: 02.03.2013).

hissetmesi onlarda psikolojik, sosyolojik derin yaraların oluşmasına yol açabilecek; bu oluşan yaralar, deformasyonlar neticesinde de yeni suçlular ve yeni suç tipleri ortaya çıkabilecektir. Sistem güvenlik için oluşturulmuş olsa da aslında toplumdaki herkesi ve her şeyi güvenilmez yapmaktadır; herkes potansiyel suçlu, her şey düzen ve huzur bozucu bir tehdit olarak değerlendirilmektedir.⁷⁵⁶ Mobesenin çıkış noktası, amaçları iyi niyetli olsa da Türkiye’de gözetim toplumuna giden yolda ister istemez katalizör görevi üstlenmektedir. Zira bireysel hak ve özgürlükler ile mahremiyetin ihlali, totaliter rejim tehlikesi, meşruiyet problemleri gibi sorunsallar içermektedir. Özellikle kişilerle ilgili verilerin kimler tarafından toplandığı, ne zaman toplandığı, nerede saklandığı, ne amaçlarla kullanıldığının bilinmemesi gözetim toplumu öngörüsünü doğrular niteliktedir.

Mobese kameralarının her ne kadar insanların yoğun olduğu, suç işleme ihtimalinin yüksek olduğu geçiş güzergahlarına konulduğu ifade edilse de belli bir süre sonra suç işleme yoğunluğunun kamera olmayan diğer yerlere kayması durumunda oralara da kameralar konulacağı bir gerçektir. Nitekim İngiltere’de durum aynen böyle olmuş ve belli bir süre sonra kameralar ülkenin her köşesine yerleştirilmiştir. İngiltere’de 2013 yılında İngiltere Güvenlik Sanayi Otoritesi (*Ing; The British Security Industry Authority*) tarafından yapılan bir araştırmada her 11 kişiye bir kamera düştüğü tespit edilmiştir.⁷⁵⁷ Türkiye’deki gözetimin gelişim seyri de İngiltere’ye benzediğinden dolayı orta vadede kameraların her yerde olacağı düşünülmektedir. Sürekli bir gözün bir yerlerde sizi takip ettiği izlenimi insanların özgür hareketlerine vurulan bir kelepçe, özel hayatlarının gizliliğini bir ötelemedir. Bunun bir ileri aşaması George Orwell’in *Bin Dokuz Yüz Seksen Dört* kitabında bahsettiği her şeyi kontrol eden, yönlendiren gizli bir el olan “*Big Brother*”ın varlığının toplumca kabullenilmesidir ki bu durumda devlet bir açıdan tanrılaştırılmaktadır. Bu anlayış paternalist devlet anlayışını körükler mi bilinmez; ama şu bir gerçek ki yurttaşlar kendilerini daima gizli bir huzursuzluk içinde hissedeceklerdir.⁷⁵⁸

Mobesenin yeni nesil bilgi ve iletişim teknolojilerine de kolaylıkla eklenilebilir bir teknolojik altyapı ile hazırlanmış olması da endişe vericidir. Örneğin, İngiltere’de özellikle Londra’da dijital veri bankasındaki verilerle karşılaştırmak üzere “*Mandrake*”⁷⁵⁹ adı verilen bir yüz tanıma sistemi kullanılmaktadır. Polis otoritelerince istenildiğinde buna benzer yüz tanıma sistemleri hızlı ve kolay bir şekilde Mobese teknolojisine entegre edilebilecektir.

⁷⁵⁶ İpek Görgün, *a.g.k.*, s.1.

⁷⁵⁷ <http://www.telegraph.co.uk>, (Erişim Tarihi: 08.06.2013).

⁷⁵⁸ Zygmunt Bauman, *a.g.k.*, 1998, s.246.

⁷⁵⁹ David Lyon, *a.g.k.*, 2006, s.117.

Böylece suçla mücadele gerekçesiyle Mobese gözetimi biometrik gözetime evrilecektir. Daha önce de ifade edilen Microsoft tarafından yeni geliştirilmiş olan insanların mimiklerini, hareketlerini analiz ederek profillemeye yapan ve bunda da %80 gibi büyük oranlarda doğruluk başarısı olan “*Kinect Sensor*” sistemi geliştirilmiştir.⁷⁶⁰ İstenildiğinde tüm ülkede yer alan Mobese kameralarına bu sensör sistemi entegre edildiğinde “mimiklerimiz” bile suça meyilli olup olmadığımızı anlamak için analiz edilebilecektir.

Sonuç olarak mevcut durumda Mobese sisteminin ve buna benzer veri toplama - analiz sistemlerine sahip olan Polnetin güvenlik boyutuyla suçlarla mücadelede ve toplumdaki suç korkusunu pasifize etme anlamında etkili olduğuna yönelik bilimsel bir ifade kullanılamamaktadır. Ancak bireysel ve toplumsal mahremiyetin zarar görmesine neden olduğu ve siyasal otoritenin halk üzerinde bir denetim aracı olduğu önceki bölümlerde ispatlanmıştır. Bütün bunlara rağmen bu tür sistemlerin varlığını devam ettirme sebebi halkın bu sistemlerden elde edilecek faydanın ödeyecekleri bedelden daha fazla olacağına inanmalarından kaynaklanmaktadır. Medya, siyasiler ve iktidar söylemleriyle halk bu sistemlerin suçla mücadelede etkili olduğuna inandırılmıştır. Neticede suçun toplumsal bir vaka olarak çok boyutlu girift bir yapısı bulunduğu, onunla mücadelenin teknoloji ile değil, toplumsal iyileştirmelerle olacağı unutulmamalıdır.

2.2. Paranoyak Toplum

Mobese başta olmak üzere Emniyet Teşkilatı’ndaki bilgi ve iletişim teknolojilerinin yurttaşlar üzerinde oluşturduğu psikolojik olumsuz etkilerin varlığının hissedilir derecede çok olduğu düşünülmektedir. Bu psikolojik olumsuz etkilerin başında yurttaşların “büyük ölçekte dünyanın, küçük ölçekte de Türkiye’nin, yaşadığı şehrin çok tehlikeli bir yer olduğu” düşüncesine yönlendirilmeleri gelmektedir.

İnsanları çevrenin güvensiz ve tehlikeli olduğu düşüncesine özellikle çevredeki kameraların varlığı yöneltmektedir.⁷⁶¹ Her ne kadar güvenliği sağladıkları, suç oluşmadan önce suçu önledikleri, suçluların hemen yakalanmalarını sağladıklarına yönelik genel inanç olsa da aslında bireye sürekli birazdan kapkaça maruz kalabileceğini, arkasından her an birisinin gelerek cinsel tacizde bulunabileceğini, köşe başını döndüğünde bomba patlayabileceğini, ilerideki bankadan silahlı soyguncuların çıkabileceğini; yani kameraların varoluş nedenlerini hatırlatmaktadır. Dolayısıyla her dükkanın kapısında bulunan kameralar, köşe başlarında yer alan Mobese kameraları tehlike ikaz işaretleri gibi bir fonksiyon icra

⁷⁶⁰ Mirela Popal, *a.g.k.*, s.1.

⁷⁶¹ “Do CCTV Cameras Make Us More Paranoid?”, <http://sciencefocus.com>, (Erişim Tarihi: 17.12.2013).

etmektedir. Durumu betimleme açısından sokağınızdaki kameralar yerine büyük ve gösterişli “Dikkat Ölebilirsin”, “Dikkat Hırsız Var”, “Dikkat Silahlı Saldırı Var”, “Dikkat Sapık Var” gibi işaret levhalarının olduğunu düşünün; işte kameralar bu işaret levhalarında yazanları bireyin bilinçaltına sürekli pompalamaktadır.

Mobese kameralarının bireylerde oluşturduğu bu algıyı medya organları da yaptıkları yayınlar yoluyla pekiştirmektedir. “Katil zanlısı Mobese kamerasından kaçamadı”, “Azılı kapkaç şebekesi Mobese’ye yakalandı”, “Canlı Bomba Mobesede” gibi spot haberlerle bir taraftan Mobese kameraların önleyiciliğine vurgu yapılırken diğer taraftan da “Mobesenin olduğu yerlerde aynı zamanda suç var” düşüncesi salınarak gözetlenen alanlarda suçun ne kadar yaygın olduğu bir şekilde ifade edilmektedir. Bu bakımdan Mobese kameralarının arkaplanda çaldığı müzik hep korku çanlarının sesidir.

Bireylerin bilinçaltlarına sürekli pompalanan “suça maruz kalma” korkusu onların sürekli yersiz bir şekilde “her an saldırıya uğrayabilirim” paranoyasıyla hareket etmelerine yol açmaktadır.⁷⁶² Bu bakımdan bir bölgede işlenen suç oranıyla, bireylerde oluşan suça maruz kalma paranoyası endeksleri farklılık göstermekte, çoğu zaman işlenen suç oranlarından yüksek bir suç paranoyası oranı çıkmaktadır.⁷⁶³ Bu bağlamda ülkemizde Mobese gözetiminin yaygın yapıldığı bölgeler ile etkin bir şekilde kullanılmadığı bölgelerdeki suç paranoyası endekslerinin ölçümüne yönelik çalışmalar yapılması gerektiği değerlendirilmektedir.

Mobese kameraları ve diğer gözetim araçlarının yurttaş üzerinde oluşturduğu başka bir rahatsızlık da kişinin tehlikelere ve işlenebilecek suçlara karşı kendisini bu gözetim araçlarının koruduğu, bunlar olmadığı takdirde başının belada olacağı algısı içinde olmasıdır.⁷⁶⁴ Nitekim günümüzde insanlar gece saatlerinde Taksim, Kızılay gibi gözetim faaliyetlerinin yoğun bir şekilde uygulandığı bölgelerde, buraların 7 gün 24 saat gözetlendiğini bildiği için rahat bir şekilde dolaşabilirken, kameraların olmadığı ara sokaklarda aynı saatlerde dolaşmaya korkabilmektedir. Halbuki örneğin, cinsel taciz ya da kapkaç olaylarının sayısına yönelik bir araştırma yapılırsa ortaya çıkan sayının kamera ile gözetlenen bu yerlerde, kamerasız yerlere oranla daha çok olacağı görülecektir. Zaten kameraların buralara yerleştirilme amacı da suç işleme ihtimalinin yüksekliğinden kaynaklanmaktadır. Dolayısıyla mevcut durumda kamera olan yerlerde kameranın varlığı o

⁷⁶² a.k

⁷⁶³ <http://www.abs.gov.au/websitedbs/c311215.nsf/web/Crime+Victimisation+in+my+state>, (Erişim Tarihi: 17.12.2013).

⁷⁶⁴ Steven Poole, “Fear of The Unknown”, *The Guardian*, 10.01.2009. www.theguardian.com, (Erişim Tarihi: 17.12.2013).

bölgelerin daha tehlikeli olmasından kaynaklandığı ifade edilebilir. Diğer taraftan yetkililer buralardan güvenlik kameralarının tamamen kaldırıldığını, hiçbir şekilde gözetim faaliyetinde bulunmayacaklarını açıklasalar aynı korkunun bu bölgeler için de geçerli olacağı düşünülmektedir. İşte yurttaşta hasıl olan bu endişe başlı başına bir ruhsal bozukluk belki belli oranda şizofrenik bir davranışın göstergesi olabilir.

Önceki bölümlerde gözetim toplumu göstergelerine sahip olduğu ifade edilen ülkemiz genelinde ve Emniyet Teşkilatı özelinde gözetim araçlarıyla donatılmanın normalleştiği ifade edilmişti. Bu kapsamda Emniyet Teşkilatı'nda kameralı gözetim, telefon dinleme, fiziki ve teknik takip gibi gözetim teknolojilerinin etkin bir şekilde kullanıldığı ifade edilebilir. Bu yoğun gözetim uygulamalarından yurttaş açısından doğan başka bir olumsuzluk da onlarda oluşan sürekli gözetlenme paranoyasıdır. Özellikle son yıllarda yapılan operasyonlarda medyada sürekli olarak “polisin fiziki ve teknik takibi neticesinde...”, “güvenlik güçlerinin yaptığı telefon dinlemelerinde...” gibi ifadelerin yaygın bir şekilde kullanılması sonucunda suça karışmamış yurttaşlarda bile “acaba benim telefonum da dinleniyor mu?” gibi sürekli gözetlendiği yönünde paranoyak algı oluşmuştur.⁷⁶⁵

2008 yılında EGM Kaçakçılık ve Organize Suçlarla Mücadele (KOM) Daire Başkanı Ahmet Pek İl KOM Şube Müdürleri ile yaptığı toplantıda şu ifadeleri ile bu tabloyu teyitlemiştir.⁷⁶⁶ “Telefon dinlemesi konusunda toplumsal paranoya oluştu. Sokaktaki simitçi bile ‘telefonum dinleniyor, bu konuları telefonla konuşmayalım’ diyor.” İşte bu durum gözetim toplumunu ifade etmek için Foucault'nun kullandığı panoptikon metaforunun temelinde yer alan sürekli gözetlenme şüphesi ile örtüşmektedir.⁷⁶⁷ Nitekim panoptikonda da gözetleme kulesinde bir gözetleyeninin olmasına gerek yoktur. Mahkumlarda sürekli gözetlendikleri düşüncesini oluşturmak yeterlidir.

2.3. Özel Hayatın Gizliliği Sorunu

Gözetim teknolojilerinin yurttaş ekseninde ortaya çıkardığı en büyük yıkım mahremiyet; yani özel hayatın gizliliği alanında olmaktadır. Özel hayatın gizliliği içerisine yurttaşın kişisel verilerinin gizliliği ve faaliyetlerinin takip edilmesi girmektedir. Bu noktada ülkemizde yurttaşlarla ilgili devletin elinde bir veri ambarı olduğu aşikardır. Mernis projesi yoluyla yurttaşın kimlik, adres bilgileri gibi kendine has bilgileri kütük halinde saklanırken, Polnet tabanlı kullanılan trafik tescil, pasaport, GBT gibi sistemlerle ona dair telefon

⁷⁶⁵ Kirstie Ball, Frank Webster, *a.g.k.*, s.2.

⁷⁶⁶ 18.12.2008 Tarihli “Dinleme Otomatiğe mi Bağlandı?” Başlıklı Milliyet İnternet Gazetesi Haberi., <http://siyaset.milliyet.com.tr>, (Erişim Tarihi: 18.12.2013).

⁷⁶⁷ Michel Foucault, *a.g.k.*, 2003, s.87 - 88.

numarası, araç bilgileri, suç kayıtları gibi diğer bilgiler toplanmaktadır. Bunun yanı sıra yine Polnet üzerinden yürütülen istihbari projeler yoluyla bireye ait olan daha özel bilgiler, Mobese projesiyle de bireyin günlük faaliyetlerine dair veriler depolanmaktadır.

Emniyet Teşkilatı dışındaki diğer kurumların e-devlet yoluyla, MİT gibi diğer istihbarat birimlerinin istihbari çalışmalarla yurttaşan topladığı veriler de birlikte düşünüldüğünde, bireyin özel alanına ait çok fazla verinin devlet kurumlarının elinde olduğu görülmektedir. Bütün bu verilere alışveriş mağazaları, bankalar, özel dedektiflik şirketleri gibi özel kuruluşların topladığı veriler de eklendiğinde korkutucu bir tablo ortaya çıkmaktadır. Bu eksende veri toplama birimlerinin bu kadar çeşitlilik gösterdiği, verilerin korunmasına dair somut düzenlemeler getiren yasal düzenlemelerin olmadığı ve bu birimlerin topladıkları verileri ne yaptıkları bilinmezliğinde ülkemizde yurttaşların mahremiyetinin güvenli bir çizgide olduğunu söylemek doğru olmayacaktır.

2013 yılının Şubat ayında TBMM’de yasa dışı dinlemeleri araştırmak üzere Telekulak Araştırma Komisyonu oluşturulmuş, Komisyon istihbari faaliyetlerde bulunan Emniyet Teşkilatı, MİT, Jandarma Genel Komutanlığı birimlerine yönelik incelemelerde bulunmuş ve 2013 yılının Haziran ayında bir raporla çalışmalarına son vermiştir. Bu raporda ülkemizde mevcut durumda gözetim faaliyetleri yürütülürken mahremiyetin ihlal edildiğine yönelik tespitler bulunmaktadır. Raporda kişisel verilerin korunmasına yönelik kanuni düzenlemeye ihtiyaç olduğu ifade edilerek mevcut durumda yurttaşın ait verilerin gözetim malzemesi olarak kullanılmasını düzenleyen yasal zeminin eksik olduğu kabul edilmiştir. İnternet üzerinden yapılan denetlemeler için yasal düzenleme yapılması gerektiği ifade edilerek internet üzerinden yapılan gözetim faaliyetlerinin kontrol dışı olduğu; Emniyet ve Jandarma istihbaratını İçişleri Bakanlığı Mülkiye Teftiş Kurulu’nun, MİT’i de Başbakanlık Teftiş Kurulu’nun denetlemesi gerektiği ifade edilerek gözetleme yapan birimlerin denetim dışı olduğu kabullenilmiştir. Ayrıca dedektiflik faaliyetlerinin TBMM gündemine yeniden taşınarak yasal bir altyapıya ve standartlara kavuşturulması istenerek özel istihbarat faaliyetleri yürüten dedektiflik müessesesinden devletin bihaber olduğu da ortaya konulmuştur.⁷⁶⁸

Meclis Telekulak Araştırma Komisyonu Başkanlığını yapmış olan Zeyid Aslan, yapılan incelemeler çerçevesinde Mobese ve diğer kameraların özel hayatın gizliliğini ne

⁷⁶⁸ 07.06.2013 Tarihli “Telekulak Komisyonu: MİT’i Başbakanlık Teftiş Kurulu Denetlesin” Başlıklı Radikal Gazetesi Haberi.

kadar tehlike altında tuttuğunun farkına varmış ve Mobese kameralarının kaldırılması gerektiğini savunmuştur. Bu farkındalığını şu ifadeleriyle anlatmıştır:⁷⁶⁹

“Komisyon olarak görevimiz özel hayatın gizliliğinin ihlal edilmesini önlemekle ilgili çalışma yapmak, sadece dinlemeler değil. Sokakta yürüyorsunuz izleniyorsunuz, çarşıya gidiyorsunuz izleniyorsunuz, AVM'lere gidiyorsunuz, izleniyorsunuz. Kendi apartmanınıza girerken koridorlarınız dahil izleniyorsunuz. Hayatımızın yüzde 90'dan fazlası zaten Mobese'lerle izleniyor. Bana göre bunların kalkması lazım. Alışveriş merkezinde çok özel şeyler de alıyor. Belli yaştan üzerindeki erkeklerin özel alışverişleri olabilir. Öyle ki, eşi bile bilsin istemeyebilir. Ama orada kameraya alınıyor. Adam girdiği AVM'de kimsenin bilmesini istemediği bir ürün almak istiyor, ama o tepeden çekiyor. İşte bu da aslında mahremiyet alanına müdahaledir. Sokakta da insanın özeli olabilir. Sevgilisine sarılır, eşiyle dolaşır, kendine göre birtakım hareketler yapar. Kameraların her alanı çekmesi rahatsız edici.”

Mobese kameraları bağlamında hangi şekillerde özel hayatın gizliliğine yönelik müdahale gerçekleşmektedir? Birincisi, bireylerin günlük faaliyetleri takip edilebilmektedir. Yani saat kaçta evden çıktığı, işyerinin neresi olduğu, eğlence için gittiği mekanlar, bulunduğu şahıslar, camiye ya da kiliseye gidip gitmediği (bugün birçok cami ve kilisede de Mobese kameraları bulunmaktadır.)⁷⁷⁰, giydiği kıyafetler (mesela mini etek giyip giymediği) gibi hayat tarzına yönelik verilere ulaşılabileceği değerlendirilmektedir.⁷⁷¹

İkincisi Mobesenin temel bileşeni olan Görüntüleme Modülü ile entegre olan Plaka Tanıma Sistemi vasıtasıyla kişilerin kullandıkları araçlar, araçta birlikte olduğu şahıslar, aracı ile günlük hareket tarzı gibi verilere ulaşılabileceği düşünülmektedir. Bu sistem trafik ihlallerinin tespiti amaçlı kullanılmaktadır. Ancak belirtilen verilere de ulaşmak mümkündür. Hakkında bu kameralar yoluyla trafik cezası uygulanan şahsın, trafik ihlalini işleme anının resimleri posta yoluyla evine gönderilmektedir. Eğer erkek şahıs ceza aldığı bir anda başka bir bayanla birlikte aynı araçta ise bundan eşine bir anlamda haber verilmektedir. Bu durum en basit haliyle bir özel hayatın ihlali olarak değerlendirilebilir. Nitekim eve gönderilen fotoğraflı cezaların zaman zaman aile içi çatışmalara yol açtığına yönelik de somut örnekler bulunmaktadır.⁷⁷²

Üçüncüsü Mobese kameralarının görüş alanları içine yurttaşların evleri, işyerleri girebilmektedir. Bu bakımdan eğer kamera görüntülerinde konutlara yönelik perdeleme⁷⁷³

⁷⁶⁹ 21.02.2013 Tarihli “Böcek Komisyonu Başkanı: Mobese Dahil Tüm Kameralar Kaldırılsın” Başlıklı Radikal Gazetesi Haberi.

⁷⁷⁰ <http://tks.ibt.gov.tr/noc-player.php?id=35> internet adresinden İstanbul'da Eyüp Sultan Camisi'ne girip çıkanlar 7 gün 24 saat canlı olarak izlenebilmektedir.

⁷⁷¹ Nigel Gilbert, *a.g.k.*, s.42.

⁷⁷² 16.03.2013 Tarihli “Çapkın Erkeklerle Mozaikle Koruma” Başlıklı Sabah Gazetesi Haberi.

⁷⁷³ “Perdeleme” yöntemi denilen sistem sayesinde kameralar otomatik olarak evlerin balkonlarını ve pencerelerine siyah bir bant çeker ve evin içindeki şahısların hareketleri hiçbir şekilde görünmez. Bu sayede bilgisayar başında oturan ve şehrin en işlek caddelerini kameralarla denetleyen yetkili, evlerin hiçbir şekilde içini göremez.

yapılmazsa pencerelerden tamamen özel hayata ilişkin olan evlerin içini veya balkonlarda bulunan şahısları gözetlemek mümkün olabilir.⁷⁷⁴

Dördüncü olarak Mobese kameralarına entegre edilmesi planlanan yüz tanıma sistemlerinin kullanılması halinde ortaya çıkaracağı biyometrik veri tehlikesi ifade edilebilir. ABD ve İngiltere’de “Kartal Gözü (*Ing; Eagle Eye*)” adında gelişmiş bir yüz tanıma sistemi kullanılmaktadır. Bu sistem kamera önünden geçen şahısların kimliklerinin tespiti, aranan şahısların ülke içinde bulunması, ülkeye sahte pasaport ile giriş yapanların tespiti ve yabancı uyruklu şahıslardan şüpheli görülenlerin kara listeye alınarak takip edilmesi gibi faaliyetler amacıyla kullanılmaktadır.⁷⁷⁵ Türkiye’de de bu sistem kullanılmak istenmektedir ve buna yönelik EGM Haberleşme Dairesi Başkanlığı’nın ve KOM Dairesi Başkanlığı’nın bir takım çalışmaları olduğu bilinmektedir. Yüz tanıma sistemlerini Mobese ile entegre ederek terör, istihbarat, asayiş, narkotik, organize, mali ve kaçakçılık suçlarından sabıkalı olanlar ile araması bulunan şahısların biyometrik resimlerinin tek bir merkezde toplanarak bir kara liste oluşturulması ve bu kapsamda listede olan şahıslardan herhangi birisi Türkiye’de bulunan herhangi bir Mobese kamerasının görüş alanından geçtiği takdirde sistemin anında alarm vermesi ve gerekli takibatın ya da yakalama işleminin yapılması hedeflenmektedir.

Yüz tanıma sistemleri resim veya videoda geçen bir şahsın yüzünü veritabanlarında kayıtlı olanlar ile karşılaştırma esasına dayalı sistemlerdir. Bu sistemler; gözler, burun, ağız ve çene arasındaki mesafe, gözlerin dış çeperindeki açı, ağız genişliği, burnun ve gözlerin baş üzerindeki konumu, şakak kemiklerinin çevresinin yapısı ölçülerek her kişi için farklı olan “altın oran” olarak ifade edilen bir değere dönüştürür ve veritabanında bu oran ile aynı olan resmi bularak eşleşme gerçekleştirir.⁷⁷⁶ Dolayısıyla kişinin yüzü sayısal değere dönüştürülür. Bu ölçüler de biyometrik veri olarak kabul edilmektedir.

Mobeseye entegre olacak olan yüz tanıma sistemleri hayata geçirildiğinde polisin veri tabanlarındaki tüm fotoğrafı olan yurttaşların yüzlerinin sayısal biyometrik veriye dönüştürülme ihtimali bulunmaktadır. Böyle bir verinin Mobese sisteminde bulunması demek yurttaşın sokakta, ibadethanede, alışveriş merkezinde kameraların önünden geçtiği anda kimlik bilgilerinin otomatik olarak tespit edilmesi anlamına gelecektir. Bu durum gözetim faaliyetinin bireyin her şeyi ile görünür kılınarak gerçekleştirilmesi anlamına gelecek, gözetim

⁷⁷⁴ <http://www.olay.com.tr/haber/bursa-bolge/mobese-sadece-ceza-yazmiyor-137765.html>, (Erişim Tarihi: 18.12.2013).

⁷⁷⁵ 15.12.2012 Tarihli “FBI’nın ‘Kartal Gözü’ Türkiye’de” Başlıklı Sabah Gazetesi Haberi.

⁷⁷⁶ <http://findbiometrics.com/solutions/facial-recognition/>, (Erişim Tarihi: 19.12.2013).

faaliyetlerini derinleştirecektir. Yurttaş bakan yönüyle Foucault'nun ifade ettiği “görünmeden görme” gerçek anlamıyla vuku bulacaktır.⁷⁷⁷

Mobese, Polnet, istihbari projelerinin ve hızla hazırlanan diğer gözetim projelerinin tıpkı Orwell’ın *Bin Dokuz Yüz Seksen Dört* kitabında tasvir ettiği büyük biraderin ülkesindeki “düşünce polisi” gibi Emniyet Teşkilatı’nı gözetim toplumunun önemli bir parçasına dönüştürdüğü gözlemlenebilir. Bu gidişata dur diyecek olan güvenliği sağlama ve özel hayatın gizliliğine dikkat etme dikatomisinde özel hayatın gizliliğini esas alıp güvenliğin ihlallerini istisna olarak görme anlayışıdır. Özel hayatın gizliliğinin korunması bu noktada devlet - birey ilişkileri içerisinde devletin niteliğinin belirlenmesi açısından önemlidir. Zira özel hayatın korunmadığı bir yerde liberal - demokratik bir devlet - toplum yapısından bahsedilemeyeceği açıktır.⁷⁷⁸ Bunun için her şeyden önce ülkemizde özel alanın konumu kamusal alana göre genişletilmeli ve genişletilen bu alana kamusal müdahalelerin minimuma indirilmesi sağlanmalıdır. Zira özel alanın kamusal alana göre daha geniş tanımlandığı ülkelerde özel hayatın gizliliği konusundaki duyarlılıklar da o derece fazla olmaktadır.⁷⁷⁹ Ülkemizde başta Emniyet Teşkilatı olmak üzere güvenlik birimlerinin gözetim teknolojileri geliştikçe özel alanların kamusallaşması tehlikesi göz ardı edilmemelidir. Zira kamusallaşan özel alanların neticesinde bireyin her ihtiyacı, arzusu, zevki ve düşüncesi, kamusal bir soruşturmaya veya denetime konu olacaktır.

2.4. Bireye Ait Verinin Güvenliği Sorunu

Emniyet Teşkilatı’ndaki teknolojik dönüşümün ortaya çıkardığı tehlikelerden birisi olarak veri güvenliği sorununun kuruma ve personele bakan yönü önceki bölümde ele alınmıştı. Bu bölümde bu tehlikenin yurttaş bakan tarafı ortaya konulmaya çalışılacaktır. Emniyet Teşkilatı’nda gelişen gözetim teknolojileri çerçevesinde kullanılan Polnet, Mobese sistemleri üzerinde yurttaş a ait olan birçok veri bulunmaktadır. Toplanan bu verilerin gerçek manada korunması, başkalarının eline geçmemesi yurttaşın mahremiyetinin deşifre edilmemesi açısından önem arz etmektedir. Örneğin, Polnet üzerinde bulunan Genel Bilgi Toplama (GBT) Projesinde yer alan tüm suç kayıtlarının çalınarak internet üzerinden yayımlandığını düşünelim. Bu durum gençlik yıllarında yüz kızartıcı bir olayda yer almış olan veya böyle bir olayda mağdur olan şahsın çocuklarının, sosyal çevresinin kişinin bu zayıf noktasını bilmesi demek olacaktır. Kişinin geçmişte karıştığı, fakat başka kimsenin bilmesini

⁷⁷⁷ Michel Foucault, *a.g.k.*, 2006, s.295.

⁷⁷⁸ Arthur R. Miller, *a.g.k.*, s.28.

⁷⁷⁹ Veysel Bozkurt, *a.g.k.*, s.5 - 8.

istemediği mahrem olayın ifşa edilmesi onun mahremiyetinin gizliliğinin ihlalinden başka bir şey değildir.

Polis Vazife ve Salahiyetleri Hakkındaki Kanunun 5. maddesinin 5. fıkrası tarafından polise verilen yetki ile emniyet birimleri silah ruhsatı, sürücü belgesi ve pasaport alanların; gözüaltına alınanların; özel güvenlik görevlilerinin ve polisler ile gönüllü olanların parmak izlerini toplayabilmektedir. Toplanan bu parmak izleri Polnet üzerinde yer alan Otomatik Parmakizi Teşhis Sisteminde (AFİS) depolanabilmektedir.⁷⁸⁰ AFİS’de depolanan tüm parmak izlerinin bir şekilde çalınması veya üçüncü şahısların eline geçmesi durumunda ortaya çıkabilecek riskleri değerlendirelim. Birincisi, yurttaşın ait olan biyometrik veriler başkasının eline geçtiği için yurttaşın mahremiyeti ihlal edilmiş olacaktır. İkincisi, yurttaş işlemediği suçların faili olarak yargılanabilecektir. Nitekim parmak izi mahkemelerde güvenilirlik derecesi en yüksek delil kategorisinde değerlendirilmektedir. Bu noktada cinayet işleyen bir kişi olay yerinde çalınan parmak izi veritabanındaki parmak izlerinden herhangi birisini kopyalamak suretiyle bırakabilir. Cinayetle uzaktan yakından ilişkisi olmayan yurttaş olay yerinde kendi parmak izi bulunduğu için yargılanabilir; hatta mahkum olarak cezaevine girebilir.

Parmak izinin çalınarak başkaları tarafından kopyalanması kredi kartının, kimlik bilgilerinin, banka şifrelerinin, nüfus cüzdanının çalınmasından çok daha tehlikelidir. Zira çalınan banka şifreleri değiştirilebilir, kredi kartları iptal edilebilir, nüfus cüzdanı yeniden çıkartılabilir; fakat parmak izleri değiştirilemez.⁷⁸¹ Yurttaş açısından kendi parmak izleri yasal da olsa kamu kurumlarının veri tabanında saklanıyor olabilir. Fakat bu veritabanlarının kontrolü yurttaşın kendi elinde olmadığı için parmak izinin çalınıp çalınmadığını bilmesi de mümkün değildir.

Mobese sistemi ile ilgili daha önce de vurgulandığı üzere toplanan görüntü kayıtlarının merkezi veritabanları yerine il birimleri bünyesindeki veritabanlarında parça parça toplanması ve kamera görüntülerinin toplanmasına, depolanmasına, analiz edilmesine yönelik standartların olmaması büyük bir veri güvenliği sorununu gözler önüne sermektedir.⁷⁸² Mevcut durumda Mobese görevlileri bu kayıtların ne zaman silinmesi gerektiğine yönelik net bir tavır koyamamaktadırlar. Tüm ülkenin günlük faaliyetlerinin görüntülü olarak tutulduğu bu kayıtların yurttaş açısından iki temel şekilde doğurabileceği risk bulunmaktadır. Birincisi

⁷⁸⁰ Murat Erdal, *a.g.k.*, s.22.

⁷⁸¹ <http://www.sileo.com/biometric-identity-theft/>, (Erişim Tarihi: 19.12.2013).

⁷⁸² 10 - 11.10.2013 Tarihlerinde Bilgi Teknolojileri Dairesi Başkanlığı Sistem Şube Müdürlüğü’nde Üç Personel ile Yapılan Derinlemesine Görüşme.

görüntü kayıtlarının güvenlik birimleri dışındaki üçüncü şahısların eline geçmesi tehlikesidir.⁷⁸³ Bunun ileride doğurabileceği sorunların sınırları henüz tam olarak kestirilememektedir. Ancak şöyle bir örnek verilebilir. Gelişmiş analiz programları kullanılarak birey odaklı görüntü parçacıkları kategorize edilebilir ve herkese açık olacak şekilde bunlar için bir internet sitesi kurulabilir. Bu internet sitesi içinde “Mobese Görüntülerinin Analizi” başlığı altında “Mini Etekliler İçin Tıklayınız”, “Camiye Gidenler İçin Tıklayınız”, “Sinagoga Girenler İçin Tıklayınız”, “Meyhaneye Gidenler İçin Tıklayınız”, “ İsimli Derneğe Gidenler İçin Tıklayınız” gibi bölümler olabilir. Hatta “Fotoğrafla Ara” bölümü oluşturularak bir şahsa dair elde bulunan dijital fotoğraf sisteme yüklenerek arama yapılabilir ve bu şahsın tüm Mobese görüntüleri çıkarılabilir.⁷⁸⁴ Diğer taraftan bu görüntüler bürokratlar, siyasiler, kamu görevlileri, öğretim görevlileri hatta normal yurttaş için bile şantaj malzemesi olarak kullanılabilir.

İkincisi görüntü kayıtlarının istihbarat birimleri tarafından geçmişe yönelik analiz edilerek bireyler hakkında fişleme yapılma tehlikesidir. Bu birimler yurttaşlarla ilgili görüntü kayıtlarını gelişmiş gözetim teknolojileriyle otomatik çözümleyip birlikte hareket ettiği şahısları, arkadaşlarını, zaaflarını, etnik/dini aidiyetini kaydedebilirler. Daha önce vurgulandığı gibi günümüz dünyası Mark Poster’ın “süperpanoptikon” kavramıyla ifade ettiği bedenlerin gözetim teknolojileriyle tespiti gibi ipe geçirildiği bir dünyayı ifade etmektedir.⁷⁸⁵ Bu nedenle Mobese verilerinin güvenliği ile ilgili iddia edilen tehlikelerin gerçek olma ihtimali her geçen gün daha da artmaktadır.

Mobese, Polnet ve diğer istihbarat projelerinin güvenliğine yönelik alınan bir takım tedbirler olsa da mevcut haliyle birçok güvenlik açığının olabileceği daha önce vurgulanmıştı. Bu güvenlik açıklarının tespitine yönelik doğru adımlar atılmalı, güvenlik standartları belirlenmelidir. Aksi takdirde bu sistemler bireyin özel hayatının gizliliği ile bireyin ve ailesinin mali ve can güvenliği için sürekli bir tehdit olacaktır. Günümüzde daha önce de ifade edilen Ankara Emniyet Müdürlüğü ihbar sisteminin hacklenerek ihbar yapan şahısların bilgilerinin alınması⁷⁸⁶ gibi olayların vuku bulması Emniyet Teşkilatı’nın veri güvenliği karnesine olumsuz yansiyarak yurttaşlarda kendileriyle ilgili tutulan verilerin güvenliği konusunda endişeye yol açabilir.

⁷⁸³ Nigel Gilbert, *a.g.k.*, s.25.

⁷⁸⁴ “Google Görsel Arama” Uygulamasından Esinlenilmiştir.

⁷⁸⁵ Mark Poster, *a.g.k.*, 2001, s.281 - 294.

⁷⁸⁶ - - - , (Erişim Tarihi:15.01.2013).

3. Gözetimin Yönetimine Yönelik Öneriler

Türkiye’de gözetim teknolojileri ve faaliyetlerindeki hızlı gelişmeler göstergesinde özellikle güvenlik tabanlı gözetim uygulamalarında geri dönüşü olmayan bir yola girildiği düşünülmektedir. Bu bakımdan özelde Emniyet Teşkilatı için gözetim faaliyetlerinin durdurulmasının söz konusu olmadığı değerlendirilmektedir. Eğer gözetim durdurulamıyorsa somut olarak yapılabilecek olan şey gözetimin sınırlandırılması ve kontrol altında tutulmasının sağlanmasıdır.

Gözetimden elde edilen bilgi iktidara meşruluk ve etkinlik kazandıran bir etmen olarak görülmektedir.⁷⁸⁷ Zira iktidarın varlığını idame ettirmesi iktidar kurdukları üzerinde kontrolü sağlama gücüyle doğru orantılı olarak değerlendirilir. Bunun bir sonucu olarak iktidarın bilgi toplama araçlarını; yani gözetim araçlarını çeşitlendirmek ve güçlendirmek isteyeceği bir gerçektir. İktidarın bu araçlarla bilgiye sahip olma arzusu deniz suyu içmek gibidir; içtikçe daha çok ister ve neticede bu konuda önü alınmaz bir güce sahip olabilir. Bu noktada iktidarın gözetim teknolojileriyle donatılmasına engel olunması gerekmektedir. Bunun da yolu gözetim faaliyetlerinin hukuki düzenlemelerle sınırlandırılması, sonrasında gözetleyenlerin bu düzenlemelere uygun hareket etmesinin denetim altında tutulmasıdır. Gözetimin başarılı bir şekilde yönetiminin bu şekilde gerçekleştirilebileceği düşünülmektedir.

Gözetimin yönetiminin iktidarın tekelinde olması başka bir çıkmaza yol açabilir. Bu bakımdan gözetim faaliyetlerinin sivil denetim mekanizmalarının denetimine açılması sağlanabilir. Örneğin Emniyet Teşkilatı’nda Polnet, Mobese, istihbari projeler bu konuda uzman özel şirketlerle anlaşarak sivil denetimin konusu yapılabilir. Sivil denetim içerisine gözetim uygulamalarına ilişkin verilerin şeffaflık raporları içerisinde halk ile paylaşılması yolu da eklenebilir. Böylece gözetimin boyutuna ilişkin halkın ve sivil toplum kuruluşlarının eleştirileri alınabilir. Bu eleştiriler kamyonun yoldan çıkarak yokuş aşağı gitmesini engelleyici kontrol mekanizmaları görevi üstlenebilir. Ayrıca gözetimde güvenliğin sağlanması - özel hayatın gizliliği dengesinin oluşturulması açısından bilimsel araştırmaların önü açılabilir. Sistemin optimizasyonu açısından bu araştırmalar yol gösterici olabilir.

Yukarıda ifade edilenler çerçevesinde Emniyet Teşkilatı’nda Polnet ve Mobese projeleri ile bunların alt uygulamaları araçlarıyla gerçekleştirilen gözetim faaliyetlerinin yönetimine yönelik yeni bir örgütsel yapı ve faaliyetlerin şeffaflığı için iki somut öneride

⁷⁸⁷ Zygmunt Bauman, *a.g.k.*, 1996, s.62.

bulunulmuştur. Bu önerilerin Milli İstihbarat Teşkilatı, Jandarma Genel Komutanlığı gibi diğer gözetim birimleri için de uygulanabileceği değerlendirilmektedir.

3.1. Gözetim Kontrol Birimi

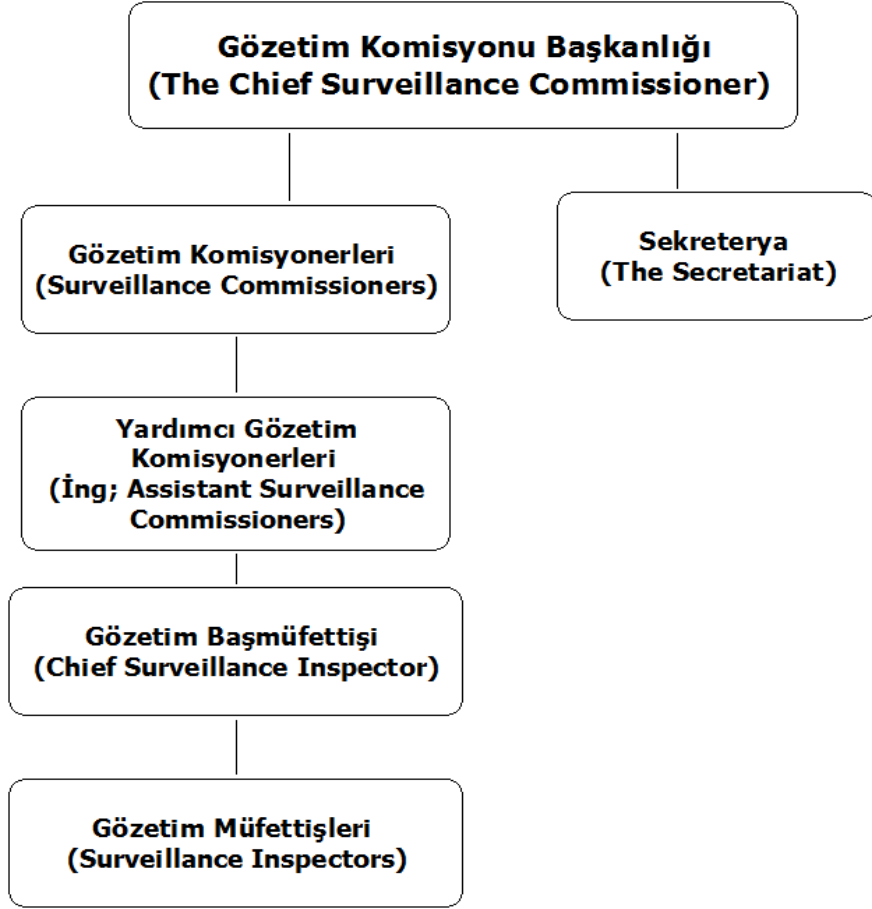
İktidarın veri toplamaya yönelik iştahı hep yükselen bir ivmeyle artmakta, asgari düzeyde veri toplamakla yetinmemektedir.⁷⁸⁸ İktidarın bu sınır tanımaz veri toplama arzusunun güvenlik tehditleri olduğu müddetçe devam edeceği düşünülmektedir. Zira güvenliği sağlamak bu noktada en önemli gereksidir. Ülkemizde de iktidarın güvenlik gerekçeli veri toplama aygıtı olarak Emniyet Teşkilatı yer almaktadır. Ülkemizde giderek artan suç oranlarıyla birlikte değerlendirildiğinde Emniyet Teşkilatı'nın gözetim faaliyetlerinin gün geçtikçe artış göstereceği analiz edilebilir. Fakat bu şekilde gözetimin her geçen gün daha tehlikeli, daha tehditkar olduğu da bir gerçektir. Neticede ortaya çıkması muhtemel tehditlerin ve tehlikelerin önüne geçmek amacıyla gözetim faaliyetlerinin kontrol altında tutulması, yönetilmesi önemli bir gereksinim olmuştur. Gerek gözetim faaliyetlerinin nüfuzunun azaltılması, gerek yurttaşların özel alanlarının koruma altında tutulması, gerekse gözetleyenlerin keyfi uygulamalarına gem vurulması amacıyla bir takım önlemlerin alınması gerektiği bir gerçektir. Ülkemizde bunları gerçekleştirebilecek yeni bir örgütsel yapıya ihtiyaç olduğu düşünülmektedir. Bu bölümde ifade edilen ihtiyaç paralelinde öncelikle İngiltere'deki örgütsel yapı incelenecek sonrasında Emniyet Teşkilatı içerisinde gözetimin yönetimine yönelik yeni bir birimin kurulması önerilecektir.

İngiltere'de gözetim faaliyetlerinin kontrol altında tutulması ve gözetim politikalarının oluşturulması amacıyla Gözetim Komisyonu Başkanlığı (*İng; The Chief Surveillance Commissioner*) kurulmuştur. Bu birimin organik yapısı aşağıdaki şekilde ortaya konulmuştur. Birim tamamen özerk bir yapıya sahip olmakla birlikte daha çok hukuki bir oluşum olarak gözükmektedir ve 1999 yılından beri faaliyetlerine devam etmektedir. Bütçesi İngiltere İçişleri Bakanlığı (*İng; Home Office*) tarafından karşılanmaktadır. Ancak İçişleri Bakanlığı, birimin faaliyetlerinin icrasına hiçbir şekilde müdahale edememektedir. Birimin temel amacı gözetim uygulamalarının insan haklarına ve yasal düzenlemelere uygun bir şekilde gerçekleştirilmesini sağlamaktır. Dolayısıyla birimin İngiltere'de gözetleyenlerin gözetimini yaptığı ifade edilebilir.⁷⁸⁹

⁷⁸⁸ Gary T. Marx, "An Ethics For the New Surveillance"; *The Information Society*, <http://www.mit.edu/gtmarx/nicolin5.html>, (Erişim Tarihi: 05.07.2013).

⁷⁸⁹ <https://osc.independent.gov.uk/how-we-work/>, (Erişim Tarihi: 14.01.2013).

Şekil-5.İngiltere Gözetim Komisyonu Başkanlığı



Kaynak: <https://osc.independent.gov.uk>.

Kamu birimleri tarafından yürütülen gizlilik içeren gözetim faaliyetleri Gözetim Müfettişleri tarafından incelenerek yıllık gözetim değerlendirme raporları hazırlanmaktadır. Hazırlanan bu raporlar Parlamento'ya ve halka sunulmaktadır. Bu kapsamda bilgisayar, cep telefonu gibi bilgi - iletişim teknolojilerine nüfuz edilerek gerçekleştirilen gözetim, konut ve işyerine dinleme cihazı yerleştirilerek yapılan takibat, fiziki takip, kameralı gözetim faaliyetlerine yönelik incelemeler yapmaktadırlar. Gözetim uygulamalarının yıl içinde kullanım oranları, kurallara aykırı yapılan gözetim faaliyetleri tespit edilmekte ve gözetim araçlarının kullanım şekli ile oranına yönelik yasal düzenlemeler çerçevesinde çeşitli tavsiyeler vermektedirler.⁷⁹⁰

İngiltere'de yıllardır faaliyet gösteren Gözetim Komisyonu Başkanlığı ülkedeki gözetim faaliyetlerinin sınırlandırılmasında, güvenlik güçlerinin bu konuda raydan çıkmasının engellenmesinde bir anlamda yurttaşların temsilcisi görevini üstlenmiştir. Bu bakımdan

⁷⁹⁰ Office of Surveillance Commissioners, *2012-2013 Dönemi Senelik Raporu*, Temmuz 2013.

güvenlik birimlerinin gözetim faaliyetlerinin hukuka aykırı sınırlara ulaşmasında bir denetim mekanizması olduğu ifade edilebilir.

Gözetim faaliyetlerinin uygulanmasıyla ilgili olarak önceki bölümlerde ifade edildiği üzere bu faaliyetleri yerine getirenler şahsi menfaatleri, görevin yerine getirilmesi için her şeyi mubah görebilmeleri gibi nedenlerle başkalarının özel hayatlarının gizliliğini ihlal edebilmektedirler.⁷⁹¹ Gözetimin konusunu oluşturan kişisel veriler üçüncü şahısların eline geçerek gözetim verilerinin güvenliği tehlikesi her zaman bulunmaktadır. Ülkemizde bu tehlikeleri bertaraf edebilecek somut bir denetim mekanizması bulunmamaktadır. Halbuki bilgi toplumu sürecinde kamu kurumları e-devlet sistemlerine, gelişmiş istihbarat teknolojilerine sahip olmuşlardır. Örneğin, Polnetin sistem odasında veritabanının başında görevli olan personelin tüm verileri kopyalayarak başkalarına verip vermediğini kontrol edecek bir mekanizma bulunmamaktadır. Normal şartlarda bu tür sistemlerde kayıtlı bilgilerin, sahiplerinin izni olmaksızın üçüncü şahısların eline geçmesi hukuka aykırıdır. Ancak bunun denetimini sağlayacak bir düzen bulunmamaktadır.⁷⁹²

Bilgi ve iletişim teknolojilerinin yaygınlaşmasıyla ortaya çıkan “bilişim tabanlı tekno - güvenlik problemleri” de gözetimin genişleyerek hukuk dışına çıkmasında ve gözetim faaliyetlerinden elde edilen bireye ait verilerin başkalarının eline geçmesinde rol oynayabilmektedir.⁷⁹³ Ağ korsanlığı, bilgisayar virüsleri, truva atları, solucanlar gibi kötü niyetli yazılımlar vasıtasıyla bunlar olabilmektedir. Bu şekilde meydana gelebilecek saldırılara veya tehlikelere yönelik olarak gözetim faaliyetlerini yürütenlerin hem bu yasadışı yolları kullanarak veri elde etmemesi, hem de gözetim araçlarıyla elde ettikleri verilere başka gözetim araçları tarafından ulaşılamaması için gözetim politikası ve bilişim güvenliği çalışmalarının başka mekanizmalar tarafından denetlenmesine ihtiyaç olduğu bir gerçektir.

Gözetim faaliyetlerinin günümüzde bireyin bedenine kadar inmiş olması onun en son ulaştığı sur olarak ifade edilebilir. Bireyin DNA’sına kadar sızabilen biyolojik gözetim teknikleri düşünüldüğünde, elde edilen verinin hassasiyeti ve derinliği ortaya çıkmaktadır.⁷⁹⁴ Bireyler güvenlik hedefli bu uygulamalara zaman zaman kendi rızalarıyla katılabilmektedirler. İster kendi rızalarıyla ister zorla bu veriler kendilerinden alınmış olsun birey için bedenine ait olan şeyin en değerli şey olduğu unutulmamalıdır. Gözetleyenlere bu verileri istedikleri gibi kullanma hakkını vermemelidir. Bedenine ait olan verileri alınan

⁷⁹¹ İsmail Tulum, *a.g.k.*, s.36.

⁷⁹² Anthony Giddens, *a.g.k.*, 2000, s.312.

⁷⁹³ Murat Erdal, *a.g.k.*, s.23 - 34.

⁷⁹⁴ Michel Foucault, *a.g.k.*, 2003, s.48.

bireyin en azından bunların kullanım şekli ve sınırları üzerinde inisiyatifi olmalıdır. Aksi takdirde Marx'a göre bu durum kişisel hak ve özgürlükleri çiğneme noktasına giden etik olmayan bir yaklaşıma dönüşür.⁷⁹⁵ Polnet bünyesinde parmak izi gibi çeşitli kriminal biometrik veriler de bulunmaktadır. Yurttaşların kendilerine ait herhangi bir biometrik verinin güvenlik birimlerinde olup olmadığını, eğer varsa bu verilerin ne kadar süre nerede saklanacağını, bu verilerin hangi olayların aydınlatılmasında kullanıldığını bilme hakkı bulunmaktadır. Bu noktada ülkemizde biometrik gözetim verilerinin kullanımına yönelik halkın bilinçlendirilmesi gerekmektedir. Polisin bu faaliyetlerine yönelik olarak bilinçlendirme ve kontrol işlemlerini gerçekleştirebilecek mekanizmalara ihtiyaç bulunmaktadır.

Gözetim faaliyetlerinin denetim altında tutulması, sınırlandırılması, veri güvenliğinin sağlanması gibi amaçlarla Emniyet Teşkilatı bünyesinde bir yapılanmaya gidilmesi ihtiyacının olduğu değerlendirilmektedir. Burada buna yönelik olarak Emniyet Genel Müdürlüğü bünyesinde Daire Başkanlığı şeklinde bir denetim mekanizması önerilecektir.

Emniyet Genel Müdürlüğü yapılanmasına yönelik olarak önceki bölümlerde bilgi verilmişti. Bu yapıda gözetim faaliyetlerini İstihbarat, Kaçakçılık ve Organize Suçlarla Mücadele, Terörle Mücadele, Asayiş, Bilgi Teknolojileri, Siber Suçlarla Mücadele, Haberleşme Dairesi Başkanlıkları yürütmektedir. Tüm bu daire başkanlıklarının ve bunların il emniyet müdürlüklerindeki karşılıkları olan şube müdürlüklerinin gerçekleştirdikleri gözetim faaliyetlerini denetleyecek, gözetleyenleri gözetleyecek Daire Başkanlığı şeklinde örgütlenmiş doğrudan Emniyet Genel Müdürüne bağlı olarak çalışacak bir yapı oluşturulabilir. Bu yapı çalışmamızda "Gözetim Kontrol Daire Başkanlığı" olarak isimlendirilmiştir. Organik yapısı aşağıdaki şemada oluşturulmuştur.

⁷⁹⁵ Gary T. Marx, "An Ethics For the New Surveillance"; *The Information Society*, <http://www.mit.edu/gtmarx/nicolin5.html>, (Erişim Tarihi: 05.07.2013).

Şekil-6.Gözetim Kontrol Daire Başkanlığı



Yukarıdaki şemada ifade edilen örgütsel yapıda Gözetim Kontrol Daire Başkanlığı'na bağlı olarak beş ana şube müdürlüğü tasarlanmaktadır. Bunlardan Polnet Projeleri Denetleme Şube Müdürlüğü, Polnet içerisinde yer alan tüm projelerin yasal gerekçelerinin incelenmesi, hukuka aykırı olanların uygulamadan tamamen kaldırılması, projelerin veri toplama sınırlarının tespiti, toplanan verilerin hangi veritabanlarında ne kadar süre boyunca saklanacağını ve bu veritabanlara erişmekte yetkili olacak personelin tespiti, yetkili personelin *log* kayıtlarının incelenmesi, verilerin güvenliğinin sağlanmasına yönelik tedbirlerin belirlenmesi, alınan tedbirlere görevlilerin uyup uymadığının kontrol edilmesi, yeni projeler uygulamaya konulmadan önce özel hayatın gizliliği ve hukuka uygunluk açısından incelenmesi gibi faaliyetlerde bulunabileceği öngörülmektedir.

Mobese Denetleme Şube Müdürlüğü'nün Haberleşme Dairesi Başkanlığı ile de uyumlu olarak Mobese ve buna bağlı alt sistemlerin çalışmalarını hukuka uygunluk açısından ve özel hayatın gizliliğine minimum müdahalenin gerçekleşmesini sağlamak amacıyla takip ve kontrol etmesi öngörülmektedir. Bu bakımdan kurulması tasarlanan şube müdürlüğü öncelikle Mobese ve alt sistemlerini mevzuat açısından değerlendirebilir ve mevzuat dışı uygulama ve faaliyetleri değiştirilmek üzere rapor edebilir. Mobesenin temel araçlarından olan kamera sistemlerinin hangi illerde, hangi bölgelerde neden kurulduğunu denetleyebilir. Bu kapsamda mütemadiyen suç endeksleriyle birlikte değerlendirerek kameraların bölgelere göre gereklilik analizini gerçekleştirip ilgili birimi bu şekilde yönlendirebilir. Kamera görüntülerinin alınmasında özel hayatın gizliliğini ihlalin sınırlandırılmasına yönelik

arařtırmalar yapabilir. Örneęin Mobese kameralarının görüntü alanı içine giren bina girişleri, balkonlar, pencereler gibi alanlara sistem tarafından otomatik olarak perdeleme yapılması sağlanabilir. Böylece hiç olmazsa yurttaşların evine girip çıkanların tespit edilmesine ve balkon ile evin içine dair gözetleme yapılmasına engel olunabilir. Ayrıca tüm Türkiye’deki kamera kayıtlarının tek bir merkezde depolanması sağlanarak bunların kaybolmasının, üçüncü şahısların eline geçmesinin önüne geçilebilir. Görüntülerin depolandığı bu tek merkezin kameralarla 7 gün 24 saat gözetimi yapılarak sistem güvenliği sağlanabilir. Toplanan görüntü verilerinin hangi şartlar altında kimler tarafından görüntülenebileceğinin belirlenmesi de gerekmektedir. Böylece şüpheli bir durumda personelden hesap sorulabilir. Görüntülerin ne kadar süre için saklanacağı, ne zaman silineceğı netleştirilerek özel hayatın geçmişe yönelik ihlalinin önüne geçilebilir. Kurulması tasarlanan şube müdürlüğü müfettişleri illerde kurulu Mobese Yönetim Sistemlerine ve Mobese Komuta Kontrol Merkezlerine ani denetimler yaparak, gözetim faaliyetleriyle ilgili belirlenen kurallara aykırı harekette bulunanları tespit ederek bunlar hakkında soruşturma açabilir.

İstihbari Projeler Denetleme Şube Müdürlüğü’nün, İstihbarat Dairesi Başkanlığı bünyesindeki tüm gözetim faaliyetlerinin kontrol altında tutulması ve keyfi uygulamaların engellenmesi amaçlı olarak faaliyet göstermesi düşünülmektedir. Bu bakımdan istihbari amaçlı gerçekleştirilen dinleme, fiziksel takip gibi faaliyetler ile bunların gerçekleştirilmesi için kullanılan sistemler düzenli olarak hukuka uygunluk ve özel hayatın gizliliğinin ihlali açılarından denetlenebilir.

Adli Projeler Şube Müdürlüğü, adli soruşturmalara yönelik yürütölen gözetim faaliyetlerinin soruşturma’nın gizliliğini ihlal etmeyecek şekilde gözetimin hukuka uygunluğuna bakan yönüyle denetleme yapabileceğı düşünülmektedir. Bu bağlamda adli soruşturma kapsamında gözetim faaliyetlerinde bulunabilen Emniyet birimlerine yönelik daha çok kullandıkları sistemlerin soruşturma kapsamına giren şahısların haricinde suçla ilgisi olmayan yurttaşlara yönelik gözetleme faaliyetlerinde bulunabilme yeteneğinin olup olmadığı, mahkeme kararı olmadan bu sistemler kullanılarak gözetim faaliyetlerinin gerçekleştirilip gerçekleştirilmediğini denetleyebilir.

Halkla İlişkiler Şube Müdürlüğü, Emniyet Teşkilatı bünyesinde yürütölen tüm gözetim faaliyetlerine yönelik halkın bilinçlendirilmesi amaçlı olarak Gözetim Kontrol Daire Başkanlığı’nın halk, medya, sivil toplum kuruluşları ile olan ilişkilerini düzenleyen birim şeklinde tasarlanmıştır. Bu birim bir sonraki kısımda ifade edilecek olan şeffaflık raporlarıyla gözetim faaliyetlerinin sınırlarını, mevcut kapasitelerini ilan edebilir. Ayrıca hakkında

gözetim işlemi yapılmış olup, herhangi bir suç unsuruna rastlanmamış olan şahıslara, “.. /.. /... - .. /.. /... tarihleri arasında hakkınızda sayılı mahkeme kararına istinaden gerekçelerle gözetim faaliyeti uygulanmıştır. Belirtilen gözetleme gerekçelerinin gerçeği yansıtmadığı tespit edildiğinden dolayı gözetim faaliyetine son verilmiştir.” şeklinde bildirimde bulunulması işlemlerini yönetebilir. Gözetim faaliyetlerine yönelik olarak yurttaşlardan gelebilecek her türlü soruya açık ve net olarak cevap verilmesini sağlayabilir.

Yukarıda belirtilen şube müdürlükleri haricinde Araştırma Geliştirme Şube Müdürlüğü’nün de tasarlanan örgütsel yapıya eklenebileceği düşünülmektedir. Bu şube müdürlüğünün iki temel görevi olabilir. Birincisi, gözetim faaliyetlerinin bizzat suçun ve suç organizasyonunun deşifresine yönelik gerçekleştirilmesi amacına matuf olarak gözetimin minimum seviyelerde tutulmasını sağlayabilecek yeni gözetim teknolojilerinin araştırılması şeklinde ifade edilebilir. Bu şube müdürlüğü yurtdışındaki gözetim birimlerinde gözetim faaliyetleri yürütülürken özel hayatın gizliliğinin ihlalini önlemeye yönelik geliştirilmiş olan mekanizmaları, denetim sistemlerini karşılaştırmalı olarak takip edebilir. İkincisi, gözetim - suç fayda analizi çalışmaları yaparak, suç tespitinde etkili olmayan ve suçla mücadelede yararı ortadan kalkmış olan; fakat özel hayatın gizliliğini ihlal eden gözetim uygulamalarının tespitine yönelik çalışmalar yapabilir. Örneğin, kapkaç gibi asayiş suçlarının işlendiği bölgeler ile Mobese kameralarının bulunduğu bölgeler karşılaştırılarak bu suçların işlenmediği bölgelerdeki kamera yoğunluğunu tespit edebilir.

3.2. Şeffaflık Raporları

Gözetim faaliyetlerinin kontrol altında tutulabilmesi amacıyla yapılabilecek olan faaliyetlerden birisi de gerçekleştirilen gözetim uygulamalarının boyutları hakkında halkın bilinçlendirilmesi, bir şekilde farkındalık oluşturulmasıdır. Nitekim gözetlenenlerin nasıl gözetlendiklerini bilmeye hakları olduğu bir gerçektir. Ayrıca gözetim birimlerinde keyfi uygulamaların olmaması için gözetimin metot, şekil ve sürelerinin şeffaf olması gerekir.⁷⁹⁶ Bu amaçla Emniyet Teşkilatı bünyesinde gerçekleştirilen gözetim uygulamalarına yönelik şeffaflık raporlarının yayımlanması gerektiği düşünülmektedir.

Gözetim şeffaflık raporlarında gözetim faaliyetlerinin neler olduğu ifade edilmelidir. Günümüzde gözetim araçları kullanılmasıyla bireye ve topluma ait bilgi iktidar güçlerinin eline çok hızlı ve kolay bir şekilde akmaktadır. Bir zamanlar gözetimin kapsamı sokak ışıkları

⁷⁹⁶ Gary T. Marx, *a.g.k*, 2005, s.1.

ve fiziksel mimari aracılığıyla kontrolü sağlamak ve çarpıklıkları önlemek demek iken, günümüzde bunun çok daha ötesinde kamera görüntüleri ve diğer teknolojik gözetleme araçlarını kullanarak bütün toplum unsurları hakkında elektronik etiketler tutulabilmesi olmuştur.⁷⁹⁷ Bu bakımdan gözetim araçları her geçen gün çeşitlilik gösterirken, bunlarla alınabilecek bireye ait olan verilerin “özel” oluşu da giderek artmaktadır. Bilgi ve iletişim teknolojilerindeki gelişmeler çerçevesinde başlangıçta gözetim türlerinden fiziki takip ile bireylerin gündelik faaliyetlerinin tespiti en uç gözetim şekliyen, artık gözetim bireyin tüm telefon görüşmeleri, mesajlaşmaları, mimikleri, yürüyüşü, tüm irtibatlı olduğu çevresi, düşünceleri hatta ruh haline kadar derinleşmiştir. Nitekim resmi otoriteler tarafından net bir şekilde ifade edilmese de yüksek güvenliqli toplum kapsamında dünyadaki tüm telefonları anlık uydudan takip edebilme ve dinleyebilme yeteneklerine sahip “*Echelon*” ve benzeri teknolojilerin olduğu bilinmektedir.⁷⁹⁸ Yakın zamanda ABD istihbarat birimleriyle yakın ilişkili olan teknoloji gurusu Jacop Applebaum’un “...Amerikan istihbarat teşkilatı NSA’nın dinleyemeyeceği bir cep telefonu yok... NSA birisini izlemek isterse hiçbir kaçış yok... Endişe etmek için çok sebep bulunuyor. Bir telefona uzaktan erişmek, telefon rehberini kopyalamak çok kolay...” ifadeleri dünyada güvenlik tabanlı gözetim faaliyetlerinin ulaştığı son noktaya ışık tutmaktadır.⁷⁹⁹

Güvenlik tabanlı gözetim faaliyetleri bu kadar güçlü hale gelirken Emniyet Teşkilatı bünyesinde özellikle istihbarat birimlerinde ne tür gözetim metot ve araçlarının kullanıldığı bilinmemektedir. Mesela “EGM İstihbarat Dairesi Başkanlığı *Echelon* sisteminde olduğu gibi uydudan gözetleme yapabilmekte midir? Türkiye’deki bütün telefon numaralarını dinleme kapasitesine sahip midir?” gibi soruların net bir şekilde cevaplanması gerekir ki yurttaşlar gözetim canavarını bir kafese koyabilsin, sınırlarını bilebilsin. Sınırları bilinen gözetim, gözetimin tanrısallaşmasıyla ortaya çıkan korkunun önüne geçilmesini sağlayabilir.⁸⁰⁰

Tasarlanan şeffaflık raporlarında belirli periyotlarda gerçekleştirilen gözetimin kapasitesi ortaya konulmalıdır. Gözetimin kapasitesiyle yürüyen adli soruşturmalar kapsamında veya rutin gözetim faaliyetlerinde kullanılan gözetim araçlarının sayısı ile bunlarla gerçekleştirilen işlem boyutu ifade edilmektedir. Örneğin İngiltere’de kamera sayıları ve yerleri bölgesel olarak harita üzerinde ilan edilmektedir.⁸⁰¹ Bu kapsamda Mobese kamera sayıları, bunların il bazında konumları, toplanan görüntü verilerine yönelik ne gibi işlemlerin

⁷⁹⁷ David Lyon, *a.g.k.*, 2006, s.113 - 114.

⁷⁹⁸ Gürdilek Raşit, *a.g.k.*, s.36 - 37.

⁷⁹⁹ <http://www.osnews.com>, (Erişim Tarihi: 15.01.2014).

⁸⁰⁰ Zygmunt Bauman, *a.g.k.*, 1998, s.246.

⁸⁰¹ http://news.bbc.co.uk/2/hi/programmes/whos_watching_you/8011103.stm, (Erişim Tarihi: 15.01.2014).

gerçekleştirildiği, veritabanlarında ne kadar süre saklandığı, bireysel profillemeye çalışmaları yapılıp yapılmadığı gibi hususlar raporda belirtilebilir. Diğer taraftan Polnet bünyesinde bulunan projeler ile istihbari projelerde ve diğer e-devlet projelerinde kaç yurttaşla yönelik ne tür sorgulamalar yapıldığı açıklanabilir. Böylece yurttaşlar gözetimin yoğunluğu hakkında fikir sahibi olabilirler.

Adli soruşturmalar kapsamında gerçekleştirilen takibat işlemlerinin sayısı da düzenli olarak örneğin ayda veya üç ayda bir kez bu raporlarda açıklanabilir. Örneğin son bir ayda dinleme yapılan telefon sayısı, günümüze kadar toplamda yapılan dinleme sayısı gibi veriler açıklanabilir. İstihbari amaçlı gerçekleştirilen gözetim faaliyetlerinin oranı da burada ifade edilebilir. Ayrıca gözetim faaliyetlerinin bu faaliyetleri gerçekleştirmedeki temel saik olan suçun ortaya çıkarılmasına, suçluların yakalanmasına olan oranları düzenli olarak ölçülerek raporlarda gösterilmelidir. Eğer bu oranlar suçla mücadelede başarılı olunduğu yönünde olursa Lyon'un ifade ettiği özel hayatın gizliliği ile güvenliğin sağlanması dikatomisinde⁸⁰² güvenliğin ağır basarak gözetimin gerçekleştirilmesinin bir açıklaması yapılabilir. Aksi takdirde gözetim faaliyetlerinde aşırılığa gidildiği anlaşılır ve baskı gruplarınca güvenlik güçlerine eleştiri getirilebilir. Mesela uyuşturucu madde kaçakçılığı konusunda hakkında dinleme yapılan telefon sahiplerinin %90'ı ile ilgili suç unsuruna rastlanılamamış olsa ve bu raporlarda cesurca ortaya konulabilirse gözetimde aşırılığın önüne geçilebilir. Gözetim faaliyetini yapan birimin bu oranları ve karşılığında ne gibi tedbirler alındığını, keyfi uygulama olup olmadığını şeffaflık raporlarında açıklaması gerektiği değerlendirilmektedir. Benzer bir durum Mobese kameralarının yerleştirildiği bölgelerdeki suç oranları ile ilgili de yapılabilir.

Emniyet Teşkilatı bünyesinde gerçekleştirilen gözetim faaliyetleriyle ilgili önerilen şeffaflık raporlarında temel amaç yurttaşların zihinlerinde gözetimin boyutlarıyla ilgili bir çerçeve çizebilmek olmalıdır. Yurttaşların gözetime dair kuruma e-posta veya diğer yollarla gönderdikleri sorular, merak ettikleri şeyler de bu raporlarda cevaplanabilir.

⁸⁰² David Lyon, *a.g.k*, 2006, s.17.

SONUÇ

Çalışmada Türkiye’de gözetimin göstergeleri çerçevesinde gözetim toplumu tehlikesini ortaya koymak; bu süreçte en büyük gözetim faktörü olarak güvenlik gerekçeli gözetim faaliyetlerini yürüten ve bilgi - iletişim teknolojilerindeki gelişim ile birlikte kendi içinde değişim, dönüşüm gerçekleştiren Emniyet Teşkilatı’nın bu dönüşüm neticesinde hayata geçirdiği gözetim teknolojilerini ve faaliyetlerini açığa çıkarmak; kurumun gözetim teknolojisi merkezli evrilen yapısının yönetsel, toplumsal ve bireysel etkilerini belirlemek amaçlanmıştır.

Çalışma Polnet, Mobese ekseninde Emniyet Teşkilatı’nda teknolojik dönüşümün merkezinde yer alan birimlerde çalışan personelle derinlemesine görüşmeler çevresinde şekillendirilmiştir. Bu teknolojik dönüşümün sonucu olan gözetim sistemleri uygulamalı olarak incelenmiştir. Böylece çalışmada ifade edilen teknolojik dönüşüme bizzat şahit olunmuştur.

Türkiye’de bilgi toplumu dönüşümüyle girilen süreç gözetim toplumuna evrilmiştir. Dolayısıyla ülke olarak önemli bir gözetim toplumu sarmalı içinde yer alındığı söylenebilir. Bu süreç gerek kamu çatısı altında gerek özel sektör eliyle yürütülmektedir. Gözetim araçlarının artış göstermesi, yurттаşlar hakkında geniş veri tabanlarının oluşturulmuş olması, halkın giderek artan gözetim faaliyetlerine duyarsızlaşması ülkemizde gözetim toplumunun önemli göstergeleri arasında yer almaktadır. İktidarın muhalif sesleri bastırarak, toplum üzerinde hegemonyasını arttırma amaçlı “birey hakkında daha çok bilgiye sahip olma” arzusu gözetim tehlikesini arttırmaktadır. Gözetimin pozitif ve üretici yanı olarak görülen meşruiyet kaynakları içinde en önemlisi suçla mücadele ve güvenliğin sağlanmasıdır. Ülkemizde de gözetimin yaygınlaşması bu gerekçelerle gerçekleşmiştir. Emniyet Teşkilatı da iç güvenlikten sorumlu birim olduğu için bu sürecin en önemli aktörüdür.

Emniyet Teşkilatı iktidarın üzerine yüklemiş olduğu baskı ve yönelimlerle kurumsal olarak teknolojik ve örgütsel bir dönüşüm sürecine girmiştir. Bu dönüşümün örgütsel yapıdaki şekli bazı daire başkanlıklarının görev stratejisini buna göre değiştirmesi ve yeni daire başkanlıklarının kurulması yönünde olmuştur. Teknolojik anlamda etkisi Polnet, Mobese, istihbarat projeleri gibi gözetim faaliyetlerini gerçekleştiren yeni gözetim sistemleri oluşturulması şeklindedir. Bu sistemler bireye ait olan verilerin toplanması, kategorize edilmesi, ilişkilendirilerek analitik bir yapıya kavuşturulması ve merkezi veritabanında depolanarak gözetleyenlerin hizmetine açılması silsilesinde işlemektedir. Neticede gözetim

pratiklerinin hayata geçirilmesi anlamında Emniyet Teşkilatı'nda teknolojik ve örgütsel tekamülün gerçekleştirildiği ifade edilebilir.

Emniyet Teşkilatı'ndaki dönüşüm sürecinin hem kurumsal anlamda hem de yurttaş bakan yönünde bazı tehditleri ve riskleri barındırdığı ifade edilebilir. Kurumsal anlamda bunlar; personelde oluşan güvenlik paranoyası, gözetimin derinleşmesi tehlikesi, toplanan verilerin güvenliğini sağlayamama riski, gözetim yapanların gözetlenmesi neticesinde gözetimin etkilerinin personelde de oluşması ve meslek etiğine uyumsuz davranışların ortaya çıkması olarak ifade edilebilir.

Güvenlik paranoyası görünürde personelin görevini üst düzeyde sahiplenmesi olarak olumsallanabilse de esasında personelin devlete ait olan güvenliği sağlama misyonunu kendinde görmeye başlamasından dolayı zamanla kendini yurttaş karşısında devlet gibi görme tehlikesi içine düşebilmesi açısından bir tehdittir. Emniyet Teşkilatı'nda Polnet, Mobese ve istihbarat projeleri ile yurttaşla dair veriler toplanmaktadır. Toplanan bu veriler ışığında iktidar kendini daha güvende hissetmektedir. Bu güven ve güvenin oluşturduğu güç gerek kurum gerek personel tarafından sahiplenilebilmektedir. Bu noktada Emniyet Teşkilatı mensupları bilginin toplandığı gözetim araçlarını meşrulaştıran güvenlik görevlerini kutsallaştırabilmektedirler. Kutsallaşan görev ile güvenlik, bir kamu hizmeti olmaktan çıkarak bazen “halka rağmen güvenlik” algısında paranoyak bir hale dönüşebilmektedir.

Gözetim teknolojilerindeki hızlı gelişimin ve güvenlik paranoyasının yayılmasının Emniyet Teşkilatı'nda oluşturabileceği en büyük tehlikelerden birisi gözetimin derinleşmesidir. Derinleşen gözetim ile istihbarat faaliyetlerinin arkasında yer alan “proaktif polislik” uygulamaları haddini aşarak suç oluşmadan önce suçu önleme hedefli olarak George Orwell'ın *Bin Dokuz Yüz Seksen Dört* isimli kitabında belirttiği “Düşünce Polisliğine” evrilebilir. Mobese kameralarına mimikler, bakışlar gibi beden dili göstergelerini analiz edebilecek olan yüz tanıma sistemlerinin ve biometrik sensörlerin entegre edilme hazırlıkları bu tehlikeyi işaret etmektedir.

Polnet ve Mobese projeleri sadece yurttaşla yönelik değildir. Bu projelerde yurttaşla yönelik olan programları kullanan polisleri kontrol etmek için de gözetim programları bulunmaktadır. Personelin günlük rutin içinde yaptığı faaliyetler yurttaşla gözetlemeye yönelik olsa da, aynı şekilde kendisinin de başkaları tarafından izlenmesinin, denetlenmesinin fabrikadaki işçinin kameralarla izlenmesiyle eşdeğer sonuçları doğuracağı düşünülmektedir. Bu bakımdan gözetimin yurttaşla dönük olumsuz etkilerinin birim içindeki personel hakkında da söz konusu olduğu söylenebilir.

Polnet, Mobese ve istihbari projelerde güvenlik açıklarının olması ve veri güvenliğine yönelik somut standartların belirlenmemiş olması bireye ait olan verilerin çalınması tehdidini içinde barındırmaktadır. Bu tehdit personel açısından verilerin çalınması korkusuyla hareket etmeyi ve soruşturmanın konusu olma riskini barındırırken aynı zamanda verilerin çalınmasıyla kurumsal anlamda büyük itibar kaybının da göstergesidir. Diğer taraftan kurumsal anlamda bireyin verilerine yönelik saygının düşük olması, keyfi uygulamalara kapı açacak davranışların normalleşmesi üzerine kurulacak bir meslek etiği de Emniyet Teşkilatı ve yurttaş açısından büyük bir tehlikedir.

Emniyet Teşkilatı gözetim teknolojilerinin yurttaşa ve topluma bakan yönüyle oluşturduğu tehditler; psikolojik ve sosyolojik zararlar, bireyin özel alanının güvenlik gerekçeleriyle kamusallaştırılarak özel hayatın gizliliğinin önünün açılması ve gözetim araçlarıyla toplanan verilerin akıbetinin belirsizleşmesi olarak ifade edilebilir.

Mobese başta olmak üzere Emniyet Teşkilatı'ndaki bilgi ve iletişim teknolojilerinin yurttaşlar üzerinde oluşturduğu psikolojik olumsuz etkilerin varlığı hissedilir derecede yüksektir. Bu etkiler kronik hale gelerek paranoyaya dönüşebilmektedir. Bireyler, Mobese kameralarının sayısının çok olması nedeniyle her yerin çok tehlikeli olduğunu düşünebilmektedirler. Bu kapsamda her an saldırıya uğrayabilecekleri yönünde suç paranoyasına kapılabilmektedirler. Bazen kameraların varlığı ters etki yaparak toplumsal bilinçte Mobesenin olmadığı yerlerin güvensiz olduğu düşünülebilmektedir. Bunların dışında yurttaşlar gözetim toplumunun da bir göstergesi olarak sürekli gözetlendiği düşüncesinde gözetim paranoyasına da kapılabilmektedirler.

Güvenlik birimleri, çalışmada ifade edilen gözetim teknolojilerini kullanırken güvenliği sağlama ve özel hayatın gizliliğine dikkat etme dikatomisinde özel hayatın gizliliğini esas alıp güvenliği sağlama amaçlı özel alana yapılan ihlalleri istisna olarak kabul etmesi gerekirken bunun tersi şekilde hareket edebilmektedirler. Diğer taraftan çalışmada somut örneklerle sistemdeki güvenlik açıklarından bahsedilmişti. Bu bakımdan sistemler, yurttaşın parmak izi gibi biometrik veriler de dahil olmak üzere kişisel verilerin çalınma veya üçüncü şahısların eline geçme ihtimalini içinde barındırmaktadır. Emniyet Teşkilatı'nda özel hayatın gizliliği ihlallerini ve veri güvenliğinin sağlanamamasını engelleyecek hukuki ve sistemsal mekanizmalar bulunmadığından dolayı yurttaşın özel hayatının gizliliğinin tehdit altında olduğu söylenebilir.

Son olarak Emniyet Teşkilatı'ndaki teknolojik dönüşümün neticesinde yurttaş ve kurumsal yapı açısından bazı tehditler barındırdığı kabul edilmelidir. Bu tehditleri bertaraf

etmenin ve gözetim faaliyetlerinin kontrol altında tutulabilmesi için bu çalışmada somut yapısal önerilerde bulunulmuştur. Bu somut önerilerden birincisi Emniyet Teşkilatı'ndaki tüm gözetim sistemlerini ve faaliyetlerini yönetebilecek Emniyet Genel Müdürüne doğrudan bağlı olarak daire başkanlığı şeklinde bir örgütsel yapının oluşturulmasıdır. Bu yapı “Gözetim Kontrol Daire Başkanlığı” şeklinde örgütlenebilir. İkincisi, yurttaşların zihinlerinde gözetimin boyutlarıyla ilgili bir çerçeve çizebilmek ve onları gözetimin oluşturduğu gizemli, baskıcı havadan kurtarmak için Emniyet Teşkilatı'ndaki tüm gözetim faaliyetlerine yönelik belli periyotlarla hazırlanacak şeffaflık raporlarının yayımlanmasıdır.

Gözetim yapısı gereği kamuoyundan gizli gerçekleştirildiğinden dolayı basına ve araştırma kaynaklarına yansıyan bilgilerin tüm gözetim faaliyetlerinin küçük bir bölümünü oluşturduğu düşünülmektedir. Güvenlik korkusuyla görünür görünmez bütün gözetim faaliyetlerine doğrudan ya da dolaylı olarak “evet” diyen yurttaşın her geçen gün daha çok gözetlendiği, daha çok sayısallaştırıldığı, hareketlerinin daha çok hesaplanabilir hale geldiği değerlendirilmektedir. “Hayır” diyen yurttaşların sayısı hissedilmeyecek kadar azdır. Bu durumun iktidar - yurttaş ilişkilerinin orta ve uzun vadede iktidarın “Büyük Biraderleşmesi” ve “totaliterleşmesi” yönünde evrilmesine yol açabileceği değerlendirilmektedir. Belkide süperpanoptikondan sonraki evreyi nitelendirmede Weber'in bürokrasi için uygun gördüğü sıradan insanların içinde avlanmış gibi tutsak kaldığını ifade eden “Çelik Kafes” metaforu ancak yeterli olacaktır. Bu durumun George Orwell'in *Bin Dokuz Yüz Seksen Dört* isimli kitabındaki ana karakter Winston'un aşağıdaki ifadeleriyle sonunda pes ederek Büyük Biraderi kabullenmesi distopyasından bir farkının olmadığı düşünülmektedir.⁸⁰³

“...Halk mahkemesindeydi, itiraf ediyor, herkesi ele veriyordu... Ama olsun, her şey yolundaydı, çekişme son bulmuştu. Kendisine karşı zafer kazanmıştı. Büyük Birader'i seviyordu.”

⁸⁰³ George Orwell, *a.g.k.*, s.258.

KAYNAKÇA

a) Kitaplar

- Akarsu, Bedia, *Felsefe Terimleri Sözlüğü*, TDK Yayınları, 1975.
- Akın, Bahadır, *Yeni Ekonomi: Strateji, Rekabet ve Teknoloji Yönetimi*, Çizgi Kitabevi, Konya, 2001.
- Arifoğlu, Ali, *E-Dönüşüm: Yol Haritası*, Sas Bilişim Yayınları, Ankara, 2004.
- Badiou, Alain, *Etik: Kötülük Kavrayışı Üzerine Bir Deneme*, Çev. Tuncay Birkan, Metis Yayınları, İstanbul 1998.
- Bal, İhsan, Fatih Beren, *Polis Etiği*, Siyasal Kitabevi, Ankara, 2003.
- Ball, Kirstie, Frank Webster ed., *The Intensification of Surveillance*, Pluto Press, London, 2003.
- Bauman, Zygmunt, *Yasa Koyucular ile Yorumcular*, Çev. Kemal Atakay, Metis Yayınevi, İstanbul, 1996.
- Bauman, Zygmunt, *Özgürlük*, Çev. V. Erenus, Sarmal Yayınevi, İstanbul, 1997.
- Bauman, Zygmunt, *Postmodern Etik*, Çev. Alev Türker, Ayrıntı Yayınları, İstanbul, 1998.
- Bell, Daniel, *The Coming of Post-Industrial Society: A venture in Social Forecasting*, Basic Books, New York, 1973.
- Bentham, Jeremy, *The Panopticon Writings*, Verso, Londra, 1995.
- Bentham, Jeremy, Catherine P. Watkin, Simon Werret, *Panoptikon: Gözün İktidarı*, Çev. Barış Çoban, Zeynep Özarslan, Su Yayınları, İstanbul, 2008.
- Bilgi, Alaattin, *Kapital Okuma Klavuzu*, Evrensel Yayın, İstanbul.
- Caputo, Anthony C., *Digital Video Surveillance and Security*, Elsevier Inc, Burlington, 2010.
- Castells, Manuel, *Ağ Toplumunun Yükselişi*, Çev. Ebru Kılınç, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2008.
- Çevik, Hasan H., *Türkiye’de Kamu Yönetimi Sorunları*, Seçkin Yayınları, Ankara, 2004.
- Çoban, Hasan, *Bilgi Toplumuna Planlı Geçiş*, İnkılap Yayınevi, Ankara, 1997.
- Dedeoğlu, Gözde, *Etik Düşünce ve Postmodernizm*, Telos Yayınları, İstanbul, 2004.
- Doğan, Suat, *Küresel Dünyada Terörizm Konsepti*, EGM Basımevi, Ankara, 2004.
- Dolgun, Uğur, *Şeffaf Hapishane Gözetim Toplumu*, Ötüken Yayınevi, İstanbul, 2008.
- Dönmezer, Sulhi, *Ceza Hukuku El Kitabı*, İstanbul, 1989.
- Dura, Cihan, Hayriye Atik, *Bilgi Toplumu, Bilgi Ekonomisi ve Türkiye*, Literatür Yayıncılık, İstanbul, 2002.

- Durmaz, Şükrü, *Bilişim Suçlarının Sosyolojik Analizi*, Ankara, 2006.
- Dülger, Murat V., *Bilişim Suçları*, Seçkin Yayınevi, Ankara, 2004.
- Eren, Erol, *Örgütsel Davranış ve Yönetim Psikolojisi*, Beta Yayınları, İstanbul, 2008.
- Ermann, M. David, vd., *Computers, Ethics and Society*, Oxford University Press, 1997.
- Ertan, Murat, *Tarihi Sözler Antolojisi*, Afşar Matbaacılık, Ankara, 2010.
- Eryılmaz, Bilal, *Bürokrasi ve Siyaset: Bürokratik Devletten Etkin Yönetime*, Alfa Yayınları, İstanbul, 2004.
- Fişek, Kurthan, *Yönetim*, Paragraf Yayınevi, Ankara, 2005.
- Foucault, Michael, *Discipline and Punish: The Birth of the Prison*, Penguin Books, Harmondsworth, 1977.
- Foucault, Michel, *Özne ve İktidar*, Çev. Işık Ergüden, Osman Akınhay, Ayrıntı Yayınları, İstanbul, 2000.
- Foucault, Michel, *İktidarın Gözü*, Ayrıntı Yayınları, İstanbul, 2003.
- Foucault, Michel, *Hapishanenin Doğuşu*, Çev. Mehmet Ali Kılıçbay, İmge Yayınları, Ankara, 2006.
- Aytekin Geleri, *Devriye Polisi*, Seçkin Yayınları, Ankara, 2002.
- Giddens, Anthony, *Ulus, Devlet ve Şiddet*, Çev. Cumhur Atay, Devin Yayınları, İstanbul, 2005.
- Giddens, Anthony, *Sosyoloji*, Çev. Talip Kabadayı, Aytaç Yayınevi, Ankara, 2000.
- Gilbert, Nigel, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, The Royal Academy of Engineering, London, 2007.
- Gleizal, Jacques, vd., *Batı Demokrasilerinde Polis*, Çev. Mustafa Kandemir, Temiz Yayınları, Ankara 2000.
- Gültekin, Buğra, *Türkiye’de E-Devlet Uygulamaları ve Toplumsal Açılımları*, Gazi Üniversitesi, Ankara, 2007.
- Gürkan, Emrah, *Ne Kadar Muasırlaşabildik? 80. yılında Cumhuriyet*, Güncel Kitaplar Yayınevi, Ankara, 2003.
- Haspolat, Evren, *Neoliberalizm ve Baskı Aygıtının Dönüşümü: Türkiye’de Özel Güvenliğin Gelişimi*, Notabene Yayınları, Ankara, 2012.
- Kaya, Elif Aksu, *Emek Süreçlerinde Dönüşüm ve Mühendis Emeği*, Elektrik Mühendisleri Odası E-Kitap Yayını, Ankara, 2012.
- Kaygısız, Mustafa, *Adli Bilimler*, Seçkin Yayınları, Ankara, 2005.
- Koçel, Tamer, *İşletme Yöneticiliği*, Beta Yayınları, İstanbul, 1998.

- Lyon, David, *Elektronik Göz: Gözetim Toplumunun Yükselişi*, Çev. Dilek Hattatoğlu, Sarmal Yayınları, İstanbul, 1997.
- Lyon, David, *Gözetlenen Toplum*, Çev. Gözde Soykan, Kalkedon Yayınevi, İstanbul, 2006.
- Martin, Brian, *Information Liberation Challenging the Corruptions of Information Power*, Freedom Press, London, 1998.
- Marx, Karl, *Kapital*, Çev. Alaattin Bilgi, Sol Yayınları, Ankara, 1993.
- Marx, Karl, Friedrich Engels, *Komünist Parti Manifestosu*, Çev. Yılmaz Onay, Evrensel Yayın, İstanbul, 2007.
- Miller, Arthur R., *The Assault on Privacy: Computerrs, Data Banks and Dossiers*, The University of Michigan Press, 2. Edition, 1971.
- Mitchell, William J., *City of Bits*, MIT Press, Cambridge, 1996.
- Morgan, Gareth, *Metafor*, Çev. Gündüz Bulut, Mess Yayınları, İstanbul, 1998.
- Nedret, Ersanel, *Siber İstihbarat*, Asam Yayınları, Ankara, 2001.
- Neyland, Daniel, *Privacy, Surveillance and Public Trust*, Palgrave Macmillan, New York, 2006.
- Orwell, George, *Bin Dokuz Yüz Seksen Dört*, Çev. Nuran Akgören, Can Yayınları, İstanbul, 2008.
- Öğüt, Adem, *Bilgi Çağında Yönetim*, Nobel Yayın Dağıtım, Ankara, 2001.
- Özçağlayan, Mehmet, *Yeni İletişim Teknolojileri ve Değişim*, Alfa Basım Yayım Dağıtım, İstanbul, 1998.
- Özdemir, Gamze Yücesan, *İletişim Emek ve Kalkınma: Ekonomi Politik Yaklaşım*, Gazi Üniversitesi İletişim Fakültesi Basımevi, Ankara, 2008.
- Özdemir, Gamze Yücesan, *Emek ve Teknoloji*, Tan Yayınları, Ankara, 2009.
- Pehlivan, İnayet, *Yönetmel Mesleki ve Örgütsel Etik*, Pegem Yayınları, Ankara, 1998.
- Petersen, Julie K., *Understanding Surveillance Technologies*, Taylor and Francis Group, New York, 2007.
- Pieper, Annemarie, *Etğe Giriş*, Çev. Veysel Atayman, Ayrıntı Yayınları, İstanbul, 1999.
- Sofsky, Wolfgang, *Privacy: A Manifesto*, Princeton University Press, Princeton, 2008.
- Staples, William G., *The Culture of Surveillance: Dicipline and Social Control in the United States*, St. Martin's Press, New York, 1997.
- Şahin, Haluk, *Yeni İletişim Ortamı, Demokrasi ve Basın Özgürlüğü*, Anadolu Matbaası, İstanbul, 1991.
- Şimşek, Hasan, *Örgütler, Yönetim ve Liderlik: Liderliğe Çoklu Bakış*, ODTÜ Eğitim Fakültesi Eğitim Bilimleri Bölümü Yayını, Ankara, 2005.

- Tanilli, Server, *Yaratıcı Aklın Sentezi: Felsefeye Giriş*, Adam Yayınları, Ankara, 1998.
- Taylor, Frederick W., *Bilimsel Yönetimin İlkeleri*, Çev. H. Bahadır Akın, Adres Yayınları, Ankara, 2005.
- Uçkan, Özgür, *E-Devlet, E-Demokrasi ve Türkiye Kamu Yönetiminin Yeniden Yapılanması İçin Strateji ve Politikalar*, Literatür Yay., İstanbul, 2003.
- Uzun, Ruhdan, *İletişim Etiği Sorunlar ve Sorumluluklar*, Gazi Üniversitesi İletişim Fakültesi Basımevi, Ankara, 2007.
- Vasseur, Frederic, *Geleceğin Medyaları*, Çev. Galip Üstün, İletişim Yayınları, İstanbul, 1993.
- Weber, Max, *Toplumsal ve Ekonomik Örgütlenme Kuramı*, Çev. Özer Ozankaya, İmge Kitapevi, İstanbul, 1995.
- Weber, Max, *Sosyoloji Yazıları*, Çev. Talha Parla, Deniz Yayınları, İstanbul, 2006.
- Wood, David Murakami (ed.), *A Report on the Surveillance Society*, Surveillance Studies Network, September 2006.
- Yaşar, Yılmaz, *Polis Meslek Hukuku*, Mustafa Kitabevi, Ankara, 2007.
- Yazıcıoğlu, Yılmaz, *Bilgisayar Suçları*, Alfa Yayınları, İstanbul, 1997.
- Yıldırım, Hakan, vd., *E-Devlet Başa*, Macar Yayıncılık, Ankara, 2006.
- Yurdakul, Ceyhun, H. Ufuk Çağlayan, *Bilgi teknolojileri Türkiye İçin Nasıl Bir Gelecek Hazırlamakta*, Kültür Yayınları, Ankara, 1997.

b) Makaleler

- Akbulut, Berrin B., “Bilişim Suçları”, *Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı*, S. 1-2, C.8, 2000, s. 546.
- Alkan, Necati, “Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler”, *Çağın Polisi Dergisi*, Ağustos 2003, Sayı 20, s.41-42.
- Anderson, Donald N., “The Spy in the Cab: The Use and Abuse of Taxicab Cameras in San Francisco”, *Surveillance and Society*, Sayı 10, s. 150-166. <http://www.surveillance-and-society.org>.
- Ataç, Ela, Davut Gürbüz, “Kentsel Mekanda Gelişen Suça Müdahale Etmede Disiplinlerarası Güvenlik Politikaları”, *Polis Bilimleri Dergisi*, Cilt: 11, 2009, s. 28-29.
- Atmaca, Kemal “E-Devletten Olgun Devlete ya da E-Devlet’in Olgunlaştırılması”, s.8., www.mfa.gov.tr.

- Aydın, Burak, “E-Devlet Kapsamında Emniyet ve Diğer Kamu Kurumlarının Bütünleşmesi”, *1.Polis Bilişim Sempozyumu*, EGM Bilgi İşlem Dairesi Başkanlığı Yayınları, Ankara, 2003, s.27.
- Ball, Kirstie, Frank Webster, “The Intensification of Surveillance”, *The Intensification of Surveillance*, Ed. Kirstie Ball, Frank Webster, Pluto Press, London, 2003.
- Baştan, Serhat, Ramazan Gökbnar, “Kamu Hizmetlerinin Sunumunda E-devletle İlgili Yeni Gelişmeler: Tümüleşik E-devlet Sistemlerine Doğru”, *D.E.Ü.İ.İ.B.F.Dergisi*, Cilt 19, Sayı 1, 2004, s.72.
- Bell, Daniel, “İletişim Teknolojisi: Gidişat Daha İyiye mi Yoksa Daha Kötüye mi?”, Çev. Ahmet Sevimli, *Sosyo-Ekonomik Perspektif*, Der. Uğur Dolgun, Asa Yayıncılık, Bursa, 2001, s.309.
- Bennett, Colin J., “Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web”, *Ethics and Informaion Technology*, Vol. 3, Issue 3, 2001, s.197 - 205.
- Bennett, Colin J., “Privacy in the Political Systems: Perspectives from Political Science and Economics”, 1995, s. 11. <http://web.uvic.ca/polisci/bennett/pdf/westinbook.pdf>.
- Bozkurt, Veysel, “Gözetim Toplumu ve İnternet”, <http://www.uludag.edu.tr>.
- Brown, Mary M., Jeffrey L. Brudney, “Achieving Advanced Electronic Government Services: An Examination of Obstacles and Implications from an International Perspective”, 2001, s.1 <http://www.spea.indiana.edu/NPMRC6/Brown&Brudney.doc>.
- Bygrave, Lee, “Data Protection Pursuant to the Right to Privacy in Human Right Treaties”, *International Journal of Law and Information Technology*, Vol. 6, No. 3, s. 247 - 284.
- Cerrah, İbrahim, “Polis”, *Almanak Türkiye: Güvenlik Sektörü ve Demokratik Gözetim*, Ed. Ümit Cizre, Tesev Yayınları, İstanbul, 2005, s.94.
- Civelek, Dilek Y., “Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi”, *Bilgi Toplumu Dairesi Başkanlığı*, Yayın No: 2821, Ankara, 2011, s.25.
- Coşkun, Enis, “Amaç Gözetlememi, Güvenlik mi?”, <http://izleniyoruz.50webs.com/oku8.html>.
- Cozetto, Don A., Theodore B. Pedeliski, “Privacy and the Workplace: Technology and Public Employment”, *Public Personnnel Management*, Vol 26, Issue 4, 1997, s.518 - 519.
- Çapar, Selim, “Open Street Surveillance in The UK and Turkey”, *Egovshare*, 2009, s.31. www.edem.todaie.gov.tr.
- Çiçek, Kemal, “Osmanlı Devletinde Asayiş ve Emniyet Hizmetleri”, *Avrupa Birliği Sürecinde Türk Polisi Uluslararası Sempozyumu*, EGM Basım, Ankara, 1997, s.123.

- Çoban, Erin, “Ülkemizin Yeni Bilgi ve Güvenlik Konsepti Mobese”, *Polis Dergisi*, Sayı 43., http://www.egm.gov.tr/egitim/dergi/eskisayi/45/web/makaleler/Erin_COBAN.htm.
- Doğan, Halil İ., Bilal Sevinç, “Suç Teorileri ve Şehir Güvenliği: Bitlis İliyle İlgili Genel Bir Değerlendirme”, *Polis Bilimleri Dergisi*, Cilt:13 (4), 2011, s.31.
- Dokurer, Semih, “Adli Bilişim”, www.logyonetimi.com/doc/adlibilisim.pdf.
- Dolgun, Uğur, “Gözetim Devleti, ‘Penguenler’, ABD ve FBI Örneği”, 20.06.2013 tarihli *Taraf Gazetesi Köşe Yazısı*.
- Elektrik Mühendisleri Odası, “Elektronik Gözaltı Dünyası: e-Göz@ltı”, www.emo.org.
- Ercan Kurt, “Hacker’lığın Kısa Tarihçesi”, <http://www.olympos.org/article/articleview/283/1/10,2004>.
- Erdal, Murat, “Tekno - Güvenlik Problemlerinin Uluslararası İlişkilerdeki Yeri ve Türkiye”, *İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, Sayı 21-22, İstanbul, 2000, s.23 - 34.
- Eren, Veysel, Uğur Durna, “Kamu Hizmetlerinin Daha İyi Görülebilmesi İçin Alternatif Bir Yönetim Yaklaşımı: Elektronik Devlet”, *İ.Ü. SBF Dergisi*, Sayı: 32, Mart 2005, s.155 - 156.
- Gandy, Oscar, “The Surveillance Society: Information Technology and Bureaucratic Social Control”, *Journal of Communication*, Vol 39, Issue 3, 1989, s. 67.
- Gangadharan, Seeta Pena, “Joining the Surveillance Society”, *New America Foundation*, Eylül 2013, s.2. <http://newamerica.net>.
- Geray, Haluk, “1980 Sonrası Yeni Teknolojiler ve İkitelli Medyası”, *Medya Gücü ve Demokratik Kurumlar*, Afa Yayıncılık, İstanbul, 1999, s.107.
- Geray, Haluk, “Enformasyon Toplumu ve Türkiye: Erişim Açısından Bir Değerlendirme”, *Yeni Türkiye Dergisi*, Yıl 4, Sayı 20, 1998, s.1416.
- Göçmen, Doğan, “Marx’ın Emek Kavramının Bugün Yürütülen Tartışmalar İçin Önemi Üzerine”, 2009, s.4., <http://dogangocmen.wordpress.com>.
- Göker, Aykut, “Enformasyon Toplumu Üzerine Kavramsal Bir Yaklaşım Denemesi”, <http://www.inovasyon.org/pdf/AYK.Mulkiye.Der.Ag.01.pdf>.
- Görgün, İpek, “Denetim Topluluklarındaki Gözetleyen - Gözetlenen İlişkisi Bağlamında Mobese ve Nobese Projeleri”, 2009, s.7., <http://izleniyoruz.50webs.com/biz.html>.
- Güldiken, Nevzat, “Türkiye’de Sanayi -Teknoloji - Kobi Politikalarına Eleştirel Bir Yaklaşım”, *C.Ü. İktisadi ve İdari Bilimler Dergisi*, Cilt 7, Sayı 2, 2006, s.143.
- Gürak, Hasan, “Teknolojik Yenilik ve Büyüme”, <http://www.hasmendi.net>.
- Gürdilek, Raşit, “Echelon”, *Bilim Teknik Dergisi*, Ekim 2001, s. 36 - 37.

- Hepaksaz, Engin, Betül Hayrullahoğlu, “E-Devlet Kapsamında Vedop Uygulamaları ve E-Haciz”, *Sosyal ve Beşeri Bilimler Dergisi*, Cilt 3, No 2, 2011, s.112.
- İrızık, Gürol, “Bilgi Toplumu mu, Enformasyon Toplumu mu? Analitik - Eleştirel Bir Yaklaşım”, *Bilgi Toplumuna Geçiş: Sorunsallar, Görüşler, Yorumlar, Eleştiriler ve Tartışmalar*, Der. İlhan Tekeli. vd., Türkiye Bilimler Akademisi Yayınları, No.3, Ankara, 2002, s.54.
- İnam, Şaban, Hakan Ayber, “E-devlet İçerisinde E-kadastro ve E-tapunun Yeri”, *Selçuk Üniversitesi Jeodezi ve Fotogrametri Mühendisliği Öğretiminde 30. Yıl Sempozyumu*, Konya, 16-18 Ekim 2002.
- Kalfa, Aslıcan, Hakan Topateş, “Çalışma İlişkilerinde Denetimin Gizilleşmesi Bağlamında Elektronik Gözetim Pratiklerinin Otoritesi”, *Sosyal Haklar Ulusal Sempozyumu*, s.438., www.sosyalhaklar.net.
- Kara, Hakan, “İnternet, Gazetecilik ve Yeni Olanaklar”, *Siyahbeyaz*, Der. Serhan Yedig, Haşim Akman, Metis Yayınları, İstanbul, 2002, s.37-42.
- Karakehya, Hakan, “Gözetim ve Suçla Mücadele”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2009, C.58 S.2, s. 333 - 335.
- Keleş, Ruşen, “Kente Karşı Suç”, *TMMOB Mimarlar Odası Ankara Şubesi*, Bülten 55, Ankara, Kasım - Aralık 2007, s.45.
- Ketizmen, Muammer, Çağlar Ülküder, "E-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması", www.inet-tr.org.tr/inetconf12/bildiri/2.pdf.
- Kocabal, Ahmet, “Cumhuriyet, Türk Polisi ve Bilgi İşlem”, <http://www.caginpolicisi.com.tr>.
- Kocabal, Ahmet, “Polnet ve Emniyet Bilgi Sistemi”, <http://www.caginpolicisi.com.tr/26/16-17-18-19.htm>.
- Kocabal, Ahmet, “Polnet ve Transpol”, <http://www.caginpolicisi.com.tr>.
- Koyun, Ali, Abdullah S. Öztürk, “Toplumsal Kontrol ve Gözetim Araçlarından Olan Mobese Teknolojisinin İşlevselliği Konusunda Halkın Bilinç Düzeyi”, *Sosyoloji Alanı Orta Öğretim Öğrencileri Arası Araştırma Projeleri Yarışması*, Tubitak, Bursa, 2012, s.4-5.
- Lee, Samantha, Brian H. Kleiner, “Electronic Surveillance in the Workplace”, *Management Research News*, Volume 26, Issue 2-3-4, 2003, s.74.
- Lefort, Claude, “What is Bureaucracy?”, s.4., www.generation-online.org/h/fplefort.
- Lyon, David, “Surveillance after September 11, 2001”, *The Intensification of Surveillance*, Ed. Kirstie Ball, Frank Webster, 2003, s.17 - 18.

- Lyon, David, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies", *Surveillance as Social Sorting*, Ed. David Lyon, Taylor and Francis e-Library, New York, 2005, s.2.
- Lyon, David, Christian Holler, "Surveillance Systems Towards an Electronic Panoptical Society?", 1997.
- Man, Fuat "Kapitalist Emek Süreci Teorisi ve Dönüşümü", *E-Akademi*, Aralık 2009, Sayı 94.
- Marx, Gary T., "An Ethics For the New Surveillance", *The Information Society*, <http://www.mit.edu/gtmarx/nicolin5.html>.
- Marx, Gary T., "Surveillance and Society", *Encyclopedia of Social Theory*, 2005, s.1. <http://web.mit.edu/gtmarx/www/surandsoc.html>.
- Marx, Gary T., "What's New About the 'New Surveillance' Classifying for Change and Continuity", s.10 - 11., <http://www.surveillance-and-society.org/journalv1i1.htm>.
- Moor, James H., "What is Computer Ethics?", *Metaphilosophy*, Vol:16(4), 1985, s. 226 - 275.
- Önder, Murat, "Toplam Kalite Yönetimi, Kamu Sektöründe Uygulanması ve Karşılaşılan Sorunlar", *Türk İdare Dergisi*, s. 416, Eylül 1997, s. 119.
- Öngen, Tülin, "Marx ve Sınıf", *Praksis*, Sayı 8, s. 18.
- Özbaran, Yavuz, "Trafik Bilgi Sistemi", 2. *Polis Bilişim Sempozyumu Sunum Bildirileri*, Ankara, 2005, s.4.
- Özcan, Mehmet, "Siber Terorizm ve Ulusal Güvenlik", *İnternet ve Hukuku*, Der., Yesim M. Atamar, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s.324 - 325.
- Özdemir, Ali R., Oktay Öksüzler, "Bilgi ve İletişim Teknolojilerinin Kamu Sektörünün Büyüme Hızı Üzerine Etkileri: Bir OECD Panel Verileri Regrasyon Analizi", s.389. www.iibf.ogu.edu.tr/kongre/bildiriler/09-03.pdf.
- Özdemir, Gamze Yücesan, "Despotik Emek Rejimi Olarak Taşeron Çalışma", *Çalışma ve Toplum*, Sayı 4, 2010, s. 37.
- Özdemir, Gamze Yücesan, "Emek Süreci Teorisi ve Türkiye'de Emek Süreci Çalışmaları Üzerine Bir Değerlendirme", *Küreselleşme, Emek Süreçleri ve Yapısal Uyum*, Der. A. A. Dikmen, İmaj Yayıncılık, Ankara, 2002, s.441 - 442.
- Özdilek, Ali Osman, "Hizmet Akitlerinde Gizlilik Maddesinin Bilişim Teknolojileri Kullanımı Açısından Değerlendirilmesi", <http://www.hukukcu.com/bilimsel/kitaplar/hizmetakitlerivebilisim.html>.
- Özsarı, Haluk "Türkiye'de Sağlık Reformu Süreci ve Sağlık Enformasyon Sistemleri İle İlişkisi", www.sbu.saglik.gov.tr.

- Öztürk, Lütfü, “Türkiye’de Dijital Eşitsizlik: Tübitak - Bilten Anketleri Üzerine Bir Değerlendirme”, *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, Sayı 24, 2005, s. 111-131.
- Payne, Timothy Pitt, “The Surveillance Society In And Out of The Workplace”, June 2009, s.1., www.11kbw.com/articles/docs/SurveillancesocietyTPP.pdf.
- Poole, Steven, “Fear of The Unknown”, *The Guardian*, 10.01.2009., www.theguardian.com.
- Popal, Mirela, Alper Kemal Koç, “Kinect Sensing of Shopping related Actions”, s.1.
- Poster, Mark, “Databases as Discourse; or Electronic Interpellations”, *In Computers, Surveillance and Privacy*, Ed. David Lyon, Elia Zureik, University of Minnesota Press, Minneapolis, 2001, s. 175 - 192.
- Preifffer, Eric, “Watchdog”, *Yahoo News*, 23.10.2013.
- Salman, Banu, “Bilgi ve İletişim Teknolojileri Kullanan mı Üreten mi Olacağız?”, www.emo.org.
- Sayılı, Müslüm, “Dünyada Gelişen Teknolojik Yenilikler ve Türk Polis Teşkilatına Adaptasyonu”, *21. Yüzyılda Polisin Eğitimi Sempozyumu*, Ankara, EGM Yayınları, 2001, s.781.
- Sözen, Üzeyir, “Polis’ten E-Polis’e”, <http://www.egm.gov.tr/egitim/dergi/eskisayi/37>.
- Stalder, Felix, “Opinion. Privacy Is Not The Antidote to Surveillance”, *Surveillance and Society*, Vol. 1, Issue 1, 2002, s.125. <http://www.surveillanceand-society.org/articles1/opinion.pdf>.
- Şahin, Ali, H. Temizel, M. Temizel, “Türkiye’de Demokrasiden E-Demokrasiye Geçiş Süreci ve Karşılaşılan Sorunlar”, s.1., <http://iibf.ogu.edu.tr/kongre/bildiriler/06-02.pdf>.
- Şen, Bilal, “Elektronik Gözetim”, s.1., <http://www.genbilim.com/content/view/8025/91>.
- Şen, Mustafa L., “Kamu Yönetiminde Yozlaşmanın Önlenmesinde Yönetmelik Yaklaşımı”, *Basılmamış Doktora Tezi*, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, İzmir, 1998, s.96.
- Şen, Osman N., “Polisin Bilişim Suçlarıyla Mücadelede Yapması Gerekenler”, *1. Polis Bilişim Sempozyumu*, Ankara, 2003, s.70 - 71.
- Törenli, Nurcan, “E-Devlet’in Ekonomi-Politiğine Giriş”, *Ankara Üniversitesi SBF Dergisi*, Sayı 60-1, s.192.
- Tulum, İsmail, “Bilişim Suçları ile Mücadele”, *Yüksek Lisans Tezi*, Süleyman Demirel Üniversitesi, Isparta, 2006, s.36.
- Tümurtürkan, Meral, “Gündelik Hayatın Gözetimi: Panoptikon Toplumu”, *Ethos: Felsefe ve Toplumsal Bilimlerde Diyaloglar*, Sayı 3 (2), Temmuz 2010, s.6.

- Türkoğlu, Recep, “Bilişim Teknolojilerinden Bilgi Yönetiminde Yararlanma Düzeyi”, http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=615.
- Uludağ, Şener, “Vatandaşların Suç Korku (Güvenlik Endişesi) Seviyesine Etki Eden Faktörler ve Alınabilecek Önlemler: Malatya Örneği”, *Polis Bilimleri Dergisi*, Cilt:12 (1), 2010, s.3.
- Wood, David, Eli Konvitz, Kirstie Ball, “The Constant State of Emergency?: Surveillance after 9/11”, *The Intensification of Surveillance*, Ed. Kirstie Ball, Frank Webster, 2003, s. 143.
- Yıldız, Mete, R.Erdem Erkul, “Elektronik Göz ve Türkiye’de Kameralı Hayat”, <http://www.inet.tr.org.tr>.
- Yüksel, Mehmet, “Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar”, *Ankara Üniversitesi SBF Dergisi*, Sayı 64 - 1, Ankara, Haziran 2009, s.292.
- Zamir, Yusuf, “1917 Devriminin Boğuluşu”, *Yaşayan Marksizm*, Sayı 3, İstanbul, Ocak 2012, s.127.

c) Raporlar

- Avrupa Birliği, *2003 E-Avrupa Eylem Planı*, Haziran 2001.
- Council of Europe, *Organised Crime Situation Report: Focus on The Threat of Cybercrime*, Strasbourg, 10 Eylül 2004.
- Cumhurbaşkanlığı Devlet Denetleme Kurulu, *Denetleme Raporu*, Sayı 2013 / 3, 27 Kasım 2013.
- DPT Bilgi Toplumu Dairesi Başkanlığı, *E-Devlet Proje ve Uygulamaları*, Nisan 2004.
- Devlet Planlama Teşkilatı, *Bilgi Toplumu İstatistikleri*, 2011.
- Devlet Planlama Teşkilatı, *Sekizinci Beş Yıllık Kalkınma Planı: Bilişim Teknolojileri ve Politikaları Özel İhtisas Komisyonu Raporu*, Ankara, 2001.
- EGM Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, *2009 Faaliyet Raporu*, Ankara, 2010.
- Gelir İdaresi Başkanlığı, *2010 Yılı Faaliyet Raporu*, 2011.
- OECD, *OECD Policy Guidance on Online Identity Theft*, Haziran 2008.
- Office of Surveillance Commissioners, *2012-2013 Dönemi Senelik Raporu*, Temmuz 2013.
- Sayıştay Başkanlığı, *Performans Denetimi Raporu: E-Dönüşüm Türkiye Projesi Çerçevesinde Yürütülen Faaliyetler*, 2006.

Sosyal Güvenlik Kurumu, *Avuç İçi Damar İzi Sistemiyle Kimlik Doğrulama Sistemine Ait Kılavuz*, 2012.

Tubitak, *Tuena Sonuç Raporu*, Ekim 1999.

Yüksek Planlama Kurulu, *Bilgi Toplumu Stratejisi 2006-2010*, 28 Temmuz 2006.

d) Haber Kaynakları

Aktifhaber, “Tüm Kimlik Bilgilerimiz Ellerinde”, 27.07.2010.

Radikal, “Böcek Komisyonu Başkanı: MOBESE Dahil Tüm Kameralar Kaldırılsın”
21.02.2013.

Radikal, “Telekulak Komisyonu: MİT’i Başbakanlık Teftiş Kurulu Denetlesin”, 07.06.2013.

Sabah, “FBI’nın 'Kartal Gözü' Türkiye’de”, 15.12.2012.

Sabah, “Çapkın Erkeklerle Mozaikle Koruma”, 16.03.2013.

The Guardian, “CCTV Aimed at Muslim Areas in Birmingham to Be Dismantled”,
25.10.2010.

TRT 2, “Birgül Ayman Güler’in Küresel Sömürgecilik Konulu Söyleşisi”, 23.01.2004.

e) Filmler

Henckel, Florian, *Das Leben der Anderen*, Film, Almanya, 2006.

Niccol, Andrew, *Gattaca*, Film, ABD, 1997.

Radford, Michael, *Bin Dokuz Yüz Seksen Dört*, Film, İngiltere, 1984.

Spielberg, Steven, *Azınlık Raporu*, Film, ABD, 2001.

f) İnternet Siteleri

<http://ankara.pol.tr/kgys/index.php>.

http://bilgi.didikle.com/Telematik_nedir.html.

<http://bilisimsurasi.org.tr/cg/rapor/rapor.zip>.

<http://dinlemecihazlari.com/dinleme-cihazlari/mini-bocek-dinleme-cihazlar.html>.

<http://en.wikipedia.org>.

<http://findbiometrics.com/solutions/facial-recognition/>.

<http://hurarsiv.hurriyet.com.tr/goster/haber.aspx?id=5822235&tarikh=2007-01-23>.

<http://iibf.erciyes.edu.tr/dergi/sayi24/lozturk.pdf>.

<http://inet-tr.org.tr>.

<http://mobese.iem.gov.tr/asos.htm>.

<http://msg-itlg.blogspot.com/2008/01/advantagesdisadvantages-of-electronic.html>.
http://news.bbc.co.uk/2/hi/uk_news/6108496.stm.
<http://news.yahoo.com/nsa-spied-on-124-8-billion-phone-calls-in-just-one-month--watchdog-group-claims-213633988.html>
http://oxforddictionaries.com/view/entry/m_en_gb0176220#m_en_gb0176220.
<http://police.homeoffice.gov.uk/operationalpolicing/impact/impact-about-the-programme/>.
<http://sciencefocus.com>.
<http://siyaset.milliyet.com.tr/dinleme-otomatige-mi-baglandi/siyaset/siyasetdetay/22.12.2008/1031013/default.htm>.
<http://sondakika.com/haber-eczane-provizyon-sistemi-nedeniyle-hasta-ve-2331077/>.
<http://tks.ibb.gov.tr/noc-player.php?id=35>.
<http://topsy.com/analytics>.
<http://turk.internet.com/haber/yazigoster.php3?yaziid>.
<http://web.mit.edu/gtmarx/www/surandsoc.html>.
<http://web.tkgm.gov.tr>.
<http://www.abs.gov.au/websitedbs/c311215.nsf/web/Crime+Victimisation+in+my+state>.
<http://www.anu.edu.au/people/Roger.Clarke/DV/DV2005.html>.
<http://www.basarsoft.com.tr>.
<http://www.bilgiguvencligi.gov.tr/...tc-kimlik-karti-ve-euygulamalari/download.html>.
http://www.bilgitoplumu.gov.tr/Documents/3/Diger/010600_eAvrupa+EylemPlani.pdf.
<http://www.bilisinterimleri.com/?arananterim=frame&dil=eng>.
<http://www.casuskamerafiyat.com>.
http://www.cyber-warrior.org/Forum/e-devletin-zararlari_315613,0.cwx.
http://www.dallaspolice.net/dpd/_crimereport.html.
<http://www.digitaldivide.org/dd/digitaldivide.html>.
<http://www.economist.com/node/1280806>.
<http://www.e-demokrasi.org/index.php?option=com>.
<http://www.egm.gov.tr>.
<http://www.ekap.com.tr>.
<http://www.ekodialog.com>.
<http://www.elektrotekno.com/about25604.html>.
<http://www.epaperflip.com/>.
<http://www.ethosfelsefe.com/ethosdiyaloglar/mydocs/Ethos-7%20Gozetim.pdf>.
<http://www.etymonline.com/index.php>.

<http://www.felsefeekibi.com/site/default.asp?PG=1270>.

<http://www.gartner.com>.

http://www.genbilim.com/index.php?option=com_content&task=view&id=3922.

http://www.gib.gov.tr/fileadmin/faaliyetraporlari/2010/Faaliyet_raporu_2010.pdf.

<http://www.gumruk.gov.tr>.

<http://www.gumrukticaret.gov.tr>.

<http://www.haberler.com/askeri-casusluk-davasi-nda-yeni-belgeler-5036186-haberi/>.

<http://www.hardwarehaber.com/haberbak.php?id=1677>.

<http://www.heise.de/tp/r4/artikel/8/8026/1.html>.

<http://www.hukuki.net/hukuk/index.php?article=445>.

http://www.ikieylul.com.tr/yazar_goster.asp?ne=y48&sira=4312.

<http://www.internetworldstats.com/stats.htm>.

<http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>.

<http://www.ip-numaram.com/ipadres.html>.

<http://www.iskur.gov.tr>.

<http://www.izleniyoruz.net>.

<http://www.kyk.gov.tr>.

<http://www.meb.gov.tr>.

<http://www.medyaplaza.net/03.html>.

<http://www.memurlar.net/haber/15517/>.

<http://www.merriam-webster.com/dictionary/control>.

<http://www.merriam-webster.com/dictionary/surveillance>.

<http://www.meslekiyeterlilik.com>.

<http://www.mhrs.gov.tr/>.

<http://www.mkutup.gov.tr>.

<http://www.mmd.org.tr/eserler/yeniekonomidedevletin.pdf>.

<http://www.modelt.ca/background.html>

<http://www.netscantools.com>.

<http://www.nvi.gov.tr>.

<http://www.olay.com.tr/haber/bursa-bolge/mobese-sadece-ceza-yazmiyor-137765.html>.

http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Social_control.html.

<http://www.privacyinternational.org/survey>.

<http://www.sbu.saglik.gov.tr>.

<http://www.securitynewsdesk.com/2013/07/11/bsia-attempts-to-clarify-question-of-how-many-cctv-cameras-in-the-uk/>.

<http://www.sgk.gov.tr>.

<http://www.sileo.com/biometric-identity-theft/>.

<http://www.spypig.com/>.

<http://www.statisticbrain.com>.

<http://www.stratejikboyut.com>.

http://www.tbmm.gov.tr/arastirma.../bilisim.../kalkinma_bakanligi.pptx.

<http://www.tdk.gov.tr>.

http://www.teknolojide.com/e-egitim_1087.aspx.

<http://www.telefondinleme.org/>.

<http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>.

<http://www.tramer.org.tr>.

<http://www.trftescil.iem.gov.tr/>.

<http://www.trt.net.tr/haber/HaberDetay.aspx?HaberKodu=a6222353-8588-485a-af47-ec075d7b27de>.

<http://www.tuik.gov.tr>.

http://www.turkoglu.name.tr/by_makale.htm.

<http://www.uyap.gov.tr>.

<http://www.vatanim.com.tr/root.vatan?exec=haberdetay&tarih=06.11.2006&Newsid=92233&Categoryid=7>.

<http://www.videomining.com/technologies/main.html>.

<http://www.wardom.org>.

<http://www.workrights.org>.

<http://www.yasanacakdunya.net/index.php?URL=kategorie&id=1023>.

<http://www1.oecd.org/publications/e-book/4203071E.PDF>.

<http://yayim.meb.gov.tr/dergiler/sayi45/akcadag.htm>.

<http://yte.bilgem.tubitak.gov.tr>.

<https://www.eff.org/nsa-spying>.

Polnet İtranet Sistemi.

ÖZET

Gözetim, denetimin bir aracı olarak tarihin her döneminde var olmuştur. Her dönemde, dönemin şartlarına göre şekil alarak günümüze kadar süregelmiştir. İlk çağlardaki gözetim, daha çok şiddet ve baskıyla, kabile, imparatorluk ya da monarşiler gibi iktidarların gücünü destekleyen bir unsur olarak vuku bulmuştur. Modern toplumların oluşmasıyla birlikte, gözetimin kaynağı şiddet ve baskıdan yönetime kaymış ve gözetim sistematik bir hal almıştır. Günümüzde gözetimin gelişen bilgi ve iletişim teknolojileri aracılığıyla kullanılmak suretiyle kapasitesi ve hedef kitlesi genişlemiştir. Bu kapsamda gerçek anlamda gözetim toplumunun varlığından bahsedilir olmuştur. Ayrıca gözetim faaliyetleri ulusal sınırların da dışına çıkmış, küresel bir boyut kazanmıştır.

Üç bölümden oluşan bu çalışmada Türkiye'deki gözetim toplumu tehlikesine dikkat çekilmiş ve bu kapsamda Emniyet Teşkilatı bünyesindeki Polnet ve Mobese gözetim araçları incelenmiştir. Bunların yurttışa ve topluma bakan ve kurumsal anlamda oluşturduğu tehditlere dikkat çekilmiştir. Bütün bu tehditleri yok etmek amacıyla gözetimin yönetimine yönelik somut yapısal öneriler geliştirilmiştir.

Anahtar Kelimeler: Gözetim, Denetim, Gözetim Toplumu, Polnet, Mobese, Emniyet Teşkilatı, Gözetimin Yönetimi

ABSTRACT

Surveillance has been in every period of history as a tool of social control. It has continued until today according to conditions of the period. Initially, surveillance was like a supporting fact of power actors such as monarchies, imperials, tribes with violence and oppression. With growing of modern societies, surveillance's source was turned from violence and oppression to administration in which surveillance was initiated to being executed systematically. Nowadays surveillance capacity and influence area have been expanded owing to information and communication technologies. In this context, surveillance society's presence has been occurred exactly. Moreover surveillance activities have been globalized.

In this study which is comprised of three parts, it is mentioned firstly surveillance society risk in Turkey then Polnet and Mobese surveillance tools in "Emniyet Teşkilatı" which is domestic security unit. Especially it is focused on threats of these tools in terms of citizens, society and institution. In order to eliminate these threats some tangible recommendations are made.

Key Words: Surveillance, Control, Surveillance Society, Polnet, Mobese, Emniyet Teşkilatı, Surveillance's Control

EK I

Derinlemesine Görüşmeler

Emniyet Genel Müdürlüğü: 10-11 Ekim 2013

EMNİYET GENEL MÜDÜRLÜĞÜ			
Görüşülen Kişi	Görüşme Yeri	Görüşmeyi Yapan	Tarih
Bilgi Teknolojiler Daire Başkanlığı'nda Polnet Konusunda Uzman Emniyet Görevlisi	Emniyet Genel Müdürlüğü Merkez Bina	Özgür Günaydın	10 Ekim 2013
Bilgi Teknolojiler Daire Başkanlığı'nda Polnet Konusunda Uzman Bilgisayar Mühendisi Personel	Emniyet Genel Müdürlüğü Merkez Bina	Özgür Günaydın	10 Ekim 2013
Haberleşme Dairesi Başkanlığı'nda Mobese Konusunda Uzman Emniyet Görevlisi	Emniyet Genel Müdürlüğü Merkez Bina	Özgür Günaydın	11 Ekim 2013

EK II

“Türkiye’de Emniyet Teşkilatı’nda Teknolojik Yeniden Yapılanma: Denetim ve Gözetimin Değişen Doğası” adlı Yüksek Lisans Tezi

POLNET ve MOBESE UZMANLARI İÇİN DERİNLEMESİNE GÖRÜŞME FORMU

1. Polnet/Mobese Projeleri nedir? Bunların genel teknik özellikleri nelerdir?
2. Polnet iletişim altyapısı nasıldır. Bu sistemin üzerinde çalışan başka projeler var mıdır? Varsa bunlar nelerdir?
3. Mobese Projesi bileşenleri nelerdir? Bu bileşenlerin fonksiyonları nasıldır?
4. Polnet ve Mobese sistemleri birimler içinde aktif olarak kullanılmakta mıdır? Günümüz itibariyle Polnet kullanıcı sayısı ne kadardır?
5. Polnet ve Mobese Projelerinin oluşturulması aşamasında ülke dışı organizasyonlardan destek alınmış mıdır? Bu projelerin maliyeti hakkında bilginiz var mı?
6. Mobese sisteminin altyapı olarak Polnet bilgi ağını kullandığı bilinmektedir. Bu kapsamda altyapı olarak Ponet güvenli midir? Sistemin güvenliği nasıl sağlanmaktadır?
7. Mobese’nin Polnetten ayrılan bileşenlerinde veri güvenliği sorunu var mıdır? Varsa bu sorunlara ve çözümlere yönelik ne düşünüyorsunuz?

EK III

POLNET PROJESİ BİLEŞENLERİ

AFİS (Otomatik Parmakizi Teşhis Sistemi)	Parmak izi tespit ve teşhis işlemleri amacıyla oluşturulmuş bir sistemdir. Bu sistemle parmak izleri dijital ortamda saklandığı için bilgisayar yoluyla sorgulamalar yapılmakta ve parmak izi bulunan failer, kimliği belirsiz cesetler ve salite kimlikler teşhis ve tespit edilmektedir.	Silah Ruhnat Projesi	İl Emniyet Müdürlükleri bünyesinde faaliyet gösteren Ruhnat Tebligat Şubelerinin silah ruhsat ile ilgili işlemlerde kullanacağı bilgilerin bulunduğu bir projedir.	Gözetli İşlemleri Projesi	Gözetim alınan şahısların tüm kimlik bilgilerinin, gözetim tarih-saat- yer-şahıs bilgilerin bulunduğu yerdir.	Olay İstatistik Projesi	Bu proje polisin adli idari yönüyle tuttuğu tüm bilgileri, çok sayıda ve çeşitli kriterlere göre istatistige dönüştürmektedir.
Tahdit (Hudut Kapıları Yolcu Giriş - Çıkış) Projesi	Bu proje "Aranan Şahıslar", "Zayıf Pasaport" ve "Yolcu İşlemleri" programlarından oluşmaktadır. Ülkeye hudut kapılarında pasaport kontrol ve denetim işlemleri sırasında giriş çıkış yapan şahısların yeri ve yabancı şahısların tespit amacıyla bu şahısların bilgilerinin içerisinde bulunduğu projedir.	Araç ve Sürücü Bilgi Sistemi (ASBİS) Projesi	Araç satışı, teslim ve sürücü belgesi işlemlerinin tek merkezden elektronik ortamda yapılarak ilk müracaat yerinde sonuçlandırılmasını sağlayan projedir.	Aranan Araçlar Projesi	Bir aracı neden, hangi birim ve hangi tarihten itibaren arandığı; eğer araçla ilgili olarak çağrılı kaydı var ise çağrıma yöntemi gibi bilgilerin bulunduğu sistemdir.	Araç Kontrol ve Sürücü Sorgulama Projesi	Türkiye geneli yapılan trafik denetimlerinin Pohet ortamına veri kaydedildiği ve istatistiklerin alındığı bir projedir.
Yabancılar Projesi	EGM Yabancılar Dairesi Başkanlığı tarafından Türkiye'de bulunan tüm yabancı şahıslar ile ilgili kimlik, ikamet, vize, suç, refakatçi, pasaport, giriş kapısı ve diğer şahıs bilgilerinin bulunduğu sistemdir.	Genel Bilgi Toplama (GBT) Projesi	Yabancı şahısların ve Türk vatandaşlarının suç kayıtları, aranan/tehlükeli şahıslar ve araçlar ile ilgili bilgiler bulunmaktadır.	Kriminal Uygulamaları Projesi	AFİS Parmak İz Sistemi, Balistik, DNA Veri Bankası, Biometrik Tanıma Sistemleri, Olay Veri İncelemeleri (OYT), Bomba İhbar ve buna benzer tüm kriminal uygulamalara ilişkin veriler	Mobil Uygulamalar Projesi (MUP)	Sahadaki personelin GSM şebekelerinin çektiği her yerde, kablo gereksinimi olmadan, ellerindeki terminalleri kullanarak Pohet veri merkezine bağlanabildiği uygulamaların genel ismidir.
E-pasaport Müracaat Tanzim ve Takip Sistemi Projesi	Pasaport Kanunu kapsamında düzenlenen umuma mahsus, hususi damgalı, hizmet ve diplomatik pasaportlar ile ilgili bilgileri kapsamaktadır. MERNİS, Dışişleri Bakanlığı, PTT Genel Müdürlüğü, TÜRKİYE SİSTEMLERİ ve Pohet Elektronik Pasaport Müracaat Sistemi arasında web servisler aracılığıyla entegrasyon sağlanmıştır.	Basın Yayın Projesi	Emniyet Teşkilatı bünyesindeki tüm basılı eser, ıyık, radyo, tv, manyetik eser ve matbaa ile ilgili bilgilerin etkin biçimde bilgisayar ortamına aktarılması, ilgili verilerin istenilen kriterlere göre sorgulanabilirdiği bir projedir.	Trafik Bilgi Sistemi (TBS)	Trafik Araştırma Merkezi Müdürlüğü tarafından yürütülen, içerisinde Trafik Hizmetleri Başkanlığının Türkiye'deki trafik ve trafik güvenliği (araç, sürücü, kaza ve karayolu) ile ilgili tüm arşiv bilgileri bulunmaktadır.	Asayiş Performans İzleme ve Takip Projesi	"Güvenli Okul" ve "Yıldırım Ekipler" projeleri kapsamında okullardan sorumlu olan polis memurlarının okul giriş - çıkışları dahil olmak üzere eğitim saatinde okul ve çevresinde emniyete yönelik olarak yapılan okullardan faaliyetlerin kaydedildiği uygulamasıdır.
Sürücü Ceza Projesi	Türkiye genelinde kayıtlı yapılan sürücü ceza belgelerinin bilgileri ile sürücü kayıtları bu projede bulunmaktadır. Bunun yanı sıra özellikle Emniyet Teşkilatının planlama çalışmalarında ihtiyaç duyacağı ıık ihali, hız kontrolü, seyir halinde kontroller ile çeşitli sürücü belgelerinin cinsiyet, yaş ve illelere göre dağılımına dair istatistik bilgileri bu projeden faydalanılarak elde edilmektedir.	İnterpol 7/24 ASF Projesi	İnterpol üyesi ülkelerin ortak veri tabanı ile entegre olarak aranan ve çağrılı araç, belge ve şahıslar ile ilgili bilgileri anlık olarak ilgili birimlere bildirilen bilgi işlem projesidir.	Mahalle Polisliği Projesi	Emniyet münkasındaki yurtaşlara yönelik olarak aile hekimini uygulamasında olduğu gibi her yurtaşın sorumlu bir polis memuru görevlendirilmiştir. Bu görevlilerin bilgilerin bulunduğu projedir.	Spor Olayları Projesi	Spor müsabakalarında ceza alan ve hak mahrumiyeti bulunan şahısların, kulüplerin ve basın kuruluşlarının ceza bilgilerin bulunduğu projedir.
Kaza Projesi	Meydana gelen ölümli - yaralanmalı trafik kazalarına ait bilgilerin toplanması ve bu bilgilere göre trafik kazalarına ait istatistik sonuçların elde edilmesini sağlamaktadır. Proje, trafik birimleri tarafından kaza kayıtlı bulunan tüm kazaları kapsamaktadır.	Güvenlik Soruşturamaları Projesi	Arşiv araştırmasının Pohet ortamında GBT, Terör, Tahdit ve Aranan Şahıs, Kaçakçılık ve Arşiv Tetkik projelerini aynı anda kullanmak suretiyle yapıma imkanı sağlayan bir programdır.	Sosyal Yardım Projesi	Emniyet Teşkilat mensupları ve yakınları tarafından talep edilen yardımların kayıt ve takibi amacıyla kullanılan projedir.	Kayıp Eşya ve Belge Projesi	Bu projede, kaybedilen veya çalınan araç, plaka, pasaport ve ruhsat bilgileri tutulmaktadır.
Dijital Arşiv Projesi	Arşiv ve Dokümantasyon Daire Başkanlığı tarafından tüm arşiv bilgilerin dijital arşive dönüştürüldüğü sistemdir.	Elektronik Belge Yönetim Sistemi (EBYS) Projesi	Emniyet Teşkilatındaki tüm yazışmalar, belgelerin herhangi bir evrak olmaksızın, dijital imzalarla yapıldığı projedir.	Gelen - Giden Evrak Projesi	EGM bünyesinde merkez ve taşra teşkilatı arasındaki tüm evrak işlemleri ve kayıtların tutulması bu projeye sağlanmaktadır.	Hukuk İşleri Dava Takip Projesi	Emniyet Genel Müdürlüğü veya personel aleyhine açılan tüm dava bilgileri ile disiplin soruşturması bilgileri bu projede tutulmaktadır.

EK IV

MOBESE PROJESİ BİLEŞENLERİ

Mobese Yönetim Sistemi	Mobese sistemi bilşim yapısının izlenmesini ve yönetilmesini sağlayan donanım ve yazılımlardır.	Küresel Yer Belirleme Sistemi (GPS, Global Positioning System)	Uydular ile kriptolu sinyal gönderme ve alma özelliğine sahip konum belirlemeye yarayan bir projedir. Bu proje sayesinde ekiplerin ve ilgili personellerin konumları anlık uydü vastasıyla tespit edilebilmektedir.
Komuta Kontrol Merkezi	Dev ekranların bulunduğu ve uzman personelin çalıştığı olağan ya da olağanüstü durumlarda güvenlik hizmetlerinin yönetildiği ve yönlendirildiği Mobese'nin beyni bileşendir.	Nezarethane Kontrol ve İyileştirme Sistemi	Gözetlme alınan bütün şahıslarla ilgili işlemlerin kameralar vastasıyla kayıt altına alınması sürecini kapsayan bir sistemdir. Bu sistem sayesinde işkence girişimleri ve iddiaları, intihar olayları önlenmektedir.
Görüntüleme Sistemi	Bu sistem Mobesenin temel bileşenidir. Sistem eş zamanlı olarak elde edilen görsel bilgilerin, delil niteliğinde saklanması, izlenmesini, otomatik olarak veya izleme neticesinde elde edilen alarmlar hakkında gerekli kayıt ve işlemlerin yapılmasını sağlayan donanım ve yazılımlardan oluşmaktadır. Sistem görüntü verisini eş zamana yakın bir sürede işlemekte ve hırsızlık, yasak bölge ihlali, park yasağı ihlali, şüpheli paket, şüpheli gezinen / duran kişi, pankart açma, bayrak yakma, şüpheli aracın öngörülen zamandan fazla parkı (bomba yüklü araç şüphesi) gibi çeşitli konularda, ilgili kriterlere uyan durumu otomatik olarak algulamakta ve olay yerine en yakın ekibe haber vermektedir.	Asayiş Otomasyon Sistemi	Komuta kontrol merkezine bir ihbar geldiğinde, sayısal harita üzerinden olay veri tespit edilir ve ihbarı veren kişinin kimlik bilgileri sisteme teyit edilir. Olay sisteme girilince otomatik olarak olay yerine en yakın ekip mobil araç ünitesi vastasıyla uyarılır, ayrıca sistem olayla ilgili bütün tutanakları otomatik olarak hazırlar. Bütün bu süreç asayiş otomasyon sistemi üzerinden yürümeaktadır.
Mobil Uygulamalar Sistemi	Bu sistem kullanıcıların akıllı telefonlarından veya dizüstü bilgisayarlarından araştırdıkları olay, şahıs veya araçlara ilişkin olarak hızlı bir şekilde rapor almalarını sağlayan, coğrafi bilgi sistemi ile de desteklenmiş yazılım ve donanımdan oluşan kriptolu bir sistemdir.	Karınca Evrak Transfer Sistemi	Mobesenin olduğu şehirlerde bütün idari hizmet yürüten birimlerde bütün evrak sirkülasyonu, arşivlenmesi dijital ortamda gerçekleştirilmektedir. Bu sistem sayesinde kırtasiyeciliğin büyük oranda azaldığı ifade edilmektedir.
Coğrafi Bilgi Sistemleri (CBS)	Diğer projelerin de altyapısını oluşturacak şekilde sayısal harita üzerinde GPS ve diğer göstergelere göre konumlama yapılma, bu haritalar üzerinde verilerin toplanması, analiz edilmesi ve profil çıkarılması imkânını da sunan bir çok alt sistemlerden oluşan bir projedir.	Çağrı Yönetim Sistemi	Coğrafi bilgi sistemleri ile entegre bir şekilde olay ile ilgili haber alır almaz, sayısal harita üzerinde olay yerine en yakın ekibi tespit ederek, bu sistem dahilinde ilgili ekiplerin olay mahalline yönlendirilmesini sağlayan sistemdir.