TÜRKİYE'DE
DİJİTAL GÖZETİM

T.C. Kimlik Numarasından E-Kimlik Kartlarına Yurttaşın Sayısal Bedenlenişi

Selma Arslantaş-Toktaş
Mutlu Binark
Ergin Şafak Dikmen
Işık Barış Fidaner
Elif Küzeci
Alkım Özaygen

TÜRKİYE'DE DİJİTAL GÖZETİM

T.C. KİMLİK NUMARASINDAN E-KİMLİK KARTLARINA YURTTAŞIN SAYISAL BEDENLENİŞİ

Yazarlar*

Selma Arslantaş-Toktaş, Ankara Üniversitesi İletişim Fakültesi
Mutlu Binark, Başkent Üniversitesi İletişim Fakültesi
Ergin Şafak Dikmen, Ankara Üniversitesi İletişim Fakültesi
Işık Barış Fidaner, Boğaziçi Üniversitesi Mühendislik Fakültesi
Elif Küzeci, Bahçeşehir Üniversitesi Hukuk Fakültesi
Alkım Özaygen, Ankara Üniversitesi Siyasal Bilgiler Fakültesi

Yayınevi: Alternatif Bilişim Derneği

*Yazarların kitaba katkısı eşit değerdedir, yazarlar soyadı sırasına göre alfabetik olarak dizilmiştir.

TÜRKİYE'DE DİJİTAL GÖZETİM T.C. KİMLİK NUMARASINDAN E-KİMLİK KARTLARINA YURTTAŞIN SAYISAL BEDENLENİŞİ

Selma Arslantaş-Toktaş
Mutlu Binark
Ergin Şafak Dikmen
Işık Barış Fidaner
Elif Küzeci
Alkım Özaygen

Yayına Hazırlayan: Mutlu Binark
Kapak Tasarımı: Ergin Şafak Dikmen
Sayfa Tasarımı: Alkım Özaygen

Yazıların hakları yazarlara aittir.
Kitabın LaTeX kodları CC Attribution-
NonCommercial 3.0 Unported License altındadır.

Yayınevi: Alternatif Bilişim Derneği
Yayın Yılı: 2012
Yayın yeri:İstanbul

Ceylan Matbaa
Güven İş Mrk. B Blok No 317 Topkapı Zeytinburnu
0 212 613 10 79

ALTERNATİF BİLİŞİM DERNEĞİ
ve
Friedrich-Ebert-Stiftung Derneği Türkiye Temsilciliği - İstanbul

ISBN:978-605-62169-2-3

"Biz, milyonlarca biz, her sabah, altı-teker şaşmazlığıyla aynı saatte ve aynı dakikada, yekvücut uyanırız. Milyonlarca biz, aynı saatte çalışmaya başlarız. Daha sonra, milyonlarca biz, yekvücut, dururuz. Ardından milyonlarca ele sahip tek bir beden gibi, Çizelge'nin gösterdiği anda kaşıklarımızı ağızlarımıza götürürüz. Ve hepimiz aynı anda kalkar, dinleme salonuna, oradan Taylor egzersizleri için ana salona ve sonunda uyumaya gideriz. Size tümüyle dürüst davranacağım: Biz bile mutluluk sorununu henüz yüzde yüz kesinlikle çözemedik."

(TekDevlet matematikçilerinden D-503)*

Yevgeni Zamyatin (1920; 2010: 13)

*Yevgeni Zamyatin (2010) Biz, Çev. Algan Sezgintüredi, İstanbul: Versus Yayınları.

İçindekiler

Sunu 1

Sunuş 5

Önsöz 7

I. Bölüm:
DİJİTAL GÖZETİM OLGUSUNA
KURAMSAL ve KAVRAMSAL BAKIŞ **12**

1.1. Neoliberal Toplumun İktidar Modeli: Yönetişim ve E-devlet 17

1.2. Güvenlik Adına Risk Yönetiminin Uygulanması 20

1.3. Devletin Yurttaşını Gözetlemesi Olgusunun Nedenleri 22

1.4. Modern Dönemin Panoptik Stratejileri 25

1.5. Kusursuz Bir İktidar İçin Sürekli Denetim: Biyo-Politika . . 27

1.6. Gözetim ve Denetimin Her Yerdeliğinin Normalleşmesi ve İçselleştirilmesi 30

1.7. Panoptikondan Süper Panoptikona 33

Sonuç olarak 36

II. Bölüm:
DİJİTAL GÖZETİM TEKNOLOJİLERİ VE UYGULAMALARI **39**

2.1. Askeri ve İstihbarat Alanları 43

2.2. Devlet Yönetimi, Nüfus Sayımı ve Suç Kontrolü Alanları . . 48

2.3. İş Yeri Gözetimi ve Denetimi Alanları 52

2.4. Tüketim ve Tüketici Yapılandırması Alanı 56

III. Bölüm:
TÜRKİYE'DE YURTTAŞLARIN SAYISAL KAYITLANMASI VE GÖZETLENMESİ:
ŞECERE KAYITLARINDAN SAYISAL BEDENLENİŞE **63**

3.1. Türkiye'de Yurttaşın Sayısal Kayıtlanmasının Kısa Tarihçesi 67

3.2. Araştırmanın Yöntemi: E-devlet Kapısı Üzerinde Yurttaşın Sayısal Bedenlenişinin Topografyasını Çıkartmak 75

3.3. Türkiye'de Yurttaşın Sayısal Bedenlenişinin Topografyası . . 76

IV. Bölüm:
TC KİMLİK NUMARASI: HUKUKSAL BİR DEĞERLENDİRME **89**

4.1. Giriş 93

4.2. Modern Devletin "Veri Açlığı" ve Hızla Şeffaflaşan Bireyin Hukuksal Kalkanı 93

4.3. Elektronik Devlet, Sayısallaştırılmış Yurttaş 98

4.4. "Ben" ya da On Bir Hanelik Kimlik Numaram... 101

4.5. Dijital Çağda Bireysel Özerklik Nasıl Sürdürülebilir? 110

V. Bölüm:
GENEL DEĞERLENDİRME **112**

Ek-1 **119**

Ek-2 **136**

Ek-3 **140**

Ek-4 **146**

Kaynakça **148**

Özet **163**

Abstract **167**

Özgeçmişler **171**

Sunu

Friedrich-Ebert-Stiftung Derneği (FES) Alman Politik Dernekleri arasında en eski kurumdur ve 1925 yılında Almanya'nın ilk Cumhurbaşkanı Friedrich Ebert'in vasiyeti üzerine kurulmuştur. FES, dünya çapında 100'ün üzerinde ülkede demokrasiyi, barışı ve sosyal adaleti destekleme amaçlı çalışmalarda bulunur. Türkiye'de ise FES, Demokrasi ve İnsan Hakları, Ekonomik ve Sosyal Kalkınma ve Dış İlişkiler olmak üzere üç ana dalda 25 yıldır aktif olarak çalışmalarını sürdürmektedir.

Kişisel verilerin korunması konusu insan hakları alanın tartışmasız bir parçasıdır ve kamusal hayatın dijitalleşmesi sürecinde daha büyük bir önem kazanmıştır. Dolayısıyla internetin, bilgi paylaşım ve iletişim teknolojileri ile ilgili olumlu gelişmelerin yanında, bu gelişmelerin birey haklarına yönelik oluşturabileceği muhtemel tehditlerin de ciddiyetle ele alınması gerekmektedir. Bireysel verilerin dijital ortamda toplanarak vatandaşların özel yaşamlarına dair hiç bir bilginin saklanamaz hale getirilmesi ve bütün kişisel bilgilerin şeffaflaşması gerçek bir risktir ve bu riski önlemeye yönelik kişisel bilgilerin korunmasına dair etkili yasaların çıkarılması kesinlikle gereklidir.

Dünyada kişisel verilerin korunması ile ilgili ilk kanun Almanya'da 1970 yılında onaylanmıştır. Bu çabanın arkasındaki kaygı, devletin bütün kişisel verileri toplayarak farklı amaçlar için kullanabiliyor olabileceğidir. Erken ortaya çıkmış bu kaygıyı giderme amaçlı zamanla ek yasalar ve Almanya Anayasa Mahkemesi'nin yargı kararları aracılığı ile kanunu güçlendirici adımlar atılmıştır. Bu gelişmeler, kişinin kişisel bilgilerinin erişiminde kendisinin belirleme hakkı olduğunu ifade eden Bilgiye Erişimin Bireysel Belirlenmesi ilkesini temel bir hak kategorisi olarak ortaya çıkarmıştır.

Bu hak talebi zamanla ilkenin ruhunda bir değişiklik olmaksızın yasal metinler üzerinde güncellenerek bu güne getirilmiştir. Halen, gelişen teknolojiler ve terörizmin yeni boyutlarının ortaya çıkardığı yeni tehditler devletin vatandaşları hakkında daha çok bilgi toplamak amaçlı öne sürdüğü gerekçeler olmaya devam etmektedir.

Temel haklar ve vatandaşlık haklarının korunması hiç bir şekilde sadece devlete bırakılacak bir sorumluluk olmamalıdır. Esas olan, bu sürece vatandaşların katılımının sağlanmasıdır.

Bu çalışma sadece Türkiye'de süregelen kişisel verilerin korunması tartışmasını içermekle kalmamakta, aynı zamanda MERNIS ve yeni e-kimlik kartı uygulamalarında oluşabilecek tehlikeleri göz önüne sermekte ve kişisel verilerin korunması ile ilgili etkin yasaların hayata geçirilebilmesi için yasa koyuycuya somut öneriler

geliştirmektedir.

Friedrich-Ebert-Stiftung Derneği bu yayın çalışmasını Türkiye'deki temel vatandaşlık haklarının güçlenmesinde önemli bir adım olarak görmekte ve desteklemektedir.

Friedrich-Ebert-Stiftung Derneği Türkiye Temsilciliği
İstanbul, Mayıs 2012

Sunuş

Gündelik yaşamda bilgi ve enformasyonun işlendiği süreçler hızla sayısallaşmakta. Bu süreçlerdeki öznelerin, nesnelerin, olguların, olayların sayısal karşılıkları/kodları var artık. Bu sayısal kodlar her geçen saniye artıyor, birbirleri ile ilişkileniyor, anlamlar kazanıyor ve topluma daha büyük sayısal kodlar üretmek için geri dönüyor.

Bu sayısal varoluş, daha kolay iletmeye, üretmeye, gereksindiğimiz gibi değiştirmeye, paylaşmaya olanak sağlıyor. Fakat aynı kolaylık, bu sayısal varoluşları kayıt altına almak, tasnif etmek, ayrıştırmak, işaretlemek, tanımlamak, etiketlemek, takip etmek ve gözetlemek için de geçerli. Maalesef dün romanlarda, kurmacalarda gördüğümüz denetim/gözetim toplumuna daha yakınız. Üstelik hemen herkes isteyerek ya da istemeyerek, bilinçli ya da bilinçsiz bu süreci hızlandırıyor.

Neyseki, ne yaşadığımızı anlama ve bize anlatma çabası içerisinde olan değerli bilim insaları var. Bu kitap, böyle bir çabanını ürünü. Ankara Üniversitesi Sosyal Bilimler Enstitüsü'nde 2011 Bahar Dönemi'nde Yeni Medya Sosyolojisi adlı doktora dersinde bir grup akademisyen, Türkiye'de dijital gözetim konusuna çalıştı. Kolektif bir çabanın sonucunda da elinizdeki değerli metinleri üretti.

Gözetim toplumu ve birbirlerini ivmelendiren tüketim toplumu yaratımlarına karşı üreterek yanıt veren bu güzel çalışmayı Alternatif Bilişim Derneği olarak sizlerle paylaşmaktan çok mutluyuz.

Metni üreten, doktora dersinin öğrencileri Alkım Özaygen, Selma Arslantaş ve Şafak Dikmen'e, dersin değerli hocası Mutlu Binark'a, dersi gönüllü olarak takip edip tüm çalışmalara katkıda bulunan Gülden Gürsoy Ataman'a, kitabın tamamlayıcı hukuk bölümünün yazarı Elif Küzeci'ye, kitabın baskısı için katkıda bulunan ve ücretsiz dağıtabilememizi sağlayan Friedrich Ebert Stiftung Vakfı'na, kapak tasarımı için Şafak Dikmen'e, sayfa düzenlemesi ve LaTeX yerleştirmelerini yapan Alkım Özaygen'e, nefis önsöz için Işık Barış Fidaner'e, dernek üyelerimize ve görünen görünmeyen emekleri için herkese teşekkürler.

Sayısal kolaylıkların sadece özgürlüklerimizi genişlettiği, böylece mutlu ve üretken olmaya daha çok zaman kaldığı bir dünya için çabalayanların emeklerinin yanında yer alması ve katkıda bulunması dileğiyle.

Ali Rıza Keleş
Alternatif Bilişim Derneği A.

Önsöz

İşaret edilmekten kaygı duyarız. Ama bizi esas kaygılandıran, muhatap alınmadan işaret edilmektir. Yani yanıt veremediğimiz cümlelerin içinde geçmektir. Bizden bahseden bu kaygılandırıcı cümle, resmi bir açıklamada, gizli bir raporda, komşular arasındaki bir muhabbette veya sevdiğimiz bir insanın aklından geçiyor olabilir. Yasal süreçler, veya mesela bankaların veritabanlarında işleyen otomatik süreçler de böyle kaygı verici cümleler kurabilir. Reddedilmek, hep böyle bir cümleyi düşündürür: "X güvenilir birine benzemiyor"

Bu cümle, doğal görüntüyü bozan tek bir işaret, bir leke, tek bir "X" olabilir. Adıyaman, İzmir, Antep ve Malatya'da yaşayan Alevi ailelerin evlerinin işaretlenmesi, Erzincan'daki tehditkar duvar yazıları, bahsettiğimiz kaygıyı örnekleyen süreçlerden yalnızca biri.

Buna karşılık, işaretlemekten haz duyarız. Muhatap almadığımız birini elimizdeki hazır bir çerçevenin içine almak özellikle haz verir... Bu kınayıcı bir tavır olabilir, bir dedikodu veya bir espri olabilir, bir reklam tasarımı, bir televizyon programı olabilir... Suç oranlarını sayıp döken bir rapor veya veri toplayan bir yazılım da böyle bir çerçeve oluşturabilir.

Hem işaret edilme, hem işaret etmede esas belirleyici olan, iletişimin yapıldığı alandır. Aynı söz, yerine göre bir tehdit, bir eleştiri veya öneri anlamına gelebilir. Her alan, konuşmayı belirli çerçevelerle biçimlendirir ve kısıtlar. Öğrenciler hocaları bol bol çekiştirirken başka şeyleri konuşamayabilir. Öğretmenler odasında öğrenciler hakkında konuşulurken başka şeyler konuşulamayabilir. Meclisteki vekiller yasa teklifi hakkında konuşurken başka şeyleri konuşamayabilir...

İletişim alanlarının ayrıklığı, çerçevelerin de ayrık olmasını getirir. Kesişimlerini kaybederek ayrıklaşan, kopan çerçeveler birbirlerini ancak birer "yabancılık" olarak işaret edebilir. Bu durum, sebepsiz, açıklaması olmayan düşmanlıkların kaynağıdır. Hukukun esas işlevi, ayrıklaşmış çerçeveleri uzlaştırarak düşmanlıkları ortadan kaldırmak olarak özetlenebilir.

İnsanlar ortak alanlarda biraraya gelip konuştukça karşılıklı uzlaşmanın doğallıkla gerçekleşmesi beklenebilir. Fakat kamu işlevlerinin giderek özel alanlarca üstlenilmesi, kamu kuruluşlarının giderek kamusal özelliğini yitirerek özel alanlara dönüşmesi gibi süreçler sonucunda oluşan statüler ve yetki alanları, iletişim olanaklarını kısıtlayarak, belirli işaretleyici çerçevelerin ve belirli düşmanlık biçimlerinin koruma altına alınması sonucunu doğurur. Bu korumanın adı devlettir.

Kamusal-özel dengesinin tersyüz olması üç aşamadan geçer: Önce kamusal alan uzlaştırıcı işlevini kaybeder ve özel alanlar birbirlerine karşı genel bir kayıtsızlık

içine girerler. Zamanla bu kayıtsızlığın yerini karşılıklı yabancılığın sebepsizce birikmesiyle gelişen gizli bir düşmanlık tutumu alır. Düşmanlık çözülmeden taraflar iletişime zorlandığında ise ikiyüzlülük gerçekleşir: düşmanlığın ikinci yüzü "rekabet" adıyla iletişim çerçevesine girer ve böylece düşmanlaşma süreklilik kazanır. Bu durum, kamusal uzlaştırıcı işlevin aksatılması, durdurulması ve askıya alınmasının günümüz dünyasının bütün toplumsal alanlarında gözlemlediğimiz somut bir sonucudur.

***

Bu kitap, devlet ve şirketlerin yurttaş ve tüketicileri işaret etmek için yaptıkları çalışmaları anlatıyor. Burada "devlet" derken, birçok kademede bulunan yetkililerin, memurların, çalışanların, hatta hassas vatandaşların tümünü kastetmiş oluyoruz. Bu özneler devlet adına "yurttaş"ı işaret ediyorlar. Böylece, (zaman zaman "derin devlet" de dediğimiz) özne-devleti oluşturuyorlar.

İşaretlenme karşısında gelişmiş bir kaygı, devlet dediğimiz yetki alanlarının koruması altına alındıktan itibaren işaretleyici bir çerçevenin hazzına, dolayısıyla sebepsiz ve çözümsüz bir düşmanlık haline dönüşür. Böylece geçmişin kaygılı yurttaşları bugünün özne-devletini oluşturabilir. Resmi devlet siyasetinin dönem dönem kendini yenileyerek sürmesini sağlayan şey bu işte çevrim sürecidir. Kemalizm, başörtüsü meselesi, Kürt meselesi gibi ana siyasi meseleler, belirli düşmanlık biçimlerinin devlet korumasına alınması şeklinde okunabilir.

O zaman "yurttaş", kararsız bir kavramdır. Bugün için "yurttaş" devletten duyulan kaygıyı temsil ediyor. Acaba yarın bunu devlet adına bir hazza mı çevirecek, işaretlenmekten kurtulabilecek mi, veya açıklamamızın kapsayamadığı farklı bir yol mu tutturacak?

"Yurttaş"taki kararsızlığın bir diğer adı özgürlüktür. Siyaset/politika da diyebiliriz buna. İşaret edilmenin kaygısı aynı zamanda özgürlüğün çıkış noktasını oluşturuyor. İsmiyle çağrılan bir bebeğin daha sonra konuşmayı öğrenmesi gibi, bu kaygı altında hiç bilmediğimiz dilleri ve söylemleri öğrenebiliriz, bunlara uyum sağlayabiliriz, veya henüz varolmayan yeni diller, söylemler, felsefeler oluşturabiliriz. Kaygının içinden özgürlüğü bulup çıkartabiliriz.

Yeni bir dile ulaşmanın ilk adımı, mevcut dil ve söylemleri değiştirebilmektir. Fakat bu, sözcükleri ve ifadeleri bir doğruculuk eleğinden geçirmek anlamına gelmiyor. Aksine, bir dilden çıkacaksak, bizi gösteren işareti de o dilin içinden söküp almalıyız. Mevcut durumda korunmakta olan çerçeveyi doğrulamanın hazzına kapılmamalı, çerçeveye karşı, çerçeveye rağmen işaret edebilmeliyiz.

Bir sözcüğün anlamını öğrenmek nasıl cümle içinde kullanarak oluyorsa, yanlış bir anlamı düzeltmek de yeni cümleler kurmakla olur. Doğrusunu daha bilmezken, hatta doğrusu henüz ortada yokken, "bu yanlıştır" diyebiliriz. "Doğrusu", yani yeni bir dil, yeni bir söylem, yeni bir çerçeve, ancak bu şekilde ele geçirdiğimiz işaretlerle kurulabilir. Bir çocuk nasıl önce inatla tek tek oyuncakları ele geçirip sonra bunlardan yeni bir oyun kuruyorsa, biz de tek tek sözcükleri ele geçirip cümle cümle yeni bir söylem, yeni bir düşünce kurabiliriz. Böylece kendi anlayacağımız anlamda bir "yurttaş" olmamız mümkün olur.

Yurttaş olmak günümüzde işaret edilmek kadar ölçülmeyi de ifade ediyor. Her işaret etmenin altında yatan bir ölçme-tartma çabası var, simgelerle ölçüleri birleştiren matematikte olduğu gibi. Ticari, bilimsel, çok çeşitli amaçlarla çeşit çeşit cetveller icat ve imal edilmiş fakat bütün bunların altında, kafamızdaki cetvel yatıyor. Bu cetvel esasında kendi eylemlerimizi ölçüp tartmak için var. Ne var ki, biz çoğunlukla bu cetveli başkalarını, yani işaretlediklerimizi ölçüp tartmakta kullanıyoruz.

İşaretlenme kaygısı, aynı zamanda ölçülüp-tartılma kaygısıdır. Gençlerin büyükler karşısında, yeni gelenin eskiler karşısında, yeni gelinin kayınvalide karşısındaki kaygısı dersek neyden bahsettiğimiz anlaşılır. Tabi ki bunun karşısına bir ölçme-tartma hazzını, ve bunu "devlet" adına, "aile" adına veya "mahalle", "millet" adına, "halk" adına, "şirket" adına yapmanın hazzını da eklemeliyiz.

Bir yurttaş olarak aynı anda çok çeşitli veri havuzlarında bulunuyoruz. Doğduğumuz andan ölümümüze kadar birçok ölçüye vuruluyoruz. Oynadığımız oyunlardan ailemizin "bu çocuk galiba X olacak" demesine, seçtiğimiz arkadaşlardan aldığımız derslere, yaptığımız alışverişlerden girdiğimiz işlere, hobilerimize ve ciddiye aldığımız meselelere kadar her alanda sergilediğimiz görünüşler, ölçülmek üzere işaretleniyor ve çeşitli veri havuzlarında biriktiriliyor. Buna karşılık biz de, ergenlikten iş hayatına ve siyasi toplantılara kadar, girdiğimiz her sosyal alanda yapılan haz verici "gözlemleme ve ölçüm-tartım" çalışmalarına katılıyoruz, ve bu çalışmalara tahammül edemediğimiz noktalarda bu alanlardan ayrılmak durumunda kalıyoruz.

Sonuç olarak işaret etme-edilmeye her zaman eşlik eden ölçme-ölçülme eylemleri, toplumdaki tüm alanları saran bir denetim ağı meydana getiriyor. Gördüğü birine bugün "şuna bak X yapmış!" demenin hazzına kapılan bir kişi, ertesi gün "X" yapmadan önce ikinci kere düşünmek zorunda kalır. Bu şekilde birbirimizi ve kendimizi sürekli denetim altında tutarız. Konuşup işaret ederek kafamızdaki cetvelleri birbirine uydurmamız, aynı zamanda toplum genelindeki davranışlarımızda genel bir uyumluluk kurulmasını, dolayısıyla "devlet" açısından bir denetim kolaylığı sağlar. Aslında "devlet" dediğimiz şey, yani nesne-devlet, kafalarımızdaki bu cetvellerin toplamından ibarettir. Bu cetvellerin diğer bir adı, çözülmemiş düşmanlığımızın ikinci yüzü olan "rekabet"tir. Bu ikinci yüz şu adlarla da anılıyor: "fırsat", "avantaj", "pozisyon", "fayda", "iyilik"...

Peki bu ölçü ve cetveller, söylem ve işaret etmenin neresinde durmaktadır? İşaret edilmek ve ölçülmenin kaygısından, "söylem adına" işaret etme ve ölçmenin hazzından bahsettik. Peki "söyleme karşı" işaret ederken, simgeyi dilden söküp alırken, kaygıdan haz yerine özgürlük bulup çıkarırken bu kafamızdaki cetvellerden nasıl kurtulacağız?

Bu cetveli var eden şey, işaret edilmekten muaf olmasıdır. "Normallik, sıradanlık, doğallık" gibi adlar altındaki görüntülerin karmaşasına saklanması ve dilin okundan kaçabilmesidir. O zaman özgürleşmenin ilk şartı, kişileri ve olayları bırakıp kafadaki cetveli işaret etmektir. "Söyleme karşı" kurulmuş cümle de zaten bu cetveli işaret eden cümledir. Simgeleri mevcut dilden söküp almak, öncelikle mevcut ölçü ve tartıların "normal-sıradan-doğal" akışından çıkmak ve cetveli

işaret etmekle mümkün. Ama bu iş kolay değildir. Çünkü cetvel acıtır.

Örnek verelim: Binlerce Kürt yurttaş ve siyasetçi yıllarca haksız yere cezaevinde tutuldu, fakat ne zaman ki bir yazar, bir yayıncı, bir hoca, bir öğrenci cezaevine atıldı, ancak o zaman bu konu konuşulmaya başlandı... Yaklaşık dört ay önce, 28 Aralık 2011 akşamı Roboskî-Uludere'de onlarca çocuk-genç Türk Silahlı Kuvvetleri tarafından öldürüldü, fakat hükümet yetkilileri Suriye'ye insanlık dersi verme çabasında. Acaba bu konunun konuşulması için daha kimlerin öldürülmesi gerekiyor? Kafamızdaki cetvel kimleri insandan sayıyor, kimleri saymıyor?

Doğruyu kurmak için önce "yanlış"ı işaret etmek gerekir. En büyük yanlış ise bugün doğruyu ölçen cetvellerin kendisidir. Bu cetveller, aslında içinden konuştuğumuz mevcut söylemlerden çok daha temel bir yerdedir. Çünkü zaman içinde egemen söylemler değişebilir, fakat zemin aldıkları cetveller büyük ölçüde aynı kalır.

Egemen söylemi kabul edemeyiz, ama onunla bağlarını koparmış bir karşı söylemle de yetinemeyiz. Farklı kılıklarla sürüp giren söylemlerin akışına yön veren, bu dönüşümün yatağını oluşturan cetvelleri bulup çıkarmak, onlara işaret etmek zorundayız. Düşmanlıklardan kurtulmak istiyorsak, önce rekabetten bütünüyle sıyrılabilmeliyiz.

Doğru alanlar ve yanlış alanlar yoktur. Beraberce yönlendirdiğimiz (veya yönlendiremediğimiz) bir akış (veya akamayış) vardır.

Heraklit'e atfedilen sözün devamını getirirsek:

Aynı nehirde yıkanamayız... Ama başka nehirde de yıkanamayız...[1]

***

Kitabın birinci bölümü, dijital gözetim olgusunun ele alınabilmesi için kavramsal bir çerçeve sunuyor. Günümüzün yeniden yapılandırmacı muhafazakarlık biçimi olan neoliberal söylemin şeffaflık, yönetişim, demokrasi gibi kavramlarının ideolojik olarak nasıl kavranabileceğini detay ve örneklerle açıklıyor. Dünya Bankası'nın dilinde "dürüstlük, adalet, serbestlik, bağımsız yargı, insan haklarına saygı, verimli ve yolsuzluktan arınmış bürokrasi" şeklinde ifade bulan bu söylemin gerçekte nasıl ölçülere dayandığını ve bu şekilde gözetim ve denetimin her alanda içselleştirilmesine eşlik ettiğini gösteriyor. Bu durumun en belirgin ifadesi olan, Panoptikon'un günümüzdeki "ileri" biçimi olan Süperpanoptikon anlatılıyor.

İkinci bölüm, dijital gözetim amacıyla kullanılan teknolojileri ele alıyor. Bunların başında İnternet iletişiminin takip altına alınması anlamına gelen DPI (Deep packet inspection - Derin paket sorgulama) geliyor. Bunun dışında birçok olgu anlatılıyor: ABD'nin İnternet iletişimini kayıtlaması, Türkiye'de BTK'nın "Güvenli İnternet" filtre sistemi, ister "demokratik" ister "komünist" olsun büyük devletlerin güvenlik kameraları ile tüm alanlarda kurdukları denetim, Türkiye'de son yıllarda oluşan yargı rejiminin "delil" ve "suçlu" bulma çalışmaları, genetik

[1] Bu öykünün geri kalanını Konstantinos Kavafis, Cevat Çapan, Hümeyra ve Ezginin Günlüğü anlatıyor: "Yeni bir ülke bulamazsın, başka bir deniz bulamazsın..."

bilgilerimizin bile bir denetim nesnesi olabileceği gerçeği olarak biyopolitika, işyerleri ve çalışma alanlarında yetkililerin hiç konuşmadan, gizlice sürdürdükleri takipleme ve ölçme-tartma çalışmaları, hepimizin kullandığı Google gibi araçların bizi izleyip kişiliğimizi ölçerek yanıt döndürmesi, bu şirketlerde kayıtlanan kişisel bilgilerin kötüye kullanılması tehlikesi...

Üçüncü bölüm, tekrar Türkiye'ye dönüyor ve Osmanlı'dan günümüze "nüfus idaresi" ile başlayıp "MERNİS" projesi olarak devam eden yurttaşların kayıtlanması sürecini anlatıyor. 19. yüzyılda başlayan bu maceranın son halkası, 1980'de ODTÜ'ye ihale edilmiş ve henüz tamamlanmamış olan MERNİS, yani merkezi nüfus idaresi sistemi. Pilot uygulaması Bolu'da gerçekleşen biyometrik (parmak izi ile çalışan) kimlik kartlarının tamamlanıp tüm TC yurttaşlarına dağıtılması ile bu proje tamamlanmış olacak. MERNİS projesi şahsında, Türkiye'nin 1980'den bugüne çalkantılı tarihinden, değişen söylemlerden neredeyse hiç etkilenmemiş, hepsine ayrı ayrı zemin teşkil etmiş bir yurttaşlık cetveliyle karşılaşıyoruz.

Dördüncü bölümde, modern devletin yurttaşlara ait kişisel verileri sınırsızca ele geçirip denetlemek konusundaki bitmez tükenmez hevesinin hukuki sonuçları anlatılıyor. Dünya savaşı ve faşizm deneyimini taşıyan Avrupa ülkelerinde kişisel veriler hukuki bir mesele olarak ele alınıp tartışılmış ve sonuçlara bağlanabilmişken, Türkiye'de bu meselenin ciddiyeti bir yana, varlığı bile pek bilinmiyor. Bu durum, kişisel verilerin korunması için çerçeve kanunun yıllarca yasalaşamaması, 2010 referandumunda anayasaya giren ilgili maddenin uygulamada görmezden gelinmesi gibi sonuçlar doğuruyor ve kişisel verilerin korunması ve savunulması işini içinden çıkılmaz bir labirente çeviriyor. Oysa hukuken yapılması gerekenler, bu bölümde ortaya konduğu gibi, bellidir.

Beşinci ve son bölümde ise toparlanmış olan bilgilere dayanarak özellikle Türkiye'ye dair çıkarımlar yapılıyor. Türkiyeli yurttaşların kişisel verilerinin hukuki ve somut olarak korumaya alınması, dijital gözetimle ilgili Türkiye özelindeki çalışmaların çoğaltılması ve yaygın bilinç yaratılması, bu farkındalığın sivil toplum örgütleri aracılığıyla toplum geneline iletilmesi ve nihayetinde "yurttaş" kavramının mevcut devletçi ödev bağlamından çıkarılarak temel hak ve özgürlükler bağlamında yeniden kurulması gerekliliği, bu çalışmanın düşünsel sonuçları olarak vurgulanıyor.

***

Bütün okuyucularımızı okumakla kalmayıp yazmaya, var etmeye, katılmaya ve yaşatmaya çağırıyoruz. Rekor kırmak için değil, rekorların anlamsızlığını göstermek için yapalım. Hiçbir cetvelin ölçemeyeceği değerler yaratalım. Ne ölçelim, ne de ölçülmekten korkalım. Beraberce yeniyi üretelim. İnsanın ölçüye vurulamayacağının delili olalım.

Işık Barış Fidaner

I. Bölüm:

DİJİTAL GÖZETİM OLGUSUNA KURAMSAL ve KAVRAMSAL BAKIŞ

Çalışanlarını denetleyen ve gözetleyen işveren, müşterilerini izlemek için her tarafa kamera yerleştiren mağaza sahibi ve hatta çocuklarını gözetim altında tutan anne ve baba... Bu kişileri ortak noktada birleştiren bir payda bulunmaktadır. Neredeyse hepsi bu eylemlerinin arkasında yatan nedeni "diğerlerini" gözetlemek ya da bir başkasının özel yaşamına izinsiz girmek olarak değil, yaşamın doğal akışını dengede ve güvende tutmak ve olası risklere karşı önlem almak, sevdiklerini korumak ve kollamak olarak açıklamaktadır. Bunun gibi birçok farklı şekillerde karşımıza çıkan gözetim olgusu gündelik yaşamın içerisine o kadar dahil olmuştur ki, toplumsal yaşamın her aşamasının sistematik olarak kayıt altına alınması doğal bir süreç olarak algılanmaya başlamıştır. Bu süreç öylesine doğal bir hal almıştır ki, devlet yurttaşlarını kayıt altına almak için özel bir çaba sarfetmek zorunda kalmamakta, yurttaşlar tüm verilerin birbirine eklemlendiği sisteme dahil olmak için kayıt altına alınmayı bizzatihi talep etmektedir. Modernitenin toplum yaşamı ve birey üzerindeki etkisini inceleyen İngiliz sosyal bilimci Anthony Giddens, gözetim ve gözetlemenin iki farklı anlamı olduğunu söylemektedir: Bunlardan ilki, şifrelenmiş bilgi birikimidir. Aslında Giddens, burada kişilerin nesneler haline getirilerek kodlanmasından bahsetmektedir. Toplanan bilgiler, basit bir bilgi toplama işleminin ötesindedir; depolanan bilgi, belli bir sınıflama ve ayırt etme işlemi de içerdiği için nitelikli bir bilgi depolama işlemidir (2008: 24). Gözetlemenin ikinci anlamı ise, otorite kuran kişilerin diğerlerinin hareketlerini takip etmesidir. Modern toplumlarda, kişilerin hareketleri sınırları daha belirgin alanlar (fabrika, büro, hapishane, akıl hastaneleri) içinde gerçekleşmektedir. Böylelikle, toplumsal yaşama egemen gruplar diğerlerinin hareketlerini daha etkin bir şekilde izleme ve denetleme kapasitesine sahip olmuşlardır. Gözetleme olgusunu, Giddens'ın vurguladığı anlamlar ekseninde düşündüğümüzde, gözetimin modern toplumlarda modern olmayan toplumlara göre daha yaygın ve etkili bir biçimde uygulandığı ortaya çıkmaktadır. Kısacası, gözetleme "yönetim iktidarı" olarak modern devlette daha fazla önem kazanmıştır ve devletin "idari kapsamını" yönetmesine denk düşmektedir (Giddens, 2008: 71).

Özellikle son yıllarda yaşanan terör eylemlerinin ardından devletler gerek ulusal gerekse de uluslararası düzlemde gözetim araçlarını terör ve güvenlik söylemleri üzerinden meşrulaştırarak devreye sokmuşlardır. Bu durumun en temel örneği 11 Eylül 2001'de[2] yaşanan terör eylemidir. Bu olayın ardından daha çok toplumun güvenliği ön plana çıkartılarak gözetime ilişkin gereklilik daha da derinleştirilmiş, güvenliklileştirme (*securitization*) söylemi meşru kılınmıştır[3]. Güvenliğinden emin

[2]Albrecht Dürer'in *Mahşerin Dört Atlısı* (1498) adlı eserinde "dört atlı"nın yarattığı terör tasvir edilmektedir. Bülent Diken, *Nihilizm* adlı kitabında Dürer'in çalışmasına referansta bulunarak 11 Eylül ile birlikte dört atlıların artık "mahşerin simgesel atlıları değil, Irak'taki ABD ordusu" olduğunu söylemektedir. "Fatih artık yayını germez, demokrasi getirir; savaş, barış kılığına bürünür, kıtlık, insani yardım ve "sonsuz adalet" ambalajına sarınır ve ölüm biyo-politikadır" . Bakınız: Bülent Diken, (2011). *Nihilizm*, İstanbul: Ayrıntı Yayınları, syf. 110.

[3]Ekim 2011'de ABD Kongresi, "Patriotic Act" (Vatanseverlik Yasası) kısa adıyla yaygın olarak bilinen, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" adlı yasayı kabul etti: Bu yasanın kapsamı oldukça

olmak isteyen toplumlarda özgürlükten vazgeçmek, yaşanan terör olayları ile iyice kolaylaşmıştır. Enformasyon teknolojilerinin de gelişmesiyle birlikte gözetlenen kitlenin hacmi daha da genişleyerek, gerek devlet organları gerekse de devlet dışı organlar tarafından yurttaşın kişiye özel, hassas bilgileri de dahil olmak üzere tüm verileri sürekli ve düzenli kayıtlanır hale gelmiştir. Çipli ve/veya biometrik kartlardan, kapalı devre televizyon sistemlerine (*closed circuit television*), parmak izli veya iris okumalı giriş geçiş turnikelerine değin yeni gözetim teknolojileri, insanların gündelik yaşamlarının önemli bir bölümüne varlıkları kanıksanarak dahil olmuşlardır. Bu yeni teknolojiler, 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 tehditi 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 gözetim olgusunun ilk etapta ön plana çıkan özelliği, caydırıcı olması ve güvenliği sağlaması olmaktadır. Ancak bir adım daha ileri gidip gözetim olgusunun arka planına bakıldığında aslında daha farklı bir görüntü ortaya çıkmaktadır: güvenlileştirme politakaların yaşama geçmesi.

---

geniştir: gizli dinlemeye, bilgisayarların aranmasına, onlara el konulmasına, yerel kütüphanelerdeki okuyucu profilini izlemeye ve federal ajanların takdirine bırakılmış diğer müdahaleci prosedürlere onay vermektedir (Mattelart, 2012:216). Bu yasayı takiben 2002 yılının başında "the Homeland Security Act" (Anavatan Güvenliği Yasası) onaylandı ve Anavatan Güvenliği Bölümü (the Department of Homeland Security) kuruldu. Bu yeni bölümün görevi, ABD içerisindeki terörist eylemleri araştırmak, önlemek, korunmak, karşı yanıt vermek ve kurtulmak şeklinde sıralanabilir (Mattelart, 2010:141). Yasa, "anavatan" olarak ABD'ni coğrafik anlamda tanımladı. Güvenlileştirme politikası da bu yasalar çerçevesinde yaşama geçirilmiştir. Örneğin, ABD ve Meksika sınırına Eylül 2006 tarihinde Kongre tarafından kabul edilen "the Secure Fence Act"a (Güvenli Çit Yasası) koşut olarak 1200 km.lik bir çit/duvar örüldü (Mattelart, 2010:142). Bu çalışma için önemi nedeniyle, Vatanseverlik Yasasının dijital gözetimi nasıl meşrulaştırdığını kısaca açıklayalım. Bu yasaya temellenerek, *Total Information Awareness Programı* (Tüm Enformasyon Farkındalığı Programı) Ağustos 2002 tarihinde yaşama geçirilmiştir. Bu programın amacı, veri tabanlarını incelemek, sınıflandırmak ve istihbarat amacı ile yeni algoritmalar oluşturmaktı. Programın adı, 2003 yılında "Terrorism Information Awareness" (Terörizm Enformasyon Farkındalığı) olarak değişti, ama amacı aynıydı: sosyal güvenlik numaralarından, kredi kartı bilgilerinden, FBI kayıtlarından, yerel polis kayıtlarından, banka kayıtlarından, hastane ve sigorta kayıtlarından oluşan tüm kişisel veri tabanlarını merkezileştirmek ve sağlamasını yapmaktı (Mattelart, 2010: 144). Bu veri eşleştirmesinde izlenen model de "risk değerlendirmesi" idi. Kirstie Ball ve Frank Webster (2003: 3) veri madenciliği yapan bu programın, uçak biletlerini, kiralama hizmetlerini, kredi kartı ekstra bilgilerini, banka bildirimlerini, trafik cezalarını, telefon konuşmalarını, ATM kullanımlarını, göçmen bürosu işlemlerini ve e-posta iletişimini incelediğini belirtir. Bu veri tabanına üstelik, havalimanları, anıtlar, kamu binaları gibi çeşitli ana lokasyonlardan alınan kamera kayıtları da eklenmektedir. 2002 yılında onaylanan "the Safety Act"a (Güvenlik Yasası) koşut olarak, terörizme karşı ileri teknoloji destekli mücadele verilmesi de gündeme getirildi ve *The Study of Terrorism and the Responses to Terrorism* (START) oluşturuldu. START, web sitelerinin semantik yapısını incelemeye başladı. START'ın web sitesine göre amaç, "terörist ağlarını bozmak için zamanında rehberlik sağlamak, terörün etkisini azaltmak ve ABD toplumunun terör tehdidi karşısında direncini artırmaktı" (Mattelart, 2012:220). *Global Terrorism Database* (Küresel Terörizm Veri Tabanı) oluşturuldu.

Başka bir deyişle, bilgisayar, cep telefonu, İnternet gibi teknolojiler gündelik yaşamı bir yandan kolaylaştırırken öte yandan da insanların gündelik yaşamlarını gözetim altında tutmaktadır. Alışveriş sırasında kredi kartı kullanımından, sağlık bilgilerinin kayıtlanmasına, telefon ve İnternet kullanımına değin birçok gündelik yaşam etkinliği gerçekleştirildiğinde, bireyler geniş bir veri tabanına dahil edilmektedir. Böylelikle gündelik yaşam pratikleri kontol alınmakta ya da suç olarak nitelendirilebilecek davranışlara zemin yaratmayacak şekilde düzenlenmiş olmaktadır. Dolayısıyla "suçtan arınmış bir toplum ütopyası"nı (Özkazanç, 2007: 15) olanaklı kılacak böyle bir düzenlenmenin gerçekleştirilmesi adına yurttaşların sıradan bilgileri ve hatta özel bilgileri dahi devletin ve özel şirketlerin elinde toplanmaktadır. Modernliğin geç modernliğe evrildiği 1960'lı yıllar böyle bir toplumsal düzene zemin hazırlamış olsa da 1980'li yıllarla birlikte gündeme gelen neoliberal politikalar dolayısıyla güvenlik politikalarına daha da fazla gereksinim duyulmuştur. Bunun içindir ki, güvenlik ve suç kavramları egemen neoliberal düzenin temel kavramları arasında yer almaktadır. Bunu sağlayan ideolojik uygulama ise yönetişim modelidir. Dolayısıyla bu noktada şeffaflık, hesapverilebilirlik ve açıklık gibi unsurlarla tanımlanan yönetişim modeline ve bu modelin önemli bir parçası olan e-devlet uygulamasına bakmak faydalı olacaktır.

1.1. Neoliberal Toplumun İktidar Modeli: Yönetişim ve E-devlet

Kapitalizmin ulusal ve uluslararası boyutunun her geçen gün daha da derinleştiği ve yeniden yapılandığı küreselleşme sürecinde dünya tek bir pazar haline gelmiştir. Böyle bir ortamda devletin gücünü zayıflatan, yasal kural ve normların yerini esnek düzenlemeye bırakan ideolojik bir araç olarak neoliberal politikaların en güçlü uygulama aracı haline gelen "yönetişim" modeli ön plana çıkmıştır. Temel kurucu aktörleri, devlet, toplum ve özel sektör olan yönetişim modeli, "birlikte yönetme ilkesinden hareket ederek 'piyasa için devlet' yaklaşımı çerçevesinde devlet aygıtını öne çıkarmaktadır" (Bayramoğlu, 2005: 57). Dolayısıyla, açık bir şekilde görüldüğü gibi, yöneten ve yönetilen karşıtlığı yerine birlikte yönetime ilişkin bir vurgu söz konusudur. Âdemi merkeziyetçilik esasına dayalı olan güvenlik toplumu, *laissez-faire* (bırakınız yapsınlar) ilkesi, akıcılık ve şeffaflık etrafında örgütlenmiş bir toplum modelidir. Bu da neoliberal yeniden yapılanma sürecinin unsurlarından biri olan ve küreselleşme ile aynı çizgide ilerleyen bir iktidar modeli olan yönetişim modeli ile aynı eksendedir.

Yönetişim, Fransızca'da 13. yy'da yönetim biçimi ve sanatını belirtmek için "*gouvernance*" kelimesiyle ifade edilmiştir (İnsel, 2005: 128). Uzunca bir süre kullanılmayan bu kavram, 1970'lerde Chicago Okulu tarafından gündeme getirilmiştir. Kavram, "şirket işletmesinde yönetim kurullarının merkezi gücünü hissedarlar lehine dengelemek ve işletmeye daha etkin katılımlarını sağlamak, işletmeyi daha saydam ve hesapverebilir kılmak için geliştirilen bir kuramın daya-

nak kavramı" olarak kullanılmıştır (Uçkan, 2003a: 5-6). Burada kavramın işaret ettiği anlam daha çok "şirket yönetişimi"ne ilişkindir. Bugünkü anlamıyla ilk kez Dünya Bankası tarafından 1989 yılında "Sub Saharan Africa: From Crisis to Sustainable Growth" adlı raporda dile getirildiğinde "siyasal iktidarın ulusal faaliyetlerin yönetimi için kullanımı" olarak tanımlanmıştır (Bayramoğlu, 2002: 86). Sözcük başlangıçta, "daha az yönetim"i ya da "minimal devlet"i anlatmak için kullanılmakta iken, bugün gelinen noktada yönetişim modelinde egemen olan görüş, "minimal" devlet söyleminden arındırılmış, bunun yerine "devletin yönlendiriciliği" daha fazla vurgulanmaya başlamıştır (Bayramoğlu, 2002: 88). Yönetişim kavramı devletin gücünü zayıflatan, yasal kural ve normların yerini esnek düzenlemeye bırakan ideolojik bir araç olarak neoliberal politikaların en güçlü aracı haline gelmiştir (İnsel, 2005: 129).

Yönetişim, "devlet toplumu yönetir" savını terk ederek, devletin dışındaki örgütlerin de devlet yönetimine eşit şekilde katılımını öneren bir modeldir. Devlet-toplum arasındaki karşıtlığın ortadan kaldırılması gerektiği düşüncesinden yola çıkan model, küreselleşmenin zorunlu bir süreç olduğu argümanından hareketle küreselleşen bir dünyaya uygun bir iktidar tarzı, yeni bir devlet anlayışı ve yeni bir yönetim üslubu geliştirmeyi hedeflemektedir (Bayramoğlu, 2002: 85). Devletle toplum arasındaki ilişki üzerine yeniden düşünmeyi öneren bu kavram, devlet-toplum karşıtlığını kaldırmayı ve devlet toplum birliğini savunuyordu. Böylece, yönetişim, bir bakıma, devlet-toplum ilişkilerinin kurulması için bir model önermiş oluyordu. Bu model, yönetime katılım ilkesini de aşarak "birlikte yönetme" iddiasını taşıyordu (Bayramoğlu, 2002: 87). Bob Jessop, "yönetişim" kavramını, tıpkı "üretim tarzı", "sivil toplum" gibi, kapitalist yönetsel ve siyasal ilişkileri anlayıp açıklamada analitik bir araç olarak kullanmaktadır (aktaran, Güney, 2006: 154). Jessop yönetişimi, iktidarın mikrofiziği – yani çeşitli devlet projelerinin ve birikim stratejilerinin sürdürüldüğü ve uygulamada birçok değişikliğe uğrayan kanallar – ile ilişkilendirir (aktaran, Güney, 2006: 170).

Yönetişim modelinin getirdiği ilk önemli yenilik, kamu işletmeciliğinin "minimal devlet" anlayışını "düzenleyici devlet" anlayışı doğrultusunda geliştirmek olmuştur. Böylece, devletin küçültülmesi anlayışı yerine, devletin piyasaların etkin bir biçimde işletilebilmesi için etkin düzenlemeler yapması vurgusu öne çıkmaya başlamıştır. Yönetişimin ikinci önemli yeniliği ise, devletin tek karar verici olduğu bir yönetim anlayışı yerine, karar alma süreçlerine devletin yanı sıra özel sektör ve sivil toplumun da katıldığı daha katılımcı bir yönetim anlayışının geliştirilmesidir. Nitekim, yönetişimin kısa sürede hegemonik bir söylem ve model haline gelmesiyle beraber, devlet modelinden demokrasi anlayışına, sosyal politikalardan girişimcilik kültürüne pek çok alanda önemli reformlar uygulamaya geçirilmeye başlanmıştır (Güzelsarı, 2003: 24). Bütün bunlar Dünya Bankası'nın 1991 yılında yayınladığı raporda belirttiği yönetişimin dört temel unsuruna işaret etmektedir: Hesapverilebilirlik, kalkınmanın yasal çerçevesi, bilgilendirme ve saydamlık. Birbirleriyle ilişkili olan bu unsurlar, denetim olgusunu dışarıda bırakıyormuş gibi gözükse de aslında denetimin daha da kuvvetlenmesine aracı olmaktadır.

Dünya Bankası, "dürüstlük, adalet, serbestlik, bağımsız yargı, insan haklarına

saygı, verimli ve yolsuzluktan arınmış bürokrasi" (Güler, 2003: 104) gibi vaatlerde bulunarak bu ilkelerin yönetişimin ve modern devletin temeli olduğunu ileri sürmektedir. Bunun içindir ki, Dünya Bankası yönetişim yerine "iyi yönetişim" (*good governence*) kavramını kullanmaktadır. Buradan hareketle yönetişimin siyasal, ekonomik ve sosyal kalkınmayı da beraberinde getireceğine ilişkin bir yaklaşım söz konusudur. Dolayısıyla hesapverilebilirlik, kalkınmanın yasal çerçevesi, bilgilendirme ve saydamlık gibi yönetişimin temel unsurları aslında etkili yönetim ve verimliliği hedeflemektedir. Hedefe ulaşmanın birincil koşulu da yönetim sürecinde katılan tüm tarafların uzlaşarak, katılımlarının etkin ve sürekliliğinin gerçek anlamda uygulanabilir olmasıdır (Uçkan, 2003a: 15-21).

Yönetişim modeli, yeni enformasyon ve iletişim teknolojileri aracılığıyla devletin yurttaşlarına daha iyi, şeffaf, katılıma dayalı bir hizmet vermesini sağlamak, etkin ve verimli bir kamu yönetimini ve dolayısıyla demokrasiyi açığa çıkaracak bir devlet modelini de beraberinde getirme iddiasındadır. Bu model "e-devlet"[4] olarak adlandırılmaktadır[5]. Yeni enformasyon ve iletişim teknolojilerinin gelişmesiyle enformasyon ağları üzerinden uygulanan ve bir yönetişim modeli olan e-yönetişim ve onun uzantısı olan e-devlet, etkileşim, katılım ve karşılıklılık esasına dayanmaktadır (Uçkan, 2003a: 19). Benimsenen neoliberal politikalar sonucunda kamu yönetimindeki mevcut anlayış yerini özel sektörde egemen olan müşteri odaklı yönetime bırakmıştır. Verimliliği temel hedef olarak alan yeni kamu yönetim anlayışı, yurttaşlarını da birer müşteri olarak konumlandırmaktadır. Bu bağlamda e-devlet uygulamaları da, etkili, verimli ve kaliteli hizmet esasına dayandırılmaktadır. Kullanıcı odaklı bir kamu yönetimini hedefleyen e-devlet olgusunun yurttaşını edilgen bir kullanıcı olarak konumlandırdığı düşünülürse, e-devlet projesinde nasıl bir yurttaş tasarlandığı sorunu ortaya çıkmaktadır. Zira devlet-yurttaş ilişkisi giderek "servis sağlayıcı-müşteri ilişkisine" doğru evrilmektedir (Karakaya-Polat, 2011: 5). Dolayısıyla e-devlet anlayışının, tıpkı yönetişim olgusu gibi, teoride dayandığı ilkelerle pratikteki temelleri arasında bir fark ortaya çıkmaktadır. Bu durum e-devlet uygulamalarına ilişkin dinamik bir tartışmaya zemin hazırlamaktadır. Bu uygulamaları destekleyenler argümanlarını yönetişimin temel unsurları olan açıklık ve şeffaflık üzerinden kurarken; eleştirenler ise dile getirilen şeffaflık ve hesapverilebilirlik gibi söylemlerin gerçekleştirilmediğini vurgulamaktadırlar. Gerek e-yönetişim gerekse onun bir uzantısı olan e-devlet politikaları daha ilk etapta temel esaslarına uymamaktadır. Erişilebilirlik ilkesini eksik bırakmaktadır. Başka bir deyişle, günümüzde e-devlet uygulamaları devlet ile yurttaş arasındaki mesafeyi kısaltmaktadır ancak bu durum enformasyon

[4] E-Devlet Kapısı Projesi'nin organizasyonunda tüm kamu kurumlarında uygulanması amacıyla alt komisyonlar bulunmaktadır. Bu çalışma açısından önem taşıyan komisyonlardan biri de "Güvenlik Grubu"dur. Bilgi güvenliğinin yönetimi önemlidir. Dolayısıyla bu grup, sistemin güvenlik temelinde bütün platformlar için uygulama esaslarını ve politikalarını belirlemektedir (Kumaş ve Birgören, 2010: 30).

[5] "Bilgi toplumu", e-devlet kavramını açıklarken sıklıkla başvurulan kavramlar arasında yer almaktadır. Bilgi toplumuna ilişkin detaylı bir tartışma için bakınız:. Frank Webster, (2004). *The Information Society Reader*, London: Routledge; Nurcan Törenli, (2004). *Enformasyon Toplumu ve Küreselleşme Sürecinde Türkiye*. Ankara: Bilim ve Sanat Yayınları; Manuel Castells, (2005). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür. Birinci Cilt: Ağ Toplumunun Yükselişi*. Çev. Ebru Kılıç. İstanbul: Bilgi Üniversitesi Yayınları.

ve iletişim teknolojilerine erişebilirlik konusundaki mevcut eşitsizlikleri ortadan kaldırmamaktadır. Çünkü "bilgiye erişebilenler ve erişemeyenler arasında ulusal ve uluslararası ölçekte giderek derinleşen uçurum yani dijital bölünme"[6] (Uçkan, 2003a: 37) demokratikleşmeyi sınırlandırdığı gibi, yönetişim modelinin temel esasları arasında yer alan erişilebilirlik unsurunu da ciddi ölçüde tehdit etmektedir.

Neoliberal toplumların karmaşık yapısı verimlilik, standartlaşma, şeffaflık gibi birtakım unsurlarla beslenirken, diğer yandan daha fazla gözetleme ve kontrol altına alma ihtiyacını da beraberinde getirmektedir. Bilgi ve iletişim teknolojileri de böyle bir ihtiyacın giderilmesini sağlamaktadır. İnternet ve akıllı cep telefonları gibi teknolojiler devletin yurttaşını kontrol etmesini ve gözetim altına almasını kolaylaştırmaktadır (Karakaya-Polat, 2011: 2). Dolayısıyla e-devlet uygulamaları da, yurttaşları gözetleyerek denetimin sürekliliğini sağlamak isteyen devletin iktidar araçlarından biri olarak nitelendirilebilmektedir. Bir ağ ile birbirine bağlı sistemler aracılığıyla güvenlik, verimlilik, hızlılık, şeffaflık gibi neoliberalizmin temel unsurları üzerinden yurttaşlar sürekli kayıtlanmakta ve bu veriler otomatik olarak güncellenmektedir. Bu nedenle yönetişimin uzantısı olan e-devlet modelinde bilgi alma süreçleri iktidar mekanizmasını beslemekte ve hatta onunla birlikte işlemektedir. Bunun ardında yatan da devletin riski en aza indirme, kontrolü ele geçirme istemidir. Elia Zureik ve Karen Hindle da yönetişim modelinin iki yanlı keskin bir bıçak olduğunu belirtmektedir: bir yanda enformasyona erişim ve katılım öte yanda da gözetlenme ve kayıtlanma (2004: 113).

Özlüce dersek, neoliberalizmde denetim, suçun önlenmesi ve güvenlileştirme politikaları üzerinden işlemektedir. Dolayısıyla neoliberal toplumlarda suçtan, çatışmadan, güvensizlikten, risk algısından arınmış bir toplumsal yaşamı düşünmek söz konusu değildir. Bunun için de neoliberal toplumlarda sürdürülebilirlik "düzen değil, düzensizliğin; huzur değil, toplumsal çatışmanın; istikrar değil, krizlerin sürekliliğine bağlıdır" (Gambetti, 2008: 146). Dolayısıyla risk yönetimi bu egemen düzende önem taşımaktadır. O halde, Birinci Bölüm'ün bundan sonraki kısmında risk yönetimi olgusunu kısaca ele alalım.

1.2. Güvenlik Adına Risk Yönetiminin Uygulanması

Günümüzde toplumların refahı, risklerin üretimi ile doğrudan ilişkili hale gelmiştir. Başka bir deyişle toplumsal yapı, modernleşmenin beraberinde getirdiği risklerle varlığını sürdürmektedir. Bunun içindir ki, Ulrich Beck (2011: 356) modern toplumu, "kendi ürettiği riskleri tartışma, önleme ve yönetmeyle giderek daha fazla meşgul olması" dolayısıyla "risk toplumu"[7] olarak kavramsallaştırmaktadır.

[6] Dijital bölünme ya da sayısal uçurum, bilişim ve iletişim teknolojilerine eşitsiz erişimi ifade etmektedir. E-devlet politikalarının temel hedefinin e-demokrasi olduğu göz önünde bulundurulduğunda öncelikli olarak, yeni enformasyon ve iletişim teknolojilerine erişim konusundaki mevcut eşitsizliklerin (cinsiyete, yaşa, yerleşim yerine, eğitim durumuna ve sınıfsal konuma bağlı) ortadan kaldırılmasına yönelik asli bir politika geliştirilmesine gereği ortaya çıkmaktadır.

[7] "Risk toplumu" ifadesi, Ulrich Beck'in 1992 yılında yayımlanan *Risk Society: Towards a New Modernity* adlı kitabıyla terminolojideki yerini almıştır. Beck'in risk toplumu kuramına

Beck, potansiyel tehlike ve tehditlerin modernleşme sürecinde büyük bir ölçekte ortaya çıktığını söylemektedir. "Normatif bir emniyet kaybı ve güven yitimi"ne yol açan riskler, deneyimlenmiş olsun olmasın "ütopyaların nesnel olarak değişmiş negatif imgeleridir" (2011: 36). Giddens'a göreyse risk toplumu, daha önceki toplumsal yapılardan daha tehlikeli ve sorunlu değildir. Çünkü, risk, gerçekleşmiş bir tehlikeli edimin yanı sıra "insan etkinliklerini, özellikle geleceğe dönük sonuçları bakımından denetleme özlemiyle yakından ilişkili" olması dolayısıyla yeni bir soruna işaret etmemektedir. Ayrıca riskler seçenekleri de çoğaltıyor olması dolayısıyla çok da sorunlu bir nitelik taşımamaktadır. Bunun içindir ki, Giddens'a göre, risk yönetimi olumlu sonuçları da beraberinde getirmektedir (aktaran Çelebi, 2002: 45). Ancak Beck için riskler tıpkı "saatli bomba" gibidir. Her an patlayacak olması ihtimali dolayısıyla toplumu teyakkuzda bekletmektedir. Dolayısıyla risk toplumunda "olağanüstü" olarak nitelendirilebilecek olay ve durumlar "normalleşmekte"dir. Suç artık modern yaşamın normal bir parçasıdır. Bunun sonucunda, "suç korkusu" kalıcı bir şekilde varolmaya başlamış ve suçları engellemek gündelik yaşamın düzenleyici ilkesi haline gelmiştir[8] . Bu nedenle "suç tehdidinin modern bilincin rutin bir parçası" olması ve "suçun gündelik bir risk" haline gelmesi, onun sürekli gündemde ve kontrol altında tutulmasını da gerekli kılmıştır (Garland, 2001: 106). Ancak risk olgusunun hareketli ve "çok merkezli" olması dolayısıyla, toplumun sadece belirli grupları değil, önemli bir bölümü "risk gruplarına" dahil edilmektedir (Çelebi, 2002: 49). Yığınların ve bireylerin risk kategorileri içerisinde ayrıştırılmaları, risk yönetimini kolaylaştırmaktadır (Lyon, 2007a: 162). Böylece güvenlik olgusu aşkınlaştırılır. Bu noktada David Lyon bireylerin güvenliklerinin sağlanması uğruna özel yaşamlarının gizliliğinden ve mahremiyetlerinden vazgeçerek böylesine yüksek bir bedel ödemeye razı olduklarına dikkat çekmektedir (2006a: 35).

Modern toplumların beslendiği neoliberalizm anlayışı, "olumsallığı[9] ve bunun

göre, risklerin biçimlendirdiği modern toplumlarda küresel risk algılarının üç temel özelliği vardır: Bunlardan ilk mekânsız olması, ikincisi sonuçlarının hesaplanamazlığı, üçüncüsü de telafi edilemezliğidir (2011: 357). Kitabın Türkçe çevirisi için bakınız: Ulrich Beck (2011). *Risk Toplumu: Başka Bir Modernliğe Doğru*, Çev. Kazım Özdoğan ve Bülent Doğan, İstanbul: İthaki.

[8]Ancak, suç korkusu ya da suçun engellenmesi meselelerinden bahsederken altının çizilmesi gereken önemli bir nokta bu korkunun ya da kontrol/engellenmenin hangi gruplara yönelik olduğudur. Ahlaki disiplin ve geleneksel değerlere dönülmesini salık veren yeni-muhafazakârlık, disiplin ve kontrolü özellikle yoksul kişiler ve marjinalleştirilmiş gruplara yöneltir (Garland, 2001: 100). Suç diğer "sınıfaltı" (*underclass*) davranışlarla ilişkilendirilerek (madde kullanımı, yalnız ebeveynlik, vb.), yoksulu etkin bir şekilde cezalandırmanın meşruiyetini sağlamaya yönelik kullanılmaktadır. Mevcut suçlu imajı, "ihtiyaç içinde olan deli" ya da "uyumsuz kişiden", bu işi kariyer için yapan vb. "tehdit edici" kişilere dönüşmüş (Garland, 2001: 102) ve ırksallaşmıştır. Bu noktada Türkiye'de suçun engellenmesi konusunda kamusal alanda alınan tedbirlerde suçun, sınıfaltı gruplarla ve belli etnik kimliklerle eşleştirildiğini, anaakım medyanın da bu etiketlemeleri dolaşıma sokarak ayrımcılığı ve nefret söylemini yeniden ürettiğini söyleyebiliriz. Özellikle, Roman kökenli vatandaşlar ile Kürt vatandaşlara yönelik çeşitli suç etiketlemeleri gerek emniyet kuvvetlerinde gerekse anaakım medyada çok yaygındır. Bu konuda bakınız: Tuğrul Çomu (Yay.Haz.) (2011). *Yeni Medyada Nefret Söylemi*. İstanbul:Kalkedon; Yasemin İnceoğlu (Der.) (2012). *Nefret Söylemi ve/veya Nefret Suçu*. İstanbul:Ayrıntı.

[9]Olumsallık, "bireysel eylemlerin önceden görülemeyen sonuçları", sosyal teorideki "risk" kavramının sosyal felsefedeki karşılığı olarak tanımlanmaktadır. Aykut Çelebi'ye göre, "modern dünyanın olumsallığı, bu düzenin aşkın ölçütleri olmadığını, insanlık tarihinde varılabilecek

kaynağı olarak gördüğü riskli birey ve grupları sınıflandırarak, sürekli denetim altında tutmakta" ve bu süreçte uygulanan politikalar "ortak sigortalama"nın yerine, şüphe oluşturan ve risk barındıran grup ve alanların "izleme ve denetimi"ne odaklanmaktadır (Çelebi, 2002: 49-50). Bu duruma ilişkin daha net bir görüntü ortaya koymak için Ulus Baker'in Mernis Projesi'ne[10] ilişkin yorumuna başvurmak yerinde olacaktır. Baker, bu projenin her ne kadar "kanun kaçaklarını izlemek ve yakalamak" için uygulamaya konulsa da, kanun kaçaklarının tespit edilebilmesinin tüm vatandaşların gözetlenmesi ve kontrol edilmesinden geçtiğini belirtmektedir (2001: 22). Bu durum, tam da Giddens'ın göstermeye çalıştığı totaliter yönetime denk düşmektedir. Devlet için halkın gündelik yaşam pratiklerine dahil olmak ve bunun için de izleme faaliyeti çok önemlidir (Giddens, 2008: 392). Modern devlet, toplumu denetim altında tutarken topluma dair bilgiye de sahip olmak istemektedir. Dolayısıyla iktidar ile bilgi arasında yakın bir ilişki söz konusudur. İktidar ve bilgi alanı dolaysız bir şekilde birbirlerini içermektedir. Zygmunt Bauman, bilginin iktidara meşruluk ve etkililik kazandırdığına dikkat çekmektedir. Bunun içindir ki, iktidar olmak, bilgiye sahip olmayı gerektirmektedir (aktaran Karakehya, 2009: 333). Bundan ötürü de iktidarlar toplumu kontrol edebilmek için onu gözetim altında tutmaktadır. İktidarın bilgiye ulaşmasının bir yolu olan gözetim, aynı zamanda toplumu disipline edici bir niteliğe de sahiptir. Dolayısıyla Foucault için iktidarın gereksinim duyduğu bilgi, "özgürleşimin önünü keserek gözetlemeye, düzene sokmaya, disipline etmeye yönelik bir kip halini alır" (aktaran, Olgun, 2007: 9). Bir başka ifadeyle, iktidarın bilgiye ulaşmak için gözetim olgusunu bir araç olarak kullanması, bu olgunun disipline edici bir araç olarak işlev görmesini de beraberinde getirmektedir.

1.3. Devletin Yurttaşını Gözetlemesi Olgusunun Nedenleri

Günümüzde gözetim olgusunu gündelik yaşamımıza yerleştiren kurumlardan birisi de devlettir. Peki, devlet yurttaşını neden kayıt altına almakta ve gözetlemektedir? Yurttaşların kayıtlanmaları ve gözetlenmeleri iktidarın dünyayı daha anlaşılabilir ve böylelikle denetleyebilir kılma projesinden bağımsız değerlendirilemez. Bundan ötürü, gündelik yaşam pratiklerinin her aşamasına dahil olan gözetim olgusu, günümüze özgü gibi görünse de, aslında yeni bir olgu değildir. Yüzyıllardır süregelen iktidar tekniklerinden biri olan gözetim, "modernite öncesi dönemlerde kabilelerin, imparatorlukların, monarşilerin ve dinlerin başlıca egemenlik mekanizması olarak işlev görmüştür" (Dolgun, 2008: 22). Modernite öncesinde gözetleme bilgisi özellikle yazıyla bağlantılıdır. Resim yazısı,

son noktanın olamayacağını, küresel kapitalizmin yarattığı yeni risk, tehditler, sağladığı yeni olanaklar karşısında her şeyin başka türlü de olma olanaklılığını" yeniden ortaya koymaktadır (2000: 43). Modernliğin ve modern toplumun çözümlenmesinde açıklayıcı bir niteliğe sahip olan risk ve olumsallık kavramlarına ilişkin ayrıntılı bir tartışma için bakınız: Aykut Çelebi (2002). "Risk ve Olumsallık: Sosyal Teori ve Sosyal Felsefe İlişkisini Anlamaya Yönelik İki Anahtar Kavram". *SBF Dergisi*, 56 (1), syf.23-52.

[10] Mernis Projesi'ne ilişkin ayrıntılı bilgi için III. Bölüm'e bakınız.

öncelikli olarak Mezopotamya'da envanter oluşturma amacına hizmet etmiştir. Ugarit'teki bir arkeolojik kazıdan çıkarılan Sami diliyle yazılmış 508 tabletin önemli bir bölümünün idari, istatistiksel ve ticari belgeler olduğu ortaya çıkmıştır (Gelb ve Kramer'den aktaran Giddens, 2008: 63-65). Bunlardan yola çıkılarak, kaydetmenin temel bir biçimi olan yazının modernite öncesinde devletler için farklı işlevlere sahip olduğu söylenebilmektedir. En genel anlamıyla bir "şifreleme bilgisi" olarak yazı, devletin idari denetimini kolaylaştırmaktadır. Bu çerçevede, listeleme yoluyla sınıflandırma, tanımlama, izleme[11] ve yazılı hukuk aracılığıyla davranış kurallarını belirleme gibi fonksiyonlara sahiptir (Giddens, 2008: 66-68). Ancak, modern devletin aksine modern olmayan devletlerde, gözetlemenin yoğun olduğu yerler sınırlıdır. Yani, modernite öncesinde kısıtlı faaliyetleri kapsarken, modernizmle birlikte gözetim genişlemiştir. Yüzyıllardır süregelen gözetim olgusunda sadece biçim değişikliği söz konusudur, ancak esas itibariyle moderniteyle birlikte yeni bir işlev daha kazanmıştır. Zira modernizmde "bütün toplumsal yeniden üretim ve nihayetinde iktidar sistemleri", gündelik yaşamdaki bütün etkinliklerin öngörülebilirliğine bağlı olarak işlemektedir (Giddens, 2008: 21). Bu çerçeve içinde, daha önce bahsettiğimiz devlet idaresi ve yahut yönetsel erk için dünyanın "okunaklı" kılınması temel bir mesele haline gelmektedir. James C. Scott, okunaklılığın devlet idaresinin en merkezi sorunlarından biri olduğunu vurgulamaktadır. Premodern devlet, bu okunaklılık açısından önem taşıyan pek çok araçtan yoksundur. Örneğin, devlet, sınırları içinde yaşayan kişilere, bunların kimliklerine ve mülklerine ilişkin düşük düzeyde bilgiye sahiptir. Başka bir deyişle, premodern devlet, Scott'a göre, ne arazilerinin ne de yurttaşlarının detaylı haritasına sahiptir. Aynı zamanda, "bildiklerini sinoptik bir bakış için gereken ortak bir standarda 'çevirmesini' sağlayacak, bir ölçüm sistemine" de sahip değildir (Scott, 2008: 14). Bu nedenle, devlet, yurttaşlarının askerlik hizmetlerini denetlemek, toplumun güvenliğini sağlamak ve vergilendirmeyi düzenlemek gibi birtakım temel fonksiyonlarının daha kolay işleyişini sağlamak adına nüfusu düzenleyerek denetim altına almaktadır. Soyadlarının oluşturulması, tapu kadastro kayıtları, nüfus sayımları da bu süreçte devletin temel denetim araçları arasında yer almaktadır. Dolayısıyla buradaki temel amaç, daha okunabilir bir toplum için "merkezi olarak kayıt alınıp denetlenebilecek standart bir sistem" oluşturmaktır (Scott, 2008: 14-15)[12]. Buna ek olarak, Scott, okunaklı bir halk oluşturmanın bir diğer yönteminin de isimlendirmelerin "kalıcı, babadan oğula geçen isimler"[13]

[11] Bu izleme faaliyetleri, resmi istatistiklerin ve vaka kayıtlarının tutulmasına dayanmaktadır. Bakınız: Anthony Giddens (2008). *Ulus Devlet ve Şiddet*. İstanbul: Kalkedon, syf. 67.

[12] Scott, çevrenin ve toplumun yeniden şekillendirilmesinin ve dolayısıyla doğanın ve toplumun kontrolünün toplum mühendisliğinin dört bileşeniyle gerçekleştirildiğine dikkat çekmektedir: "doğanın ve toplumun idari olarak düzenlenişi, "yüksek modernist ideoloji", "otoriter bir devlet" ve "bunların planlarına karşı gelme kapasitesinden yoksun, takatten düşmüş bir sivil toplum" (2008: 17-20).

[13] Scott, bu tür babadan oğula geçen isimler ve kimlik kartları, güvelik numaraları gibi çeşitli idari düzenlemelerin başarılı olmasının bunların yurttaşlar tarafından benimsenmesine ve gerekli çağrılara uyularak beyan edilmesine bağlar. Yani bu tür sistemlerin başarılı olmasının ön koşulu "yurttaşın işbirliği"dir. Devletin bu işbirliğini sağlamasının pek çok farklı yöntemi vardır. Örneğin, yurttaşlara ancak bir kimlikleri olursa haklara sahip olacağı söylenir ya da belirli rejimlerde bu tür kartları taşımamak cezalandırılır. "Nihai kimlik kartları, o halde, beden üzerinde silinmesi olanaksız bir işarettir: bir dövme, bir parmak izi, bir DNA 'imzası'" (Scott,

haline dönüştürülmesi olduğuna dikkat çekmektedir. Bu türden kalıcı soyadlarının oluşturulması devlet açısından mal sahipliğinin ve verasetin izini sürmek, vergileri toplamak, mahkeme kayıtlarını tutmak gibi pek çok işlemi kolaylaştırmaktadır. Giddens, bu durumun toplumsal sistemlerin yeniden yapılandırılması sürecini kolaylaştırdığına dikkat çekmektedir. Otorite kaynaklarının burada kullandıkları temel yöntem ise sürekli ve sistemli bir şekilde bilgi depolamalarıdır. Bu nedenle de kapitalist girişim, şiddet araçlarının merkezi denetimi ve endüstriyel üretimin yanı sıra "yoğun gözetleme" de modernitenin belirleyici özelliklerini oluşturan kurumsal kümelerden biridir (2008: 8-12).

Scott'ın bireylerin kayıtlaması ve gözetlenmesine yönelik, nüfus sayımı ve istatistik gibi yöntemlerin yeni bir yönetim biçimi ve devlet türüne yani modern devlete işaret ettiğine ilişkin vurgusunu paylaşan bir diğer isim de Armand Mattelart'tır. Mattelart, modern devletin ortaya çıkış aşamalarında, öncelikli olarak insan davranışını, özellikle suçluların ve akıl hastalarının davranışlarına odaklanarak, anlamaya yarayan yöntemler geliştirilmeye çalışıldığına dikkat çekmektedir: Frenoloji[14] ve fizyonomi[15] gibi bilimler, insan davranışını fiziksel özellikler yoluyla anlama arayışı içinde bulunmaktaydı. Aynı dönemlerde, yine matematiksel ilkeler yoluyla "ortalama insan" kavramı ortaya atılmıştır (Mattelart, 2010: 10-14). Kısacası, insan davranışı farklı yöntemlerle daha okunaklı kılınmaya çalışılmıştır. Bu yönetim biçiminde, Mattelart'ın deyimiyle "sosyal olayları yöneten olasılığın genel kanunları"nı bulma arayışı süreklilik taşımaktadır. Bunun için, öncelikle topluma ilişkin bir kavramsallaştırma ve bunu çeşitli yöntemlerle ölçme pratikleri geliştirilmiştir. Modern devletin, bireyleri ve kalabalıkları tehdit olarak algılayıp, şüpheli olarak konumlandırdığı ölçüde okunaklı kılma çabası artarak devam etmiştir. Her ne kadar 11 Eylül 2001 saldırılarının ardından yoğunlaşsa da "ben" ve "öteki" arasındaki ayrıma dayalı anlayış, kendini aslında daha Soğuk Savaş döneminde dostları düşmanlardan ayırmanın bir ölçütü olan "ulusal güvenlik" kavramsallaştırması ve uygulamalarında göstermiştir. Bunun öncüsünün Amerika Birleşik Devletleri olduğu söylenebilir. Hem yasal hem de kurumsal düzenlemeler yaparak, ABD sadece kendi ülkesi içinde değil, başka ülkelerde de farklı yöntemlerle "ulusal güvenlik" anlayışının egemen olmasını sağlamıştır[16]. Ulusal güvenliğin sürekli tehdit algısıyla biçimlendiği bu dönemlerde enformasyon özellikle "gizli ajanlık" ya da "gözetim" gibi yan anlamlara sahip olmuştur (Mattelart, 2010, 49-56). Bu yan anlamlara uygun olarak, ABD tarafından hem kendi ülkesi hem de dünyanın farklı yerlerinde ulusal güvenlik çerçevesinde yürütülen siyasi ve askeri faaliyetler, 1976'da Amerikan Senatosu tarafından oluşturulan bir komisyon tarafından incelenmiştir. Ortaya çıkan en önemli noktalardan biri de

2008: 560-561).

[14] *Frenoloji*, kişinin kafatası ölçümünün yapılarak kişiye ilişkin özelliklerin ortaya çıkartılmaya çalışılması demektir.

[15] *Fizyonomi*, yüzün incelenerek kişiliğin anlaşılmaya çalışılması demektir.

[16] Amerika Birleşik Devletleri, ülkesinde Senatör Joseph McCharty döneminde 1950-1953 yılları arasında "komünizme karşı" cadı avı başlatmış; 1970'lerin başında da Şili'de Salvador Allende yönetimini istikrarsızlaştırmak için çeşitli siyasi, askeri istihbarat ve işbirliği kampanyaları yürütmüş, hatta Şili'de askeri cunta yönetiminin darbesine destek vermiştir (Mattelart, 2010: 57). ABD'nin Türkiye'deki örtük çalışmaları için bakınız: Danielle Ganser (2005). *NATO's Secret Armies: Operation GLADIO and Terrorism in Western Europe*. New York: Routledge.

"ulusal güvenlik, iç eylem, yıkıcı eylem ve dış istihbarat" gibi nedenlerle gözetim teknolojilerinin meşru olmayan bir şekilde kullanımıdır. Bu gayrimeşru kullanım "suçu olmayan kişi ve kurumlara" dek uzanmıştır[17]. Mattelart, bu pratiklerin, ilgili sivil toplum kuruluşlarının tepkisine rağmen artarak devam ettiğini belirtmektedir[18] (Mattelart, 2010: 58-59). Peter Shields de ABD'nin çeşitli dijital gözetim tekniği uygulamaları üzerine odaklandığı çalışmasında, ABD'nin "terörizme karşı savaş" söylemi adı altında kişisel verilerin ve özel yaşamın gizliliğini ihlal eden bir çok uygulamayı normalleştirdiğine dikkat çekmektedir (2006: 19-38).

Buraya kadar görüldüğü üzere, devletin yurttaşını kayıt altına alıp gözetlemesinin ardında üç temel unsur yatmaktadır: Bunlardan bir tanesi, modern devletin her şeyi hesaplanabilir ve okunabilir kılmak istemesidir. Nüfus sayımı, tapu, askere alma gibi işlemler aracılığı ile devlet, aslında yurttaşlarını daha anlaşılabilir ve dolayısıyla daha açık bir şekilde denetim altına almaktadır. İkincisi, devletin yurttaşlarını potansiyel suçlu olarak konumlandırmasıdır. Aslında bu, özellikle 11 Eylül 2001, Londra metrosu (7 Temmuz 2005) ve Madrid metrosu (11 Mart 2004)[19] gibi birtakım terör saldırılarının ardından devletlerin gerekçe olarak sundukları bir madde olarak değerlendirilebilmektedir. Artık modern devlette suç her an, her yerde yapılabilir bir nitelik teşkil ettiği için, devlet, yurttaşlarını güvende tutmak adına kayıtlama gerekçelerini öne sürmektedir. Bir diğeri de ulusal güvenliğin sağlanmasıdır. Bu unsur aslında devletin herkesi potansiyel suçlu olarak konumlandırması ile alâkalıdır. Bunun içindir ki, bu gerekçeleri öne sürerek devletler yurttaşlarını kayıt altına almaktadır. Dolayısıyla, enformasyon, modern devletin âdeta gizli gözü haline gelirken; gözetim ise, yaşamın doğal akışını dengede tutmak, güvenliği sağlamak, risk yönetimini kolaylaştırmak ve okunaklı bir halk yaratmak için gerekli hale gelmiştir.

1.4. Modern Dönemin Panoptik Stratejileri

Modernite ile birlikte gözetim, sistematize hale gelerek toplumsal yaşamın tümünü neredeyse kapsamıştır. Böylelikle gözetim, ulus-devlet ve demokrasinin ayrılmaz parçası haline gelmiştir. Başka bir deyişle, "ulus-devlet, vatandaşlarının beklentilerini yerine getiren ve onları –çift yanlı biçimde- gözeten; ancak mutlak gücü de elinden bir an olsun bırakmayan bir iktidar olarak" ortaya çıkmaktadır.

[17] Bunun kurumlara değin uzatılmasının bir örneği ECHELON isimli ağdır. Bu elektronik ajanlık sistemi özellikle, mesaj alıkoyma ve düşmanın stratejik bağlantılarını çözme konusunda bir hayli ileri gitmiştir. Başka ülkelerle yapılan ortaklıklarla ABD bu ağı genişletmiştir. Temel amaç soğuk savaş mantığı içerisinde Doğu Bloku'ndan gelen askeri ve diplomatik mesajların gözetlenmesidir (Mattelart, 2010: 59-60).

[18] 2001 senesinde başlayan terörist gözetim programı, "casusluk yapan ajanın, 1978'de Senato soruşturması ardından Dış İstihbarat Gözetim Yasası ile kurulan özel mahkemeden izin almaksızın, yabancı ülkelere telefonla yapılan iletişime ya da e-posta iletilerine el konulmasına izin veriyordu" (Mattelart, 2010: 59).

[19] Detaylı bilgi için bakınız: Sabah Gazetesi'nin 9 Temmuz 2005 tarihinde yayınlanan "Londra'da Terör Dehşeti" başlıklı haberi, http://arsiv.sabah.com.tr/ozel/londrada1110/dosya_1110.html, (Erişim tarihi: 29 Şubat 2012).

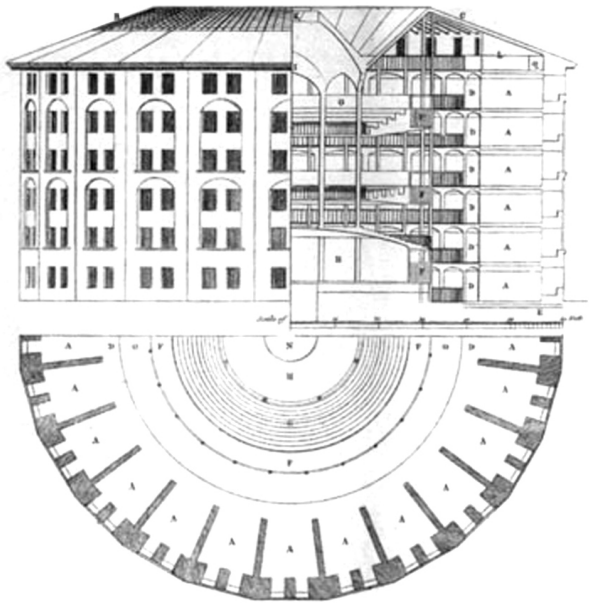
(Dolgun, 2008: 99). Gözetim olgusunun modernite içerisinde önemli bir yer edinmesi sonucu bu olgu, kuramcıların üzerinde durdukları temel sorunlardan biri haline gelmiştir. Her biri gözetimi kendi yaklaşımları ve çalışma alanları çerçevesinde açıklamıştır. Karl Marx üretim sürecinden hareket ederek gözetim olgusunu sınıf ilişkileri bağlamında analiz ederken, Max Weber, bir gözetim unsuru olarak bürokrasiyi incelemiştir. Marx, kapitalist ekonomilerde gözetimin emek ve sermaye arasında verilen mücadelede açığa çıktığını ve sermayenin, idari denetimi sağlayabilmek için işçileri gözetlediğini söylemektedir. Gözetimin sadece sınıf ilişkileri ile sınırlandırılmasına karşı çıkarak modern toplum içerisinde bir bütünsellikle açıklanması gerektiğini düşünen Weber'e göre ise gözetim, "modern örgütler ile devlet idaresindeki yöneticilerin, bireyleri ve topluluğu fişlemeye yönelik dosyalar tutması paralelinde, kişisel bilgileri içeren veri saklama tekniklerini ve bu verileri çağırma araçlarını geliştirdikleri bir yöntemi ifade eden bürokrasi ile çevrilidir" (aktaran, Dolgun, 2008: 98-99).

Gözetim olgusuna ilişkin en temel vurgu modernitenin bireyler üzerindeki etkisi ve getirdiği yeni iktidar ilişkileri üzerine çalışmış olan Fransız filozof Michel Foucault'ya aittir. Gözetime ilişkin çalışmaların beslendiği Jeremy Bentham'ın "panoptikon"u[20] aslında Foucault ile gündeme gelmiştir. Panoptikon, gözetlemenin, bir kulenin etrafında birçok hücreden oluşan ve bir gardiyanla bile birçok mahkûmun aynı anda denetlenebildiği merkezi bir yapıdır. Foucault, bu mimari yapıyı şöyle açıklamaktadır:

> "Halka şeklinde bir bina ve ortasında bir kule ve kuleden halkanın iç cephesine bakan geniş pencereler... Kuleye bakan bina hücrelere ayrılmıştır. Hücrelerin her biri bina boyunca derinlemesine uzanır. Bu hücrelerin iki penceresi vardır: Biri içeriye doğru açıktır, kulenin pencerelerine denk diğer; 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" (2007: 86).

Foucault'nun da işaret ettiği bu mimaride gözetmen locasında gözetleyici ailesi ile birlikte kalmaktadır. Ailenin kalabalık olması durumunda bir kişi görevli olmasına ve ailenin diğer fertlerinin başka uğraşları olmasına rağmen dışarıyı izleme ve pencereden dışarı bakma gibi gündelik eylemler bile gözetleme sürecinin parçası haline gelmektedir. Bu da Bentham'ın daha 18. yüzyılda tasarladığı panoptikon modelinde bakışın bir iktidar tekniği olarak algılandığını göstermektedir

[20] Panoptikon, Jeremy Bentham ile gündeme gelmiş ve projenin büyük bir bölümü ona ait olsa da, esas olarak kardeşi Samuel Bentham'ın fikridir. 1789 yılında Samuel Bentham tarafından tasarlanan panoptikon, merkezi denetim ilkesine dayanarak, daha çok işçinin gözetim altında tutulmasını sağlayan bir yapı olarak düşünülmüştür. Jeremy Bentham, 1786'da Rusya'ya abisini ziyarete gittiğinde bu projeden etkilenenerek, bu mimarinin gözetimevi olmasının ötesinde hapishane gibi çok sayıda insanı gözetim altında tutacak yapılara uygulabileceğine karar vermiş ve bunun üzerine tasarladığı bu yapıyı 21 mektuptan oluşan "Panoptikon Mektupları"nda dile getirerek İngiliz hükümetine göndermiştir. Bu konuda detaylı bilgi için bakınız: Barış Çoban ve Zeynep Özarslan (Yay. Haz.) (2008). *Panoptikon: Gözün İktidarı*, İstanbul: Su Yayınları.



Jeremy Bentham'ın hapishane modeli

(Bentham, 2008: 24). Aklın akıl üzerinde güç kazanmasının yeni biçimi olan panoptikon, Bentham'ın pragmatik ceza hukuku teorisini, cezalandırma hakkı olarak geliştirerek somutlaştırdığı bir model olarak tasarlanmıştır (Mattelart, 2010: 9).

Bentham'ın panoptikonu tasarladığı dönemde bu yapı, mimari bir model olarak tasarlansa da günümüzde mimari yapının da ötesinde politik ve toplumsal bir yapılanmaya gönderme yapmaktadır. Gerek kapitalist sistemin devamlılığı gerekse de iktidar ve güç odaklarının egemenliklerinin sürdürülmesinde panoptikon, "güvenlik ve verimlilik modeli" olarak nitelendirilmektedir (Çoban, 2008: 139). Dolayısıyla Bentham'ın tasarladığı bu kavramın, zamanla farklı bir kullanıma dönüştüğünü söylemek mümkündür. Bauman'ın deyişiyle, panoptikon, modernitenin ikonu haline gelmiştir (2005: 128). Dolayısıyla birçok düşünür, Bentham'ın panoptikonunu bir metafor olarak kullanarak modern toplumlarda gözetim olgusunun toplumdaki yeri ve etkilerini tartışmaktadır. Foucault da bu düşünürler arasında yer almaktadır.

1.5. Kusursuz Bir İktidar İçin Sürekli Denetim: Biyo-Politika

Panoptikon metaforunu merkeze koyarak hapishane ile fabrika arasında ilişki kuran Foucault, insanların yaşamlarındaki tüm alanlarda nasıl gözetim altına alındığına dikkat çekmiştir. Foucault, panoptikon modelini en geniş biçimde

tartıştığı eseri olan *Gözetim Altında Tutma ve Cezalandırmak: Hapishanenin Doğuşu* kitabında akıl hastanesi ve hastane gibi 18. yüzyılda kurumsallaşan hapishaneyi aynı zamanda modern toplumun disipline edici mekanizmalarını ortaya çıkaran bir yapı olarak tanımlar. Foucault, gözetlenen bireylerin, görüldüğünü ama göremediğini, böylelikle bir bilginin nesnesi olduğunu ama hiçbir zaman iletişim sürecinin öznesi olamayacağını vurgulamaktadır. Foucault'ya göre, bu durum panoptikonun en temel özelliğidir. Yani panoptikon tutuklanan, gözetlenen kişide "iktidarın otomatik işleyişini sağlayan bilinçli ve sürekli bir görülebilirlik halini" yaratmaktadır (Foucault, 2000: 296-297). Dolayısıyla, bu görünmeden görme edimi, ne zaman, nerede ve kim tarafından gözetlediğini bilmemesi dolayısıyla insanlarda her an gözetleniyor olma hissini yaratmakta ve bir süre sonra bu his doğallaşarak boyun eğmeyi kolaylaştırmaktadır. Foucault, doğallaşmaya başlayan bu iktidarı "biyo-iktidar" olarak kavramsallaştırarak, bu iktidar modelinin "nüfus olarak ortaya çıkan bir canlılar topluluğuna özgü fenomenlerin (sağlık, doğum, uzun yaşam, ırklar) hükümet uygulamalarının karşısına çıkardığı sorunların nasıl akılsallaştırıldığını" anlattığını ifade etmektedir (2001: 109). Daha açık bir şekilde ifade etmek gerekirse, Foucault'da biyo-iktidar kavramı "bedenlere incelikle hükmederek, yaşamları dikkatlice yönetme üzerine kurulu"dur (aktaran, Bozok, 2011: 42). Dolayısıyla bu iktidar biçimi, insanların doğumlarından ölümlerine dek hayatlarının akışını kendi içerisine çekmektedir[21].

Biyo-iktidar, normlarla çerçevelenmiş bir toplumda "normal" insanlar yaratmayı hedeflemektedir. Foucault'ya göre biyo-iktidar, disiplin ve denetim mekanizmalarıyla birlikte işlemektedir[22]. Disiplinci iktidar, ideal bir davranış modeli tasarlayarak norm belirlerken, diğeri ise "güvenlik" vurgusuyla "normalliği hesap etmekle başlar, yani normalliğin eğrisini çıkarır" ve normun genel çerçevesini buna göre çizmektedir (Gambetti, 2008: 151). Michael Hardt ve Antonio Negri, yeni bir iktidar paradigması olarak biyo-iktidarın ortaya çıkışını, disiplin toplumundan denetim toplumuna geçiş bağlamında tartışmaktadırlar. Onlara göre, biyo-iktidar, "toplumsal hayatı onu izleyerek, yorumlayarak, soğurarak ve yeniden eklemleyerek içeriden düzenleyen" bir iktidar türü olarak tanımlamaktadırlar[23] (2008: 48). Dolayısıyla, buraya kadar aktarılanlardan görüldüğü üzere biyo-iktidar, aslında her şeyi bilen, her yerde olan ve her şeye gücü yeten olarak[24] kavramsallaştırılmaktadır. Bunun içindir ki, Foucault, panoptikonu, "iktidar laboratuarı" olarak

[21]Yönetişim olgusunun biyo-iktidar ile birlikte gerçeklemesi üzerine zihin açıcı bir çalışma için bakınız: Elia Zureik ve Karen Hindle (2004). "Governance Security and Technology: The Case of Biometrics", *Studies in Political Economy*, 73, Spring/Summer, syf. 113-137.

[22]Foucault, iktidarın üç farklı türünden bahsetmektedir. İlki, egemenlik, ikincisi normlara uygun davranan bireyler üreten ve 17. yüzyılda gündeme gelen disiplin paradigmasıdır. Sonuncusu ise, 18. yüzyılın sonunda gündeme gelen güvenliktir. Bu konuda detaylı tartışma için bakınız: Michel Foucault (2001). *Ders Özetleri* 1970-1982, Çev. Selahattin Hilav, İstanbul: Yapı Kredi Yayınları; Zeynep Gambetti (2008). "Foucault'da Disiplin Toplumu-Güvenlik Toplumu Ayrımı", *Mesele*, No. 20, syf. 43-46.

[23]Hardt ve Negri, biyo-iktidarın "maksimum çoğulculuk ve sayısız tekilleşme içeren bir olay ortamı" yarattığını savunmaktadır. Biyo-iktidar ve denetim toplumunun "İmparatorluk" kavramlarıyla benzeştiğini söylemektedir. Bakınız: Michael Hardt ve Anthony Negri (2008). *İmparatorluk*, Çev. Abdullah Yılmaz, İstanbul: Ayrıntı Yayınları, syf. 46-56.

[24]Her şeyi bilen *omniscience*; her yerde olan *omnipresent* ve her şeye gücü yeten *omnipotent* iktidar.

değerlendirmektedir (2000: 301). Foucault'ya göre panoptik toplum, sürekli gözetim esasına dayanmaktadır ve "denetim/cezalandırma ve ödüllendirme gibi mekanizmalar yoluyla bireylerin belli kurallara göre dönüştürülmesini hedefleyen ve direkt bireyler üzerine uygulanan iktidar biçimi"dir (aktaran, Dolgun, 2008: 105).

Böyle bir ilişkinin ardında iktidarın yaratmaya çalıştığı "her yerdelik" hissi yatmaktadır. Devlet her şeye muktedirdir. Bu his, insanların sürekli izlendiklerine ilişkin bir düşünceye kapılmalarına neden olmaktadır. Simon Werret, "Potemkin ve Panoptikon: Samuel Bentham ve On Sekizinci Yüzyıl Rusyasında Mutlakiyetçi Mimari" makalesinde Ortodoks kilisesi ile panoptikon arasındaki ortak noktaya dikkat çekmektedir: "Ortodoks kilisesi ile panoptikon arasında doğrudan bir ilişki olduğu öne sürülemez, ama panoptikon ve kilisenin her ikisinde de merkezi nokta, yapıların mimarisi tarafından ifade edilen, bu görünüşteki "her yerdelik"tir. Her ikisinde de "görünmeden görme" teması söz konusudur (2008: 103). "Görünmeden görme" özelliği dolayısıyla gözetim olgusu içselleştirilerek kişiliğin parçası haline getirilmiştir. Foucault, böyle bir disiplinin 19.yüzyılda okullar, hapishaneler ve hastane gibi kurumlarda kurumsallaştığını gözönünde bulundurarak, panoptikonu toplumun "idealize edilmiş bir mikrokosmozu" ya da "kafesi" olarak adlandırır. Panoptikonu düşsel bir yapı olarak algılayarak, bu yapının iktidarı ideal biçime getiren bir diyagram olduğunu belirtir. Her tür direnç ve çatışmadan uzak, saf bir yapıdır, panoptikon (Foucault, 2000: 302-303). Temel referans noktasını iktidar olarak belirlediği gözetim çalışmalarında, Foucault, tek bir iktidarın değil, birden fazla iktidarın varlığından bahsetmektedir. Heterojen özellikler taşıyan iktidarlar farklı tahakküm ilişkileri içerisinde açığa çıkmaktadır (Dolgun, 2008: 93). Özü itibariyle, Foucault'ya göre, gözetimden beslenen iktidar, toplumsal yaşamın bütününe hakim olarak mikro ve makro düzeylerde güç ilişkileri içerisinde varlığını sürdürmektedir.

Foucault'ya göre, panoptikonnun önemi, tuğla ve harçla yapılan inşasında değil, yarattığı disiplin mekanizmasında yatmaktadır. Ona göre 19. yüzyılda oluşan toplumların temel özelliği şöyledir:

> "Tek bir kişiye verilmiş olan ve bu kişinin başkaları üzerinde uyguladığı bir güç yoktur, bu herkesi içine alan bir makinedir. İktidarı işletenler kadar üstlerinde iktidar işletilenler de buna dahildir. ... İktidar doğumundan itibaren iktidara sahip olan ya da onu işleten bir kişiyle artık maddi olarak özdeş değildir. Yasal sahibi olmayan bir makineler bütünü haline gelmiştir" (2007: 96).

Dolayısıyla Foucault, panoptikon'un, iktidarı otomatikleştirip bireysellikten çıkarttığını öne sürmektedir. Denetim mekanizması artık bireysel olarak işlemez hale gelir ve merkezi kulede gözetleme yapan kişinin kim olduğu önemli değildir. Sistemi sürekli kılarak baskının içselleştirilmesinin sağlanması önem taşımaktadır (Foucault, 2007: 95). Bunun içindir ki, herkesin artık kendini gözetlemeye başlamasıyla birlikte, Foucault'nun da "mükemmel formül" olarak nitelendirdiği sürekli gözetim hali böylece ortaya çıkmaktadır. Bu da gözetimin en

temel prensiplerinden olan "kendi kendine gözetim"i geliştirmekte, beslemektedir. Dolayısıyla bu durum, toplumun "uysal bedenler"e dönüşmesini de beraberinde getirmektedir ve "uysal bedenler, sadece otoritenin bakışından değil, içsesin akışa dönüşmüş şekliyle beraber oluşmaktadır" (Güven, 2007: 90). Nick Mansfield'e göre, panoptikonun işlevi, bireyselleştirme, normalleştirme ve hiyerarşize etmedir:

> "Foucault'a göre panoptikon, modern yaşamı yöneten öznelleştirme süreçlerinin tipik bir örneğidir. İktidar toplumu bireysel birimler halinde düzenler, bunun amacı özneyi maksimum görülebilir bir sistem içerisinde gözlem altında tutmaktır. Bu, en etkin şekilde kurumlarda işler. Hastahaneler, okullar ve üniversiteler, bankalar, sosyal güvenlik ve vergi daireleri, hepsi bizimle ilgili dosyalar tutar. Bunları basitçe unutur geçeriz ya da onları bu kurumların işleyişinin kaçınılmaz ve zorunlu bir parçası olarak kabul ederiz. Ancak onlar etkili toplumsal gerçekliğimizdir ve bizimle ilgili, kontrolümüz dışında manipüle edebilir 'hakikatler' içeriler. Dosyaların kendileri gibi, hakkımızda içerdikleri hakikatler de, bizim tasarrufumuzda değildir" (2006:81).

Ali Toprak, Ayşenur Yıldırım, Eser Aygül, Mutlu Binark, Senem Börekçi ve Tuğrul Çomu da Foucault'un iktidar çözümlemesini izleyerek, *Toplumsal Paylaşım Ağı Facebook: "Görülüyorum Öyleyse Varım!"* adlı (2009) çalışmalarında, gözetlenmenin ve kayıtlanmanın bireyin yaşamının içine nasıl dahil olduğunu şu şekilde açıklamaktadırlar:

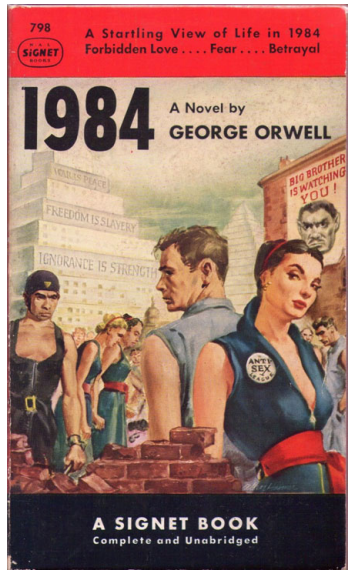
> "Günümüz dünyasında iktidar çok daha görünmez patikalara sahiptir. Mimari yapının yerini elektronik mimari almıştır. Hemen her köşe başına konulan kameralardan edinilen görüntü kayıtları, cep telefonlarının yaydığı sinyaller, bilgisayar IP numaraları, e-posta takip sistemleri, ilerisi, uzaya fırlatılan uydular aracılığıyla tüm dünya gözetim altında tutulmaktadır. Birkaç yıl öncesinde piyasaya sürülen Googleearth programı ile evinde, oturduğu yerde tüm dünyayı gözetleme olanağına erişebilen "sıradan" bireyler için iktidarın ne denli kapsamlı sistemlere sahip olduğunu düşünmek ürkütücüdür. Bugün teknolojinin ulaştığı bu korkunç nokta ile, bireyin gözetlenmekten korunma olanağı yoktur. Cep telefonu, bilgisayar gibi görece daha yeni ve pahalı ürünler bir yana, televizyon ve hatta radyo dâhil hiçbir teknolojik ürüne sahip olmayan, dahası evinden dışarı adım atmayan bireyler dahi bu enternasyonal gözetim ağına yakalanmışlardır. Isıya duyarlı takip sistemleri ile artık kapalı bir mekân içinde, sözgelimi evde dahi insanların tüm hareketleri rahatlıkla gözetlenebilmektedirler (Toprak vd., 2009: 146-147).

1.6. Gözetim ve Denetimin Her Yerdeliğinin Normalleşmesi ve İçselleştirilmesi

Panoptikonun iktidarın kendini yeniden kurduğu temel mekanizmalarından biri haline geldiğini savunan bir diğer düşünür de Bauman'dır. Modernleşme süreci ile birlikte panoptik stratejilere daha sık başvurulduğunu dile getiren Bauman, panoptikonun yapay bir mekân olduğunu savunmaktadır. Panoptikonun aslında güç ilişkileri içerisinde "mekânın şeffaflığını bilinçli bir biçimde manipüle etmek ve iradi olarak yeniden düzenlemek" için yapılandırıldığını söylemektedir (2006: 43). Böylelikle mekânın iktidar için kolaylıkla erişilebilecek bir haritası da ortaya çıkmaktadır. Bauman böyle bir iktidar stratejisinin modern öncesi dönemlerden farkını, seyretmek ve seyredilmek üzerinden kurmaktadır. Modernite öncesinde kendisini ve gücünü benimsetmek için seyredilmeyi tercih eden iktidar ve güç odaklarının yerini artık yeni modern dönemde gücünü uyruklarını gözetim altında tutarak sağlayan ve buradan beslenen iktidarlar almıştır (Bauman, 2006: 62). Bauman, bu noktada Foucault ile ortak paydada buluşarak iktidarın sürekli her yerdeliğine vurgu yapmaktadır. Öyle ki, yeni iktidar teknikleri "karşılıklı bağımlılık ve sürekli karşılıklı angaje olma durumu"nu gereksiz görerek iktidarını sağlamaktadır (Bauman, 2005: 49).

Buradan hareketle, iktidarın her yerdeliğini anlayabilmek için aslında gözetim olgusunu toplumsal denetim ve iktidar ilişkileri içerisinde ele almak gerekmektedir. Deleuze'ün denetim toplumunu takiben Foucault'nun disiplin ve güvenlik toplumu modelleri aslında gözetim olgusunun işleyiş haritasını açık bir şekilde ortaya koymaktadır. Beden üzerinden otorite uygulayan disiplin toplumunun aksine, güvenlik toplumu otoritesini, bir bütün olarak topluma, 'insanların yaşamları' üzerine uygulamaktadır. Denetim toplumunda ön plana çıkan temel nokta, "disiplinci kulluğun zemin kaybetmesi ve yerini başat hükmetme tarzı olarak hizmetçiliğe bırakması"na dayanmaktadır (Holland, 2005: 83). Denetim toplumunda ön plana çıkan bir diğer olgu da güvenliktir. Güvenlik kavramı, Deleuze'ün çizdiği denetim toplumunun sınırları içerisinde "bireysel ya da sayısal bedenin yerine denetlenmesi gereken 'bölünebilir' bir materyalin kodunu koyan" bir nitelik kazanmaktadır (Deleuze, 2006: 203). Güvenliğin sağlanmasındaki temel paradigma ise gözetim ve denetimin her yerdeliğidir. Disipline dayalı iktidar, hapishane, okul, fabrika gibi kapalı alanlarda işlerken, denetim "gizil" bir biçimde her yerdedir.

İktidarın gözünün sürekli toplumun üzerinde olmasına rağmen iktidar, çok da fazla göz önünde değildir. İktidarın özünde gizliliğin yattığını dikkate alındığında iktidarla toplum arasında asimetrik bir ilişkinin olduğu açık bir şekilde ortaya çıkmaktadır (Mattelart, 2010: 9). Gözetim toplumlarındaki asimetrik güç ilişkisine vurgu yapan isimlerden biri de Kiyoshi Abe'dir. Bu ilişki biçimine örnek olarak da "The Myth of Media Interactivity: Technology, Communications and Surveillance in Japan" makalesinde Japon toplumsal paylaşım ağlarından biri olan Mixi üzerinden örnek vermektedir. 20 milyondan daha fazla kullanıcısı olan Mixi'de kullanıcılar sistemde bütüne dahil olamamaktadır. Ancak kendi sayfalarını



George Orwell'in 1984 romanı

kontrol edebilmektedirler. Buna karşın bütün veriler tek bir sistemde kayıt altına alınmaktadır (Abe, 2009: 79). Böylece kullanıcı oluşan büyük bir veri tabanına dahil olmakta, iktidarın heryerdeliğini hissetmemektedir.

Panoptikon gibi sürekli denetimi sağlayan iktidar aygıtlarına bir örnek de George Orwell'in 1984[25] romanında teleekran olarak adlandırdığı 24 saat kapatılmayan ekranları verebiliriz. Bu disütopik romanda kule ve gözetleyiciler yerine, teleekranlar ve onlar aracılığıyla insanları gözetleyen "Büyük Birader" (*Big Brother*) gözetimi gerçekleştirmektedir. Ekranlarda görünen Büyük Birader insanlara sürekli gözetim altında olduklarını hissettirerek, davranışlarının disipline olmasını sağlamaktadır. Bugüne dair birçok gönderme yapan ve özgür olduğunu düşünen insanların aslında basit gündelik yaşam pratikleriyle bile iktidar aygıtına teslim olduğuna dikkat çeken bir roman olan Yevgeny Zamyatin'in *Biz*[26] adlı romanı burada belirtilmesi gereken bir diğer önemli eserdir. Roman 26. yüzyıl toplumunda geçmektedir. Romanda sınırları belli, belirsizliğin olmadığı bir yaşam söz konusudur. Dolayısıyla mutluluğun kaynağı, kusursuz matematiksel bir yaşam olarak ileri sürülmektedir. Sayılarla kodlanmış bireyler söz konusudur. İnsanlar tektipleştirilerek, bürokratik devlete teslim edilmiştir. En önemlisi saydam cam duvarlar arasında her an denetlenebilen bir yaşam söz konusudur.

Seyredilme olgusu, panoptikonda da, teleekranda da aslında azınlığın çoğunluğu izlemesi olarak gündeme gelmektedir. Ancak özellikle televizyonun gündelik yaşamın ayrılmaz bir parçası haline gelmesiyle birlikte, artık çoğunluğun azınlığı

[25] George Orwell (1989). *Bin Dokuz Yüz Seksen Dört*, Çev. Nuran Akgören, İstanbul: Can Yayınları

[26] Yevgeny Zamyatin (2011). *Biz*, Çev. Algan Sezgintüredi, İstanbul: Versus Kitap Yayınları.

izlediği bir gözetim kültürü ortaya çıkmıştır. Bu toplumsal ve kültürel olgu Norveçli bir sosyolog olan Thomas Mathiesen'in geliştirdiği "sinoptikon" kavramıyla gündeme gelmiştir. Burada, bedenlerin, insanların oturdukları yerde, yerellikten kopartılmayarak, siber mekâna çekilerek, başkalarının hayatını gözetlediği bir gözetim süreci söz konusudur. Günümüzde ise İnternet'in yaygınlaşmasıyla birlikte, sinoptikondan "omniptikon"a geçilmiştir. Artık çoğunluğun birbirini izlediği bir gözetim süreci söz konusudur. Burada da sosyal paylaşım ağları olan Facebook, Twitter gibi araçlar üzerinden insanların birbirlerinin yaşamlarını gözetim altında tuttuğu görülmektedir. Dolayısıyla, aslında "Bentham'ın hayalini kurduğu, Foucault'nun akademik alanda kuramsallaştırdığı, Orwell'in karşı ütopya şeklinde tahayyül ettiği panoptik toplum" (Dolgun, 2008: 22), 20. yüzyılla birlikte elektronik ağlarla, siber mekânda yaşama geçmiştir, denebilir. Toprak ve arkadaşlarının Facebook üzerinden bireylerin kendi özel yaşamlarını sergilemesi ve diğerlerinin yaşamlarını/paylaşımlarını gözetlemesi, diğer bir deyişle dikizlemesi üzerine yaptıkları saptamaları ilgi çekicidir:

> "Bu noktada, bireylerin gözetlenmekten haz duymaya evrilmesi durumu ele alınmalıdır. Toplumsal kaygı, artık gözetlenmek değil, göz önünde bulunamamak yönündedir. Görünürlüklerini, erişilebilirliklerini arttıran teknolojik araçlara büyük bir istek ve arzu ile yönelen, her an, her yerde görünür olmak kaygısı taşıyan bireylerin toplamı anlamında bir teşhir toplumundan söz etmek artık hiç de abartı sayılmamaktadır. Zygmunt Bauman'ı izleyerek, dersek: "Toplumun gözetlenmekten zevk alması, hatta iktidarın istemine gerek kalmadan kendisinin gözetlenmesini istemesi (teşhircilik) toplumun iktidara teslimiyetini gösterir; "panoptikon insanları seyredilebilecekleri bir duruma zorla getirir. Synoptikonun ise baskıya ihtiyacı yoktur, insanları seyretsinler diye ayartır" (aktaran Çoban, 2008:122)" (Toprak vd. 2009: 152).

Toprak ve arkadaşları, özel olarak Facebook vb. toplumsal paylaşım ağları üzerinde varoluş gösteren bireylerin, genel olarak İnternet öznelerinin hem röntgenci, hem teşhirci hem de muhbir olmayı başarabildiğini de iddia eder (2009:186). Bireylerin, elektronik ağlarda varoluşunun bu şekillerde gerçekleşmesi gözetimin heryerdeliğini daha da olanaklı kılmaktadır.

1.7. Panoptikondan Süper Panoptikona

İnsanlık tarihi kadar uzun bir geçmişe sahip olan gözetim olgusunun günümüzde yeni bir olgu olarak gündeme getirilmesinin ardındaki itici güç, enformasyon teknolojileridir. Yeni iletişim teknolojilerinin de etkisiyle, yeni iktidar ve toplumsal denetim pratikleri arasında merkezi bir yer edinen gözetim olgusu, gündelik yaşam ve toplumsal ilişkiler içerisinde daha da derin bir yer edinmiştir. Gözetimin post-modern toplum yaşamının her aşamasına işleyişini David Lyon şöyle ifade etmektedir:

> "Eğer bir seyahate çıkmak zorundaysam ve eğer güzergâhım da Kanada'dan Amerika'ya doğru ise, bütün evraklarımı dikkatli bir şekilde incelerim ve havaalanı güvenlik istasyonunda sınır geçiş kontrolleri için gerekli fazla zamanı hesaplayarak yola çıkarım. Havaalanına gelince başta güvenlik bölgesi ve havaalanı resepsiyonu olmak üzere gözetimin heryerdeliği varolan kameralarla aşikârdır. Aslına bakarsanız ben havalanına ulaşmadan önce gözetimim zaten başlamaktadır: Rezervasyon bilgilerim yemek tercihlerim, sağlık durumum gibi kendimle ilgili birçok bilgiyi açığa çıkarmaktadır" (2007b: 11).

Lyon'un da altını çizdiği bu güvenlileştirme edimi bugün sadece havaalanlarına özgü değildir. Günümüz toplumu, 20. yüzyılın sonlarından itibaren elektronik ağlar ve dijital gözetim teknolojileri dolayımıyla huzur ve güven arayışı içinde bulunan bireylerin kendi rızaları ile gözetlenmeyi arzu ettikleri bir topluma dönüşmüştür. İnternet'te ziyaret edilen web sitelerinin izlenmesi, elektronik postaların okunması, şehrin dört bir yanına yerleştirilen MOBESE'ler, cep telefonlarının dinlenmesi, kredi kartlarının insanları tutsak alması ve bunlar gibi birçok teknoloji odaklı eylem iktidarın denetim ve gözetim faaliyetlerini her geçen gün daha da güçlendirmektedir (Dolgun, 2008: 14). Özel alandan kamusal alana kadar bireyin günlük bütün etkinlikleri Lyon'un benzetmesi ile, "elektronik gözler" (1997) tarafından izlenir hale gelmiştir. Gözetimin enformasyon teknolojilerinin gelişimine bağlı olarak yaygınlık ve işlerlik kazanması üzerine ilk çalışmaları yapan Gary T. Marx, 1985 yılında yazdığı "Gözetim Toplumu: 1984 Tarzı Tekniklerin Tehdidi"[27] başlıklı makalesinde enformasyon teknolojilerinin gündelik yaşamın en küçük ayrıntılarını dahi izlediğine dikkat çekmektedir:

> "Bir çocuk bakım merkezinin İnternet ağından bebeklerini denetleyen bir anne baba; işverenler için iş bulma formunu dolduran kişilerin ismini içeren veri tabanı; bir mağazada müşterileri tarayıp suratlarını şüpheli hırsızlarla eşleştiren video monitör; çalışanların e-postalarını ve telefon görüşmelerini denetleyen işveren; bir çalışanın her zaman nerede olduğunu gösteren sinyal rozeti; bir ATM'de bulunan gizli kamera; tuş basım sayısını ya da aranan anahtar kelime ya da model sayısını denetleyen bilgisayar programı; sokağın karşısına kadar bir evin sıcaklığını ölçen alet; uyuşturucu kullanımını belirlemek için kullanılan saç analizi; alkol seviyesini belirlemek için kendi kendine yapılabilen testler; kablosuz ve hücresel telefon görüşmelerini tespit eden tarayıcı; bir DNA örneği; bir kişinin doğru söyleyip söylemediğinin beyin dalgalarının denetleyerek belirlenmesi; arayan kişinin numarasının telefonda gözükmesi..." (aktaran Güven, 2007: 75).

[27] Bakınız: Gary T. Marx (1985). "The Surveillance Society: The Threat of 1984-Style Techniques", *The Futurist*, syf. 21-26.

Gary T. Marx'a göre, dijital gözetim teknikleriyle elde edilen kişisel veri veya profil, o kişiyi "şüpheli" kategorisine sokuyorsa, kişi suçsuzluğunu ispat edene değin, sistem içerisinde "olası suçlu" olarak konumlandırılmaktadır. Bu durum da dijital gözetim olgusunun risk toplumu modelinde temel uygulama olduğuna bir kere daha işaret etmektedir.

Ekonomi politik kuramcı Oscar Gandy Jr. da, küresel kapitalizmin veri tabanlarını nasıl kullandığını incelediği *The Panoptik Sort: A Political Economy of Personal Information* (1965)[28] adlı çalışmasında, ağ yapılarında düzenli olarak kayıtlanan yedi kişisel veri türünü sıralamaktadır: Bireyin kimlik bilgileri, ekonomik bilgileri, sağlık ve sigorta bilgileri, sosyal güvenlik hizmetleri bilgileri, örneğin İnternet, telefon, kablo tv., güvenlik ve kargo/taşımacılık vb. çeşitli hizmetlerden yararlanma bilgileri, çeşitli tapu kadastro ve emlâk bilgileri, boş zaman ve eğlence bilgileri, tüketim alışkanlıkları bilgileri, istihdam bilgileri, eğitim bilgileri ve hukuki bilgileri (aktaran Whitaker, 1999: 126-127). Gandy'e göre böylece bu kişisel veriler üzerinden veri madenciliği[29] yapılmaktadır. Ancak Reg Whitaker *The End of Privacy* (1999) çalışmasında tüm bu bilgilerin gönüllü olarak yurttaş tarafından verildiğine dikkat çekmektedir. Görüleceği üzere bireyin kayıtlanması giderek gönüllük esası üzerinden gerçekleşmektedir.

Enformasyon teknolojileri ile güçlenen gözetim toplumu konusundaki en güncel çalışmaları yürüten, Lyon ise bireylerin artık yurttaş olmaktan öte, adeta "kodlanmış numaralar" olarak tanımlanmaya başladığına ve böylelikle sayısal bedenlere büründüğüne dikkat çekmektedir. Gözetim toplumunu buradan hareket ederek tanımlayan Lyon, bu toplum modelinde "kişisel yaşama ait her tür ayrıntının sürekli olarak büyük şirketler ile devlet dairelerine ait bilgisayarın veri tabanları içinde toplanması/saklanması/çağrılması ve işlenmesi"nin söz konusu olduğunu vurgulamaktadır (aktaran, Dolgun, 2008: 28).

Enformasyon teknolojilerinin gözetim toplumunun itici gücü haline geldiğini söyleyen bir diğer kuramcı da "süper panoptikon" kavramını geliştiren Mark Poster'dır. Poster'ın gözetim ve toplumsal denetim mekanizmalarının yeni biçimi olarak nitelendirdiği "süper panoptikon"unda hapishanelerden dışarı çıkarılan gözetim olgusu "duvarsız, penceresiz ve kulesiz" bir ortamda gerçekleştirilmektedir. İnsanlar gözetlendiklerinin ve siber mekânda bir yerlerde kayıtlı olduklarının farkında olmadıkları süper panoptikon'da, "siberuzayın dışında bir yerde bireylerin eğilimlerini denetleyen, kullanan ve satan başka bir gerçeklik" süregelmektedir (Güven, 2007: 92). Böyle bir sanal dünyada aslında bireyler bir ağ şebekesi içerisinde yer almaktadırlar.

[28] Oscar Gandy Jr. (1965) *The Panoptik Sort: A Political Economy of Personal Information*. Boulder: Colo.: Westview Press.

[29] Gandy, veri madenciliğini, veri tabanına kayıtlı kişisel bilgiler üzerinden anlamlı bilgiler çıkartan istatistiki işlem olarak tanımlar (2003:28). Veri madenciliğinin amacı, verileri tasnif etmek ve kategoriler oluşturmaktır. Veri madenciliği küresel kapitalizmde ticari işletmelerin günümüzde en yaygın olarak yararlandığı tüketici veya müşteri profili hakkında bilgi edinme uygulamalarındandır. Devlet tarafından veri madenciliği toplumda risklerin azaltılması için kullanılmaktadır. Ayrıca veri madenciliğinin yurttaşın eğilimlerinin saptamak için de kullanılması söz konusudur. Bu tür bir uygulama yurttaşlar arasında ayrımcılığı besleyebilir, demokratik temsil ve katılım alanını daraltabilir.

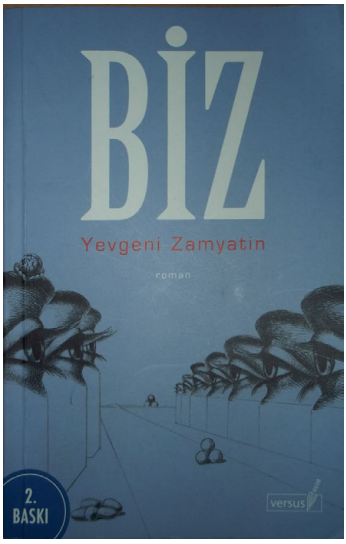
Panoptikonun siber mekâna taşındığı günümüz toplumunda Poster, "bedenlerimizin şebekeler, veritabanları, enformasyon koridorları içine çekildiğini" ileri sürerek, böylesi bir ortamda gözetlenmekten ya da kayıt altına alınmaktan kaçabilinecek bir sığınağın olmadığını söylemektedir (aktaran, Bauman, 2006: 60). Hatta öyle ki, bir süre sonra bu durum gönüllülük esasına dayanmaktadır. Süper panoptikonu panoptikondan ayıran temel unsur da budur: Kayıt altına alınanların "gözetimin birincil ve gönüllü unsuru" haline gelmeleri. Bu noktada Bauman'un yaptığı benzetmeyi aktaralım: Bauman, veritabanına dahil edilmiş olmanın eğlenceye giriş biletini almış olmakla aynı anlama geldiğini söylemektedir. Bireyler artık "kredi verilmeye değer"dir (Bauman, 2006: 61)[30].

Sonuç olarak



Farklılıkların yok edildiği ve modernliğin sürekliliğini mümkün kılan bir düzenin süregeldiği günümüzde belirsizlik, olasılık ve tehlike unsuru taşıyan her şey toplumların varlığını tehdit eder hale gelmiştir. Bu nedenle, devletler, yurttaşlarına ilişkin her türlü bilgiyi bilme, onları denetleme ve emniyet altına alma adına, giderek dijital gözetim tekniklerine başvurmaktadır. Toplum içerisinde günden güne artan güvensizlik ve belirsizliğin yarattığı tedirginlik, yurttaşların da iktidarın gözetimi altında yaşamayı kabul etmelerine ve hatta gözetim ağları içerisinde yaşamayı talep etmelerine neden olmaktadır. Dolayısıyla gözetim, modern devletin, hatta modernite öncesinin de her aşamasında iktidarın sıklıkla başvurduğu bir denetim mekanizması olarak işlemektedir. Günümüzde ise gözetim olgusu, bilgi ve iletişim teknolojileriyle, e-yönetişim, e-yurttaş, e-demokrasi gibi bir dizi kavramla konumlandırılan e-devlet olgusuyla gündeme gelmiş durumdadır. Aslında e-devletin temel hedefi, yurttaşlara demokratik bir katılım süreci sağlayarak, onları bütün süreçten haberdar etmek ve uygulamalara katılmalarını sağlamaktır. Ancak burada göz ardı edilen iki temel unsur bulunmaktadır: Bunlardan bir tanesi dijital uçurum, diğeri asimetrik iletişimdir. Dijital uçurumla kastedilen, insanların bu yeni iletişim teknolojilerine erişimindeki çeşitli eşitsizlik ilişkileridir. Bu da aslında enformasyon zengini ve enformasyon yoksulu olarak kavramsallaştırılan toplumun iki ayrı parçasına işaret etmektedir. Türkiye'de enformasyon

[30]Panoptikon ve veritabanı ayrımı için bakınız: Zygmunt Bauman (2006). *Küreselleşme*, Çev. Abdullah Yılmaz, İstanbul: Ayrıntı Yayınları, syf. 61.



Yevgeni Zamyatin'in Biz romanı

yoksulu olanlar kadınlar, yoksullar, kırsal yerleşim alanlarında ve ekonomik olarak gelişmemiş bölgelerde yaşayanlar, eğitim düzeyi düşük olanlar ile yaşlanan nüfustur[31]. Asimetrik iletişimde de, kişiler özneleştirilmekten koparılarak nesne haline getirilmekte ve sürece çok da fazla katıl(a)mamaktadırlar.

Bugün artık elektronik devletin e-gözetiminden/dijital gözetimden bahsedilmektedir. Daha önce bahsettiğimiz üzere Lyon, artık yurttaşların kodlanarak, kodlanmış numaralarla konumlandırılarak tanımlandığını söylemektedir. Aslında burada Lyon, Zamyatin'in romanındaki "biz"lere gönderme yapmaktadır. Kişisel yaşama ait her türlü ayrıntı artık şirketlerle devlet dairelerine ait bilgisayarlardaki veritabanlarında kayıt altına alınmaktadır. Buradaki veriler toplanıp depolanarak işlenilmekte ve çoğaltılarak istenildiği zaman bütün veriler birbirleriyle

[31]Bu konuda TUİK'in 2011 yılı Hane Halkı Bilişim Teknolojileri Kullanım Araştırması bulgularına göre, İnternet erişim imkânı olan hane oranı kentsel yerlerde %51,0 iken, kırsal yerlerde %22,7'dir. İBBS Düzey-1'e göre %56,9 ile TR1-İstanbul, %56,7 ile TR4-Doğu Marmara, %49,2 ile TR7-Orta Anadolu, %48,0 ile TR5-Batı Anadolu ve %43,4 ile TR2-Batı Marmara bölgelerinde İnternet erişim imkanı olan hane oranı Türkiye ortalamasının üzerindedir. Genişbant bağlantı ile İnternet erişim imkânı kentsel yerlerdeki hanelerde %47,5 iken, kırsal yerlerde %18,6'dır. İBBS Düzey-1'e göre genişbant bağlantı ile İnternet erişim imkânının en yüksek olduğu bölge %56,1 ile TR1-İstanbul, en düşük olduğu bölge ise %20,0 ile TRC-Güneydoğu Anadolu bölgesidir. Bilgisayar ve İnternet kullanım oranları 16-74 yaş grubundaki erkeklerde %56,1 ve %54,9 iken, kadınlarda %36,9 ve %35,3'tür. Bilgisayar ve İnternet kullanım oranlarının en yüksek olduğu yaş grubu 16-24 yaş grubudur. Bu oranlar tüm yaş gruplarında erkeklerde daha yüksektir. Bilgisayar ve İnternet kullanımı kentsel yerlerde %54,7 ve %53,2, kırsal yerlerde ise %26,9 ve %25,7'dir. İBBS Düzey-1'e göre bilgisayar ve Internet kullanımının en yüksek olduğu bölge %57,2 ve %56,5 ile TR1-İstanbul bölgesidir. Bunu %53,3 bilgisayar ve %51,7 İnternet kullanım oranı ile TR4-Doğu Marmara bölgesi takip etmektedir. Tüm bu bulgular Türkiye'deki mevcut cinsiyete, yaşa, yerleşim yerine ve ekonomik duruma temelli dijital uçurum olgusuna açık bir şekilde işaret etmektedir. Ayrıntılı bilgi için bakınız: http://www.tuik.gov.tr/PreHaberBultenleri.do?id=8572, (Erişim tarihi: 26 Şubat 2012).

eşleştirilerek, gözetim mekanizması için bir araç haline getirilmektedir. Polis kameralarından, kredi kartlarına kadar farklı birçok araçla iktidarın gözetim ve denetim mekanizmaları her geçen gün daha da güçlenmektedir. Sonuç olarak, özel alandan kamusal alana değin bireyin günlük yaşam etkinlikleri, elektronik gözler tarafından izlenilir hale gelmektedir. İleri enformasyon teknolojileri aracılığıyla kişisel bilgiler arşivinin oluşturulmasının daha sistemli bir hale gelmesiyle gözetim ve denetim mekanizmaları da kolay gerçekleşmektedir. Bu mekanizmalar, insanların gündelik yaşamlarını denetim altına almakta ve buna bağlı olarak insanların kendilerine dahi yabancılaşmalarına neden olmaktadır. Bu da denetim mekanizmalarının toplumsal yaşama dayatılmasıyla birlikte iktidarın tüm alanlarda yeniden üretilmesini beraberinde getirmektedir (Çoban, 2008: 112).

Buraya kadar anlatılanlardan görülmektedir ki, disiplin toplumlarından denetim toplumlarına geçilmesiyle birlikte, yurttaşların konumlandırılma politikaları da değişmiştir. Denetim toplumlarında yurttaşları kodlama, şifreleme ve sayısallaştırma oldukça önemli bir role sahiptir. Tıpkı Zamyatin'in Biz romanında olduğu gibi, e-devlette de yurttaşların sayılardan ve kodlardan ibaret olduğunu görülmektedir. Yurttaş olmak, artık, veritabanına dahil olmak ve aynı zamanda bir sayı olarak var olmak anlamına gelmektedir. Devlet, bireyleri kayıt altına almak için çaba sarf etmemekte, bireyler sistem içerisinde varolabilmek için kendilerinin gönüllü olarak kayıt altına alınması istemektedir. Burada devletin yurttaşına yönelik olarak ürettiği en güçlü söylem, bu kayıtlamanın verimli, hızlı bir bilgi akışını sağladığı; toplumsal yaşamın böylece güvenli ve şeffaf bir temel üzerine kurulu olduğudur. Ancak toplumsal, ekonomik adaletsizliklerin yaşamın her alanına yayıldığı bir ortamda, şeffaflık, güvenlik, yenilik, katılımcılık gibi ilkeleri bir arada barındıran bir kamusal alandan söz etmenin halihazırda mümkün olmadığı da açık bir şekilde görülmektedir. Üstelik, Türkiye bağlamında devlet-yurttaş ilişkilerini düşünecek olursak, bu ilişkideki asimetri daha da görünür olmaktadır. Özellikle, 61. Hükümetin İçişleri Bakanı İdris Naim Şahin'in "mevzu bahis devletse, gerisi teferruattır" açıklaması anımsanacak olursa[32].

[32]Bakan Şahin, 5 Şubat 2012 tarihinde Edirne Ticaret ve Sanayi Odası'nda düzenlenen AKP Edirne Merkez İlçe Olağan Kongresi'nde yaptığı konuşmasında "özgürlük" sorununa da değinmiştir: "... Birilerine ne oluyor acaba? Sıkıntı nedir? Özgürlük... Hangi özgürlükten bahsediyorsun. O zaman tutuklanınca da şikayet etme. Özgürlük yoksa dışarda, farkı yok içerinin demek ki. Niye şikayet ediyorsun, demek ki var dışarda özgürlük... Tek inkar ettiğin şey, var olan özgürlükleri söylemeyi, kabul etmeyi inkar ediyorsun. Yaşadığın özgürlüğün varlığını söylemeye özgürlüğün yok çünkü kafan ipotekli, kalbin, düşüncen ipotekli. Onu söylemeye özgür değilsin. Var olan sonuna kadar yaşadığın özgürlükleri, 'var' diyecek özgürlüğün yok. Orada tutsaksın. Seni tutsak yapan, sana sanal, özgürlük yok dedirten o güçle de mücadele ediyoruz. Seni de, seni konuşturanı da yok ederek, seni de, senin yapını da, bölücüler ve uzantılarını da özgürleştirmeye çalışıyoruz. Yaptığımız iş bu. Çok derin, çok kapsamlı bir iş..." Bakan'ın özgürlüklere ilişkin algısının devlet-yurttaş ilişkisinde Türkiye'de yaşanan eşitsizliğe ve asimetriye açık bir örnek olduğu aşikârdır. http://www.hurriyet.com.tr/gundem/19851115.asp, (Erişim tarihi: 26 Şubat 2012).

II. Bölüm:

DİJİTAL GÖZETİM TEKNOLOJİLERİ VE UYGULAMALARI

Teknolojinin ilerlemesi, kişisel bilgilerin gizliliği ve güvenliği konusunda toplumsal ve etik birtakım sorunları da beraberinde getirmektedir. Günümüzde artık birçok kişi bilgisayar teknolojilerinde, özellikle İnternet üzerinden gelen saldırıların ve gözetimin farkındadır. Bu olgunun, en bilineni kişisel bilgilerin gizliliğinin ve güvenliğinin ihlal edildiği bilgisayar korsanlığı olarak tanımlanan, bilgi almak için bir sisteme izinsiz olarak girme işlemidir. Oysa sayısal ortamda gerçekleşen kişisel bilgilerin gizliliğinin ve güvenliğinin ihlali yalnızca bilgisayar korsanlığıyla sınırlı değildir. Dijital gözetim olgusu da kişisel bilgilerin gizliliğinin ve güvenliğinin ihlalinde potansiyel bir tehlike arz etmektedir. David Lyon, dijital gözetim alanlarını, amaçlarına ve neye hizmet ettiklerine göre sınıflandırarak, belli bir çerçeve oluşturmuştur. Bu çerçeve izleğinde, dijital gözetim alanlarını incelersek, kişisel bilgilerin gizliliği ve güvenliği konusunun önemi daha açık bir şekilde ortaya çıkabilecektir. Lyon dijital gözetim alanlarını şu şekilde tanımlamaktadır:

1. Askeri ve istihbarat alanları,
2. Devlet yönetimi, nüfus sayımı ve suç kontrolü alanları,
3. İş gözetimi ve denetimi alanları,
4. Tüketim ve tüketici yapılandırması alanları (2007).

Aslında bu alanların günümüzde birbirleriyle bağlantılı olduğu görülmektedir. Yapılan araştırmalar göstermiştir ki, esas amaçlanan "assemblage" adı verilen, bu alanlardaki bilgilerin bir araya toplanması işlemidir. Çalışmanın bu bölümünde bu alanlara dair dijital gözetim teknolojileri uygulamaları örneklerle birlikte açıklanmaktadır.

2.1. Askeri ve İstihbarat Alanları

Uzmanlar askerlik hizmeti öncesi ve sonrasında yapılan sağlık kontrollerinin artık Sağlık Bakanlığının ulusal sağlık sistemiyle beraber kullanılabileceğini belirtmektedir. Aslında böyle bir sistem İngiltere'de mevcuttur ve Türkiye'de de kullanıma geçmiş durumdadır[33]. İngiltere'deki durumu inceleyen uzmanlar bu hasta kayıtlarının ordu tarafından da kullanılma isteğinin olduğunu ve bunun da kolaylıkla yapılabileceğini belirtmektedir.

Yalnız ordu açısından değil, toplumun güvenliği açısından da dosttan düşmanın ayırtedilmesi için hem dışarıdaki hem de içerideki düşmanlar hakkında veri toplanması gerekmektedir. Askeri istihbarat eskiden fiziksel casusluk şeklinde

[33] "Sağlık-NET Nedir?", Sağlık Bakanlığı Sağlık-NET Portalı, http://www.sagliknet.saglik.gov.tr/portal_pages/notlogin/sagliknetnedir/sagliknetnedir.htm, (Erişim Tarihi: 31 Ocak 2012).

yapılırken, günümüzde teknolojinin gelişmesiyle artık İnternet üzerinden hem içerideki hem dışarıdaki şüphelilerin izlenmesi olanaklı hale gelmiştir. Örneğin 2000'li yılların başında FBI'ın kullandığı *Carnivore*[34] sistemi İnternet'te dolaşan milyonlarca e-posta mesajını kontrol edebilmekteydi. FBI'ın *Carnivore* sistemini kullanmasının amacı her seferinde İnternet servis sağlayıcıların (İSS) yönetimiyle iletişime geçmek yerine doğrudan İSS'lerin sisteminden bilgi almayı sağlamaktı. FBI'da müdür yardımcısı olan Donald Kerr, 2000 yılında Amerikan Kongresinde yaptığı konuşmada Carnivore yazılımının tıpkı İSS'lerin kullandığı ticari koklayıcı (*sniffer*) yazılımlar gibi çalıştığını, tek farkının FBI'ya yasal olarak hangi alanlarda dinlemede bulunacağını, hangi alanlarda bulunamayacağı konusunda ayrımlaştırma sağladığını belirtmektedir. Buna göre, örneğin mahkeme tek tip iletişimi (ör. e-posta) dinleme hakkı verebilir, ancak diğer iletişim çeşitlerini (ör. çevrimiçi alışveriş) bu hakkın dışında tutabilmektedir. Buna göre *Carnivore* yazılımı, izlemeye alınan kişinin gönderdiği ve ona gelen e-postaları izleyebilmektedir[35]. Yapılan açıklamalara göre FBI bu teknolojiyi 1998 ve 2000 yılları arasında 25 kez kullanmıştır. 2002 yılında beş, 2003 yılında sekiz kez İnternet dinlemesi gerçekleştirdiğini ve bunların hiçbirinde *Carnivore* ya da daha sonraki verilen adıyla DCS-1000 yazılımının kullanılmadığı belirtilmiştir. Bu yazılım için FBI ne kadar para harcadığını belirtmese de yazılım endüstrisindeki uzmanlar büyük olasılıkla 6-15 milyon dolar arasında bir para harcandığını iddia etmektedir. 2005 yılında yapılan açıklamada FBI sözcüsü Paul Bresson, e-posta içerikleri ve İnternet izlemesinde daha ucuz olmasından dolayı ticari izleme yazılımlarına geçtiklerini belirtmiştir[36].

Burada ülkelerin dijital gözetim için ne kadar kaynak ayırdıklarının genel olarak bilinmediğinin altını çizelim. İngiltere'de kurulmuş olan kâr amacı gütmeyen bir şirket olan Privacy International (*Uluslararası Özel Hayatın Korunumu*)[37] Kurumu'nun bu nedenle "Elektronik Gözetim: Kim Kimdir"[38] çalışmasında tüm ülkelerin vatandaşlarını kendi hükümetlerine "hangi elektronik gözetim ekipmanına ne kadar para harcadıklarını" sormaya çağırdıklarını belirtelim[39].

Privacy International Kurumu dünya çapında özel yaşamın korunması hakkının savunulması için çalışan, özel yaşamın hükümetler ve şirketler tarafından gözetlenmesine ve başka şekillerde müdahaleye uğramasına karşı mücadele eden bir kuruluştur. Nitekim bu kuruluş "Elektronik Gözetim: Kim Kimdir?" çalışmasında dijital gözetim olgusunun ticarileşmesine de dikkat çekmektedir. On

[34] Carnivore İngilizce'de etobur demektir.

[35] *Statement for the Record of Donald M. Kerr, Assistant Director Laboratory Division Federal Bureau of Investigation, on Internet and Data Interception Capabilities Developed by FBI*, 24 Temmuz 2000, http://web.archive.org/web/20010308191403/http://www.fbi.gov/pressrm/congress/congress00/kerr072400.htm, (Erişim Tarihi: 15 Temmuz 2011).

[36] "FBI Ditches Carnivore Surveillance System", *Fox News*, 18 Ocak 2005, http://www.foxnews.com/story/0,2933,144809,00.html, (Erişim Tarihi: 15 Temmuz 2011).

[37] Bakınız: http://www.privacyinternational.org

[38] "*Who's Who*", Privacy International, https://www.privacyinternational.org/big-brother-incorporated/countries, (Erişim Tarihi: 1 Mart 2012)

[39] Günindi, E., "Elektronik Gözetleme – Büyük Biraderin şirketleşmesi", *Sendika.org*, 22 Şubat 2012, http://www.sendika.org/yazi.php?yazi_no=43118, (Erişim Tarihi: 1 Mart 2012).

yıl öncesine kadar çok büyük olmayan gözetim piyasasının günümüzde 5 milyar dolar dolaylarında olduğu tahmin edilmektedir. Söz konusu bu çalışmasında kuruluş, piyasada hangi firmaların olduğunu ve hangi hükümetlerin bu piyasanın alıcıları olduğunu açığa çıkartmayı amaçlamaktadır. İşte bu büyüyen piyasayla artık devletler yazılımları kendileri bizzatihi geliştirmek yerine, ticari yazılımlara geçmektedir.

Türkiye'de devlet, ne tür bir dinleme yaptığını tam olarak açıklamasa da[40], bu konuyla ilgili yapılan haberlerde devletin telefon ve telsiz dinlemelerinin dışında İnternet hareketlerini de yakından izleyebilecek teknolojiye sahip olduğu yazılmaktadır[41]. Hükümet bu konuda hangi tür teknolojiler kullandığı bilgisini vermese de, özellikle İnternet'te filtreleme ve gözetim sistemlerinin kurulması konusundaki başlattığı projeyle, Türkiye'de de Derin Paket İncelemesi (*Deep Packet Inspection, DPI*) teknolojisinin kullanıldığı şeklindeki şüpheleri pekiştirmektedir[42]. Bu filtreleme projesi Bilgi Teknolojileri Kurumu'nun (BTK) 22 Şubat 2011 tarihinde yayınladığı "Güvenli İnternet" adı altındaki yönetmelikle, İnternet sansürünü, denetimini ve gözetimini genelleştirerek 22 Kasım 2011 tarihinde uygulamaya başladığı devlet eliyle merkezi bir filtre uygulamasıdır. Buna göre sistem, bir yandan tüm İnternet kullanıcılarını fişlerken; diğer yandan DNS, Proxy gibi İnternet için vazgeçilmez teknolojileri de engelleyebilmektedir[43]. Özgür Uçkan'a göre Türkiye bu uygulamayla Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) bölgesindeki 56 devlet içerisinde, İnternet'te devlet eliyle merkezi ve zorunlu filtre uygulayan ilk ve tek ülke konumundadır[44]. Her ne kadar 22 Kasım 2011 tarihinde uygulamaya konan bu sistemde "aile" ve "çocuk" profili ile "standart" profil adı altında sözde seçiş olanakları mevcutsa da, aile ve çocuk profili seçişlerinde devlet eliyle hazırlanan filtreler, İnternet erişim kısıtlaması halen söz konusudur. Özellikle bu

[40] Türkiye'de ilk kez Faruk Bildirici gizli telefon dinlemelerinin tarihini ortaya koyduğu *Gizli Kulaklar Ülkesi* adlı çalışmasında, askeri ve istihbarat amaçlı dinlemeler dışında siyasi liderlerin, siyasetçilerin ve basın mensuplarının da çeşitli nedenlerle dinlemesi olgusuna kapsamlı bir şekilde dikkat çekmiştir. Gizli ve yasal olmayan bir şekilde kişilerin özel yaşamlarının dinlenmesi olgusu günümüzde dijital gözetim olgusuna dönüşmüş durumdadır. Bildirici çalışmasının sonunda, bu tür gözetim tekniklerinin özel yaşamın gizliliğini ihlal ettiğine dikkat çekmekte ve Türkiye'de yurttaşların "...bu ve benzer uygulamalara karşı haklarını arama yolları 'gerçekten' açık tutulmalıdır" (1998:327) önerisinde bulunmaktadır. Bu önerinin bugün de geçerliliğini koruduğunun burada altını çizme gereğini duymaktayız. Bakınız: Faruk Bildirici (1998). *Gizli Kulaklar Ülkesi*. İstanbul: İletişim.

[41] "Kandil internetten de vurulacak", *Radikal Gazetesi*, 19 Ağustos 2011, http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetayV3&ArticleID=1060531&Date=19.08.2011&CategoryID=77, (Erişim Tarihi: 31 Ocak 2012).

[42] Kırlıdoğ, M., Uçkan, Ö., Fidaner, I.B., "Derin Paket İzleme: Mahremiyet ve İletişim Hakları İhlalleri", *XVI. Türkiye'de İnternet Konferansı*, 2011. İzmir.

[43] Uçkan, Ö., *22 Ağustos: Türkiye internetinin kara deliği*, 24 Temmuz 2011, http://www.gennaration.com.tr/yazarlar/22-agustos-turkiye-internetinin-kara-deligi/, (Erişim Tarihi: 1 Mart 2012).

[44] *Freedom of Expression on the Internet*, Avrupa Güvenlik ve İşbirliği Teşkilatı, http://www.osce.org/fom/80723, (Erişim Tarihi: 1 Mart 2012). Bu konuda ayrıca bakınız: *Evrensel Kültür*, Ağustos 2011, sayı: 236, "Perdesiz İnternet, Özgür İletişim" özel dosyası.

filtreler VPN[45], Tor[46] ve BitTorrent[47] uygulamalarına erişimi engellemektedir.

DPI teknolojisinin mantığı aslında basittir. İnternet'te bir web sayfasına bağlandığınızda aslında sizin bilgisayarınızla, bağlandığınız web sitesinin bulunduğu sunucu bilgisayar arasında yoğun IP paketleri şeklinde bir veri alışverişi olur. Bu veri paketleri bir bilgisayardan diğerine gidip bir araya gelmeden önce, gitmeleri gereken en doğru yoldan gitmeleri için, yol boyunca içerilerinde bulundurdukları paket başlık kısmı bilgilerini (zarfın üzerindeki adres bilgileri gibi düşünebilirsiniz) okuyacak birçok yönlendirici ve anahtarlayıcı cihazdan geçerler. DPİ ekipmanları tam da bu işlem sırasında yönlendirici ve anahtarlayıcı cihazların okuma fonksiyonunu taklit ederek, eşanlı olarak paketlerin içerisine bakabilmektedirler[48].

Bir başka uygulamaysa Amerikan Savunma Bakanlığı'nın bir teknoloji birimi olan DARPA (The Defense Advanced Research Projects Agency - *ABD Savunma Bakanlığı İleri Araştırma Projeleri Ajansı*) Biriminin 14 Temmuz 2011 tarihinde "Stratejik İletişimde Sosyal Medya" (SMISC - *Social Media in Strategic Communication*) programıdır. Bu sayede birim, artık sosyal ağlarda yürütülen propagandaları açığa çıkarabileceğini açıklamıştır. Bu program yardımıyla ordu bir yandan sosyal medyada ne olduğunu gerçek zamanlı olarak öğrenebilecek, bir yandan da kendi propagandasını yapabilecektir. DARPA'nın açıklamasına göre SMISC algoritması sosyal medyada "yeni anlayışların, fikirlerin nasıl oluştuğu, geliştiği ve yayıldığı"nı bulup izlemeye alabilecektir[49].

Öte yandan ABD yönetimi Utah Çölü'nde Ulusal Güvenlik Ajansı'na (NSA) bağlı dünyanın en büyük telekulak merkezini kuruyor[50]. Yapılan yorumlarda bu merkez dünyadaki tüm telefon konuşmalarını, bütün İnternet trafiğini, gizli yazışmaları anlık olarak yakalanıp depolanabilecek. 2013 yılının Eylül ayında hizmete girmesi planlanan merkez 2 milyar dolara mal olacağı söyleniyor[51].

---

[45]VPN (Virtual Private Network - Sanal Özel Ağ) ağlara güvenli bir şekilde uzaktan erişimde kullanılan bir teknolojidir. Sanal bir ağ uzantısı yarattığından uzaktan bağlanan makine konuk gibi değil, ağa fiziksel olarak bağlıymış gibi görünür. Günümüzde firma ve kurumlar tarafından yaygın olarak kullanılan VPN, çalışanların nerede olursa olsun güvenli bir şekilde kurumlarının bilgisayar ağlarına bağlanmalarını sağlar.

[46]Tor (The Onion Router - Soğan Yönlendiricisi) kullanıcının İnternet kullanımında anonimliğini sağlayan bir sistemdir. Tor istemci yazılımı İnternet trafiğini dünyanın dört bir yanındaki gönüllü Tor sunucuları üzerinden geçirerek kullanıcının konumu ve kullanım bilgilerini ağı gözetleyenler ve trafik analizi yapanlardan saklar. Tor sayesinde İnternet etkinliklerini (hangi web sitelerine girildiği, çevirimiçi mesajlaşma vb.) izlemek zorlaşır. Amacı kullanıcıların İnternet kullanımında kişisel özgürlüklerini ve kişisel verilerini korumaktır.

[47]BitTorrent İnternet üzerinden dosya paylaşım yazılımına ve aynı tekniği kullanan dosya takas sistemine verilen isimdir. Diğer eşten eşe paylaşım programlarından farkı; sabit olmayan bağımsız sunucu tanımlama dosyaları sayesinde sabit bir sunucuya ihtiyaç olmaksızın paylaşıma devam etmesidir.

[48]Conti, J.P., "Is Seeing Deceiving?", *Engineering and Technology Magazine*, Nisan 2011 (s.70), Volume 6, Issue 3.

[49]Rawnsley, A., Pentagon Wants a Social Media Propaganda Machine, *Wired Magazine*, 15 Temmuz 2001, http://www.wired.com/dangerroom/2011/07/darpa-wants-social-media-sensor-for-propaganda-ops/#more-51990, (Erişim Tarihi: 25 Temmuz 2011).

[50]Uğur Koçbaş, Takip Altındasınız, *OdaTV*, 20 Nisan 2012, http://www.odatv.com/n.php?n=takip-altindasiniz-2004121200, (Erişim tarihi: 22 Nisan 2012).

[51]James Bamford, The NSA Is Building the Country's Biggest Spy

Avrupa Parlamentosu da 17 Nisan 2012 günü onaylanan anlaşmaya göre AB'den ABD'ye PNR (Passenger Name Record) adı verilen uçan yolcuların verilerini ABD'li yetkililerle paylaşılmasına karar verdi[52]. Anlaşmaya göre ABD, Avrupalı yolcuların bilgilerini "aktif sistemde en fazla beş yıl saklayacak". Altı aydan sonra yolcuların isim ve bilgileri şifrelenerek gizli hale getirilecek. ABD verileri beş yıldan sonra bir beş yıl daha tutma hakkına sahip olacak ancak bunu aktif olmayan bir veri bankasında saklayacak. AB'nin ABD'yle paylaşacağı veriler arasında yolcunun uçuş rezervasyonu ve check-in sırasında verdiği isim, adres, telefon numarası, kredi kartı bilgileri ve dini inancına göre yaptığı yemek tercihi ve tıbbi yardım talepleri de bulunmaktadır.

Her ne kadar Avrupa Komisyonu'nun içişlerinden sorumlu üyesi Cecilia Malmström, anlaşmanın kişilik haklarını daha iyi koruduğunu söylese de bu anlaşmaya büyük bir tepki sözkonusudur. Örneğin Avrupa Parlamentosu'nun Yeşiller Milletvekili Jan Phillipp Albrecht, büyük birader gözetimini kabul ederek Avrupa Birliği yurttaşlarının kişisel özgürlükleri kenara atılmış olduğunu belirtmiştir[53]. Alman Sosyal Demokrat Partili Birgit Sippel ise anlaşma için "tüm vatandaşları genel şüphe altına yerleştiriyor ve kendi değerlerimizi savunmak yerini onları ABD adalet sistemine teslim ediyor" yorumunu yapmıştır.

İngiltere'deyse yasal olarak durum daha da vahimleşmektedir. İngiliz hükümeti, polis ve istihbarat servislerine İnternet'i izleme imkanı verecek yasa tasarası hazırlamaktadır. Bu yasayla, telefon görüşmelerinin, e-postaların, Facebook, Twitter ve Skype gibi sosyal medya ve iletişim kanallarının yakından takip edilmesi amaçlanmaktadır. Diğer yandan bu yasayla birlikte İnternet servis sağlayıcılarına, polis ve istihbarat servislerinin istemesi halinde yurttaşların ziyaret ettiği siteleri anında bildirme yükümlülüğü getirmektedir. İngiltere'deki sivil toplum kuruluşları, bu düzenlemeyle vatandaşların izlenmesinde İngiltere'yi İran ve Çin'le aynı seviyeye getireceğini vurgulamaktadır[54].

Öte yandan devletin kişileri gözetimi yalnızca İnternet'le sınırlı değildir. Aynı zamanda fiziksel olarak kamera aracılığıyla da kişileri izlemektedir. Teknolojinin ilerlemesiyle artık kameralar çok daha küçük ve taşınabilir olmuştur.

İngiltere'de kolluk kuvvetleri ve iç istihbarat teşkilatı olan MI5 ile ortak çalışan Ciddi Organize Suç Kurumu (SOCA - *Serious Organised Crime Agency*) 2010 yazında havadan gözlem yapan sistem sağlayıcı şirketlerinden başvurular istediğini

---

Center (Watch What You Say), *Wired Magazine*, 15 March 2012, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1, (Erişim tarihi: 22 Nisan 2012).

[52] ABD Yolcusu Kalmasın, Bilgileri Gitti Bile, *BiaNet - Bağımsız İletişim Ağı*, 20 Nisan 2012, http://www.bianet.org/bianet/dunya/137738-abd-yolcusu-kalmasin-bilgileri-gitti-bile, (Erişim tarihi: 21 Nisan 2012).

[53] Jennifer Baker, European Parliament agrees to send airline passenger data to US, *Computer World UK*, 19 Nisan 2012, http://www.computerworlduk.com/news/public-sector/3352378/european-parliament-agrees-to-send-airline-passenger-data-to-us/, (Erişim tarihi: 21 Nisan 2012).

[54] İngiliz istihbaratı her şeyi dinleyecek, *Radikal Gazetesi*, 2 Nisan 2012, http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetayV3&ArticleID=1083670&CategoryID=81, (Erişim Tarihi: 7 Nisan 2012).

açıklamıştır. Buna göre, üstünde video kamera, termal görüntüleme cihazı, radyasyon detektörü, cep telefonu bağlantısı bozan cihazların takılabileceği *mikrodron* adı verilen 60 metre yükseklikte uçan insansız cihazları kullanmayı planladıkları ortaya çıkmıştır[55].

2.2. Devlet Yönetimi, Nüfus Sayımı ve Suç Kontrolü Alanları

İlk zamanlardan beri devlet nüfus sayımı gibi vatandaşlarını sınıflandırmak için birtakım teknikler kullanmıştır. Örneğin Roma İmparatorluğu döneminde askerlik ve vergilendirme için nüfus sayımları yapılmıştır. Marksist bakış açısına göre, kapitalist toplumlarda devletin gözetim tekniklerini kullanmaları sınıf kontrolü amacıyla gerçekleştirilmektedir. Günümüzde genel nüfus içinde tehdit unsuru olarak görülenler (azınlıklar, farklı din ve mezhep sahipleri, göçmenler vb.) üzerinde özellikle bu tür denetim ve gözetim teknikleri yaygın olarak kullanılmaktadır. Örneğin 2010 yılında İngiltere'de 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 başlattığını açıklamıştır. Uzmanlara göreyse, kapalı devre kamera güvenlik sistemleri, otomatik plaka okuma ve yüz tanıma kameraları terörizm karşıtı bir amaçla yerleştirilmişti. Ancak polis kuvvetleri daha sonra bu kameraları sökmüştür. Bunun nedeni de bu nüfus kesimiyle kaybolan güvenin tekrar inşası olarak belirtilmiştir. Polis kuvvetleri suç ve terörle savaşmada bölge halkının güven ve desteğini kazanmanın kolluk kuvvetleri için en önemli şey olduğunu açıklamıştır[56]. 2002 yılında sadece İngiltere'de yaklaşık 4.2 milyon kapalı devre gözetim kamerası olduğu tahmin edilmektedir[57]. Buna göre her 14 İngiltere vatandaşına bir kamera düşmektedir ve bir kişi her gün 300'den fazla kamera tarafından kaydedilebilmektedir[58]. Türkiye'de ise, Türkiye Büyük Millet Meclisi'ndeki bir soru önergesine yanıt veren dönemin İçişleri Bakanı Beşir Atalay Kent Güvenlik Yönetim Sistemi Projesi kapsamında 2010 Nisan ayı itibariyle 55'i il ve 18'i ilçe merkezi olmak üzere toplam 73 yerleşim biriminde kurulan kamera sayısının 6 bin 454 olarak açıklamıştır. Buna göre Atalay, İstanbul'da bin 179 noktada, 4 bin 17 MOBESE[59] kamerası

[55] "Unmanned drones may be used in police surveillance", *The Guardian*, 24 Eylül 2010, http://www.guardian.co.uk/uk/2010/sep/24/police-unmanned-surveillance-drones, (Erişim Tarihi: 15 Temmuz 2011)

[56] "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-areas-surveillance, (Erişim Tarihi: 15 Temmuz 2011).

[57] McCahill, M. and Norris, C. 2002. *Urbaneye: CCTV in London*. Working Papers No: 6, http://www.urbaneye.net/results/ue_wp6.pdf, (Erişim Tarihi: 15 Temmuz 2011).

[58] "Britain is 'surveillance society'", *BBC News*, 2 Kasım 2006, http://news.bbc.co.uk/2/hi/uk_news/6108496.stm, (Erişim Tarihi: 15 Temmuz 2011).

[59] Mobese (Mobil Elektronik Sistem Entegrasyonu) güvenlik kameralarıyla oluşturulmuş bir kent izleme, denetim ve kontrol teknolojisini anlatır.

olduğunu belirtmiştir[60].

Teknoloji ilerledikçe bazı devletlerin yeni iletişim ortamlarını da kontrol altına almaya başladığı gözlemlenmiştir. Örneğin Çin Halk Cumhuriyeti (ÇHC), 2010 yılında yeni cep telefonu satınalan herkesten kimlik bilgisi istediğini açıklamıştır. Buna neden olarak da istenmeyen mesajların önüne geçmek olduğunu belirtmiştir. Ancak bu uygulamayı eleştirenler, bunun devlete vatandaşlarını izlemek için yeni bir araç olduğunu belirtmektedir. Hatta bu uygulama kısa süreliğine ülkeye gelen yabancılar için de geçerlidir. ÇHC tarafından yapılan açıklamadaysa bu uygulamayla spam, pornografik mesaj ve sahtekârlığının önlenmesinin amaçlandığı yer almaktadır. Hong-Kong'da bulunan Çin İnsan Hakları Savunucularından araştırma koordinatörü Wang Songlian'a göreyse bu uygulama yeni iletişim teknolojileri üstünde devlet kontrolünün sıkılaştırılmasıdır. Ona göre, bu yeni düzenleme Çin'de oturan vatandaşları çok etkilemeyecektir çünkü zaten telefonları oldukça sıkı bir şekilde dinlenmektedir. Ancak Wang'a göre bu düzenleme, zaten Twitter, Facebook ve YouTube gibi birçok web sitesine erişimin engellendiği Çin'de istihdam koşulları tartışması, hava kirliliği ve başka konularda artan çok sayıdaki spontane protestolarda yer alan sıradan insanların izlenmesini mümkün hale gelecektir. Şu anda Çin'de 800 milyonun üzerinde cep telefonunun yaklaşık 320 milyonu gerçek bir isimle kayıtlanmamış durumdadır. Bu numaraların 2013 yılına kadar kayıtlanması gerekmektedir, aksi taktirde kullanım dışı kalacağı belirtilmektedir[61]. Nitekim Türkiye'de de yurttaşların TC kimlik numarası telefon bankacılığından, internet alışverişi ve oyununa, kargo tesliminden GSM hattı alımına kadar her aşamada istenilmektedir[62].

Türkiye'deyse telefon dinlemeleri Milli İstihbarat Teşkilatı'nın verdiği bilgiye göre yargı kararı ve yasayla sınırlandırılmıştır[63]. Buna göre 2006 yılından bu yana mahkeme kararıyla polis, jandarma ve MİT tarafından yapılan tüm dinlemeler Telekomünikasyon İletişim Başkanlığı (TİB) tarafından denetlenmektedir. Ancak 14 Eylül 2011 tarihinde CHP Antalya Milletvekili Gürkut Acar Başbakan Recep Tayyip Erdoğan'ın yanıtlaması istemiyle yasadışı dinlemelere ilişkin bir soru önergesi vermiştir. Buna göre soru önergesinde, "İletişim özgürlüğünü yok eden yasadışı telefon ve ortam dinlemeleri ile elde edilen kayıtların yayınlanması olayları, iktidarınız döneminde ciddi bir şekilde artmış olmasına karşın, önlem konusunda hiçbir adım atılmadığı"nı vurgulamıştır[64, 65]. Daha önceden de 2009

[60] "MOBESE'li kent sayısı artıyor", *Cumhuriyet Gazetesi*, 11 Ağustos 2010, http://www.cumhuriyet.com.tr/?im=yhs&hn=164932, (Erişim Tarihi: 31 Ocak 2012).

[61] "China demands ID from all buyers of mobile phone numbers", Associated Press, Pekin, 1 Eylül 2010, http://www.guardian.co.uk/world/2010/sep/01/china-mobile-phone-number-identity, (Erişim Tarihi: 15 Temmuz 2011).

[62] TC numarası ile gelen tehlike, Milliyet Gazetesi, 25 Ocak 2012, http://gundem.milliyet.com.tr/tc-numarasi-ile-gelen-tehlike/gundem/gundemdetay/25.01.2012/1493514/default.htm, (Erişim tarihi: 25 Mart 2012).

[63] "Merak edilenler", Milli İstihbarat Teşkilatı Web sitesi, http://www.mit.gov.tr/me_diger.html, (Erişim Tarihi: 31 Ocak 2012).

[64] "CHP'li Acar Başbakan Erdoğan'a dinlemeleri sordu", *Milliyet Gazetesi*, 15 Eylül 2011, http://siyaset.milliyet.com.tr/chp-li-acar-basbakan-erdogan-a-dinlemeleri-sordu/siyaset/siyasetdetay/15.09.2011/1438856/default.htm, (Erişim Tarihi: 31 Ocak 2012).

[65] "Yazılı Soru Önergesi Bilgileri", Türkiye Büyük Millet Meclisi web sitesi

yılında Demokratik Toplum Partisi (DTP) Diyarbakır milletvekili ve Demokratik Sol Parti (DSP) İstanbul Milletvekili Süleyman Yağız, Başbakan Recep Tayyip Erdoğan'ın yanıtlaması istemiyle telefon ve ortam dinlemesine dair uygulamalar konusunda çeşitli sorular yöneltmiştir[66]. Ancak daha önce Başbakan Erdoğan bu konuda telefon dinlemelerinin mahkeme kararıyla yapıldığını belirtmiş, "Benim de dinlendiğim ortaya çıktı. Yasadışı dinleme yakıştırması çok çirkin" açıklamasını yapmıştır[67].

Ancak telefon dinlemesi özellikle son yıllarda Türkiye'de gazetecilere yönelik sürmekte olan davalarla yaygınlaşan, dava delillerinin büyük bir kısmının sağlandığı ve hukuken tartışmalı durumlara yol açtığı belirtilen sıradan ve yaygın bir uygulama haline gelmiş bulunmaktadır. Örnek olarak Odatv iddianamesinde[68] gazeteci Nedim Şener'in siyasetçi, bürokrat, gazeteci ve işadamları ile yaptığı, herhangi bir itham ya da atıfta bulunulmayan 271 ayrı telefon görüşmesinin 550 sayfa tutan iddianamede ve delil klasörlerinde yer alması durumu gösterilebilir. Ya da 2009'dan itibaren telefonları dinlenme süresi iki kez üç ay ve üç kez de bir aylığına uzatılan Soner Yalçın için Ocak 2011'de tekrar telefon dinleme talebinde bulunulması durumu verilebilir. Bunun üzerine 10. Ağır Ceza Mahkemesi, iki gün sonra Yalçın'ın telefonlarının üç ay süreyle dinlenmesine karar vermiştir. Ancak daha önce de Yalçın'ın telefonunun dinlenmesinden ötürü üç ay dinleme kararı alınması hukuksuz olduğundan, 14. Ağır Ceza Mahkemesi tarafından bu karar geçersiz ilan edilmiştir. Bu nedenle normal koşullarda 2 Şubat tarihinden itibaren bir aylık dinleme başlatabilecek olan söz konusu mahkeme dinlemeyi 19 Şubat tarihinde başlatmış gibi göstermiştir[69].

Telefon dinlemeleri konusunda bir başka örnekse İçişleri Bakanı İdris Naim Şahin'in TBMM'deki gensoru görüşmeleri sırasında BDP'li milletvekillerinin aralarında yaptıkları konuşmayı aktarması milletvekillerinin de dinlenip dinlenmediği sorusunu akla getirmiştir. Telekomünikasyon İletişim Başkanlığı (TİB) yetkililerine göre, bir milletvekilinin telefonunun TİB üzerinden yasal olarak dinlenmesi imkansız. Hatta özel yetkili savcılar terörle mücadeleyi bahane edip başvuru yapsalar bile, milletvekilinin dokunulmazlığı olduğu için hiçbir hakim dinleme kararı veremez. Dolayısıyla İçişleri Bakanı Şahin'in kastettiği konuşma ya TİB dışındaki bir yöntemle dinlendiği ya da daha önce örnekleri olan, BDP'li vekillerin telefonları, başka 'kod isimlere' ait gibi gösterilerek mahkemeden karar çıkartılmış olabileceği belirtilmektedir. Nitekim iki yöntemin de suç ve ağır yaptırımları var-

---

http://www.tbmm.gov.tr/develop/owa/yazili_sozlu_soru_sd.onerge_bilgileri?kanunlar_sira_no=94764, (Erişim Tarihi: 31 Ocak 2012).

[66] "Başbakan'a DTP ve DSP'den İki Ayrı "Dinleme" Önergesi", *Bianet – Bağımsız İletişim Ağı*, 19 Kasım 2009, http://bianet.org/bianet/ifade-ozgurlugu/118386-basbakana-dtp-, (Erişim Tarihi: 1 Şubat 2012).

[67] "Erdoğan: Ben de dinlendim, telekulak çirkin", *NTVMSNBC*, 16 Kasım. 2009, http://www.ntvmsnbc.com/id/25021648/, (Erişim Tarihi: 1 Şubat 2012).

[68] ODATV iddianamesi, http://im.haberturk.com/images/others/2011/09/10/odatv_iddiname.doc, (Erişim Tarihi: 1 Şubat 2012).

[69] "Telefonlar MİT kriterlerine göre dinleniyorsa, ülke ihanetten geçilmiyor!", *Sol Portal*, 27 Ocak 2012, http://haber.sol.org.tr/devlet-ve-siyaset/telefonlar-mit-kriterlerine-gore-dinleniyorsa-ulke-ihanetten-gecilmiyor-haberi, (Erişim Tarihi: 1 Şubat 2012).

dır[70]. Daha sonra İçişleri Bakanlığı söylendiği gibi bir dinleme olmadığını, bunun 'bilinçli bir karalama ve yıpratma kampanyasının' ürünü olduğunu belirtmiştir[71]. Nitekim Türkiye'de yasadışı dinleme olayları ve tartışmaları sıklıkla gündeme gelmektedir.

Devlet gözetimi konusunda bir diğer örnekse, 1995 yılında Japonya'da Aum Shinrikyo adlı dinsel bir örgütlenmenin düzenlediği ve 12 kişinin ölümüyle sonuçlanan Tokyo metrosunda sarin gazı saldırısıyla ilgilidir. Bu olayda polis çalınan arabaları teşhis etmek için geliştirilen elektronik bir kamera sisteminden yararlanarak şüphelileri yakalamıştır. Japon sosyolog Kiyoshi Abe bu olayın hükümet ve polise gözetimin güçlendirilmesi için büyük bir fırsat sunduğunu belirtmektedir. Abe, devletin bu tür gözetim teknolojileri uygulamaları konusunda yurttaşların öğrenme hakkının yasalarla güvence altına alınması gereğini vurgulamaktadır. Bu yolla yurttaş devletin uygulamalarını öğrenip eleştirebilme hakkına sahip olacaktır. Ancak Mayıs 2002'de Japon Savunma Bakanlığı'nda çalışan bir kişinin, Bakanlığın etkinlikleri konusunda bilgi edinmek isteyen kişileri fişlediği ortaya çıkmıştır. Bu olay Japonya'da büyük bir skandala neden olmuştur. Burada Bakanlık ne tür kişilerin (ör. bağımsız gazeteci, savaş karşıtı organizasyon üyeleri, STK çalışanları vb.) bilgi edinme hakkına başvurduğu bilgilerini toplamıştır. Olay duyulduğunda Bakanlık bunun bir kurum çalışması olmadığını, kişisel bir çalışma olduğunu açıklasa da, Abe bu skandal gazetelerde duyulduğunda Bakanlığın hemen bu dosyayı yok etmeye çalıştığını belirtmektedir[72]. Bu da Abe'ye göre yurttaşın devlete olan güvenini zedelemiştir.

20. yüzyılın başlarından itibaren halk sağlığı birimleri bildirilmesi zorunlu hastalıklar üzerine veri toplamaya başlamıştır. Örneğin İngiltere'de çeşitli halk sağlığı etkinlikleri gelişmiştir. Bu etkinlikler belli bir hastalıkla savaşacak kaç erişkin erkek olduğunu bulmaya yönelikti. Zaman içerisinde özellikle genetik biliminin gelişmesi, gelecek tahminlerinden dolayı, kamu sağlığı konusunda birçok yeni gözetim sorununu da beraberinde getirmiştir. E-devlet uygulamasına geçen toplumlarda özellikle bu gibi bilgilerin kurumlar arasında paylaşılması giderek mümkün hale gelmiştir. Bu olguda, yeniden veri paylaşımı, verilerin güvenliği[73] ve gözetimin artan boyutları konusunda dikkatle düşünülmesini gerekli kılmaktadır. Nitekim BTK tarafından tüketici şikâyetlerinin hızlı ve etkili bir şekilde çözümü amacıyla 30 Ocak 2012 tarihinde hizmete açılan Online Şikâyet Bildirim Sistemi'ne ait "tuketici.btk.gov.tr" sayfasına 12 Şubat 2012 tarihinde Anonymous

[70]Deniz Zeyrek, Milletvekilini dinleme yasadışı, *Radikal Gazetesi*, 19 Nisan 2012, http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetayV3&ArticleID=1085386&CategoryID=78, (Erişim tarihi: 20 Nisan 2012)

[71]Tartışma yaratan konuşma için açıklama geldi, *Radikal Gazetesi*, 21 Nisan 2012, http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetayV3&ArticleID=1085636&CategoryID=78, (Erişim tarihi: 21 Nisan 2012)

[72]Abe, K., "Everyday Policing in Japan:Surveillance, Media, Government and Public Opion", *International Sociology*, 2004 19: 215.

[73]CHP Ankara Milletvekili Emine Ülker Tarhan tarafından, yanıtlanmak üzere Ulaştırma, Denizcilik Ve Haberleşme Bakanı Binali Yıldırım'a verilen Yazılı Soru Önergesi, *Türkiye Büyük Millet Meclisi web sitesi*, http://www.tbmm.gov.tr/develop/owa/yazili_sozlu_soru_sd.onerge_bilgileri?kanunlar_sira_no=101751, (Erişim Tarihi: 31 Ocak 2012).

grubu tarafından bir saldırı gerçekleştirilmiş olup, BTK'nın veri tabanında yer alan yüzlerce kişinin ad, soyad, ev adresi, ev ve iş telefonları, e-posta adresleri ve şifreleri ama en kötüsü vatandaşlık numaraları İnternet'te herkese açık şekilde yayımlanmıştır[74].

Washington Üniversitesi'nde teknoloji ve kamu politikaları profesörü Philip Bereano'ya göre, devletin, bireylerin kişisel verilerinin korunmasına karşı istilası belki de en iyi genetik test alanıyla tasvir edilebilir. Amerikan devleti tarafından desteklenen 'İnsan Genomu Projesi' (*Human Genome Project*) tarafından temsil edilen genetik gözetim ve izleme, en temel mahremiyet alanımıza ve özgür irademize tehdit oluşturmaktadır. Herkesin test edilip sınıflandırılması bilgisinin kötü bir şekilde kullanılması olasılığı, genetik ayrımcılığa karşı yasaların oluşturulmasını zorunlu kılmıştır[75].

Günümüzde 1500'den fazla genetik test çeşidi mevcuttur. Uzmanlar bu testlerin standart sağlık uygulamaları haline gelmesiyle sağlık kayıtlarında da genetik bilgilerin bulunabileceğini belirtmektedirler. Her ne kadar birçok biliminsanı bu teknolojiyi rutin olarak uygulamak için henüz erken olduğunu belirtse de, ABD'deki 23andMe ve İzlanda'daki deCODE Genetics gibi firmalar, sağlık laboratuvarı lisansına sahip olmadıkları halde, piyasada genom taraması pazarlamaya başlamışlardır. Uzmanlar on sene içerisinde bütün DNA'nın 1000 Amerikan dolarının altına taratılabileceğinden bahsetmektedir[76].

Sorun görüldüğü üzere yalnızca güvenlik sorunu değildir. Örneğin sağlık durumu iyi olmayanların sağlıklı olanlara göre, daha fazla para mı ödemesi gerekmektedir? Gazeteci Esther Dyson'a göre esas sorun sigorta endüstrisinin iş modelidir. Yakında birçok sigorta şirketi başvuranlara genetik test uygulamak isteyecektir ve belki de genetik risk taşıyanların başvuruları reddedilecektir. Bundan ötürü, 21 Mayıs 2008 tarihinde ABD Başkanı George W. Bush genetik bilginin ayrımcılık amacıyla kullanılmasına karşı yasayı (*GINA - Genetic Information Nondiscrimination Act*) imzalamıştır. Bu kanuna göre sigorta şirketlerinin ya da işverenlerin temel genetik testler sonucunda ayrımcılık yapması suç sayılmaktadır[77].

---

[74] Vatandaşlık numaranız internete düşmüş olabilir!, Yurt Gazetesi, 15 Şubat 2012, http://www.yurtgazetesi.com.tr/icerik/4302/vatandaslik-numaraniz-internete-dusmus-olabilir.html, (Erişim tarihi: 25 Mart 2012)

[75] Philip Bereano, Washington Public Health, Vol. 17 Fall 2000, s. 19-21, http://www.doh.wa.gov/sboh/Goals/Past/Genetics/2002/_02-25/docs/Tab05-BereanoArticle.pdf, (Erişim Tarihi: 15 Temmuz 2011).

[76] Dyson, E., "Reflection on Privacy 2.0", *Scientific American*, Eylül 2008.

[77] "GINA" The Genetic Information Nondiscrimination Act of 2008, Information for Researchers and Health Care Professionals, National Human Genome Research Institute and the Department of Health and Human Services (HHS), 6 Nisan 2009, http://www.genome.gov/Pages/PolicyEthics/GeneticDiscrimination/GINAInfoDoc.pdf (Erişim Tarihi: 20 Temmuz 2011).

2.3. İş Yeri Gözetimi ve Denetimi Alanları

İş ortamı gözetimi konusunda tarih boyunca çeşitli modeller sunulmuştur. Örneğin Jeremy Bentham panoptikon planını bir hapishane için geliştirmiştir[78]. Çalışmanın Birinci Bölümü'nde açıklandığı üzere Bentham aslında fikri kardeşi Samuel'in fabrikadaki işçilerin kontrol edilmesi planından almıştır. Bu modeli Bentham endüstrileşmenin çocukluk dönemi olan 18. yüzyılda yazmıştır.

Günümüzde çalışanın gözetlenmesi ve denetlenmesi teknikleri daha gelişmiş olsa bile, aslında mantık son birkaç yüzyıldakiyle aynıdır. Elbette Bentham'ın döneminde çalışanlar aynı zaman ve fiziksel ortamda bulunmaktaydılar. Ancak günümüzde artık esnek çalışma koşullarıyla çalışanların gözetlenmesi hem zaman hem de mekân olarak çok genişlemiştir. Bu nedenle çalışanların cep telefonu ve GPS'lerinden işverenleri tarafından İnternet üstünden nerede oldukları takip edilebilmektedir. Öte yandan çalışanlar hakkında firma işe başlamadan önce polis kayıtları (diğer bir deyişle adli sicilleri) ve hastalıkları konusunda bilgi toplamaktadır. Örneğin polis kaydı konusunda Amerika'da hizmet veren İnternet siteleri mevcuttur (Örneğin, http://www.comprehensivebackgroundcheck.info/). Lyon özellikle 11 Eylül saldırılarından sonra bu gibi sitelerin çok daha gözde olmaya başladığını belirtmektedir. Örneğin Backgrounds Online sitesi Kasım 2001'de aldıkları isteklerde yaklaşık yüzde 33'lük bir artış olduğunu belirtmektedir. Bu gözetim alanlarının genişlemesini Gary T. Marx "hareket eden her şeyin ölçülmesi" olarak belirtmektedir.

İş ortamının gözetlenmesi genel olarak kalite kontrolü, eksikliklerin ortaya çıkartılması, işe alma, çalışanların performansı, terfi ya da işyerindeki istismarların engellenmesi gibi konularda önem kazanmaktadır. Ancak bu gözetleme, çalışanların iş saati dışında kişisel alanlarının gözetlenmesini içerdiği ya da emek gücü ile işveren arasında eşit olmayan güç ilişkisi içerisinde emek gücünün daha da güçsüzleştirilmesi amacıyla kullanıldığı durumlarda büyük bir sorun yaratmaktadır.

İş yerinde elektronik gözetim uygulamaları arasında çalışanların,

- e-postalarının ve sohbetlerinin izlenmesi,
- telefonlarının dinlenmesi,
- iş yeri dışında bulunmaları durumunda küresel konumlama sistemi (GPS) ya da diğer teknolojilerle nerede bulunduklarının izlenmesi,
- Web'de hangi sayfalara girdiğinin izlenmesi,
- kapalı devre video sistemiyle işyerinde izlenmesi,
- klavyede hangi tuşlara bastığının izlenmesi,

[78] Bentham'ın panoptik modeli detaylı olarak Birinci Bölümde açıklanmıştır.

- biyometrik ve/veya RFID'li akıllı kartları kullanmasını zorunlu kılarak izlenmesi

gibi yöntemler kullanılmaktadır.

Bunun yanında kimi işyerleri uyuşturucu testi (kan, saç ya da idrar örneği alarak[79]) , genetik tarama[80] ve psikolojik test de yapmaktadır[81].

Uluslarası Çalışma Örgütü'nün (ILO) 1993 yılında işyerindeki yeni gözetim teknolojileri üzerine yayımladığı çalışmada[82]

- gözetim teknolojilerinin kullanılmasının temel insan haklarını ve itibarını ihlal etmekte olduğunu, bu konudaki gerekli özenin yerine getirilmemesinin yanı sıra yerel yasaların yarattığı boşluklardan yararlanıldığı,
- iş yerinde gerçekleştirilen gözetim alanının çalışanların özel yaşamını da izlemeye kadar genişlediği,
- gözetimin işveren ve işçi arasında ayrımı daha da beslediği,
- gözetimin çalışanlar arasında ayrımcılığa neden olduğunu ve çalışanların bu durumun farkına varmasının çok zor olduğu

belirtilmektedir.

ILO 1996 yılında yapılan toplantılarda, çalışanların kişisel bilgilerinin korunmasına ilişkin bir davranış kodu da yayımlamıştır[83, 84]. Bu davranış kodunda benimsenen kimi ilkeler şunlardır:

- Çalışanların özel yaşamına ilişkin bilgilerin koruma yolları geliştirilerek, kişisel bilgilerle ilgili bilgisayar kayıtları en aza indirgenmelidir.
- Çalışan ve temsilciler bilgi toplama sürecinden, bu sürecin kurallarından ve haklarından haberdar edilmelidir.

[79] Holland, P. (2003). "Case-Study. Drug Testing in the Australian Mining Industry", *Surveillance and Society*: 204–9.

[80] "Equality at work - Just a family medical history: genetic testing before getting a job?", *ILO Haber bülteni*, 9 Mayıs 2007, http://www.ilo.org/global/about-the-ilo/press-and-media-centre/news/lang–en/WCMS_082589 (Erişim Tarihi: 26 Temmuz 2011).

[81] "PHR2006-Privacy Topics-Workplace Privacy", Privacy International, 18 Aralik 2007, https://www.privacyinternational.org/article/phr2006-privacy-topics-workplace-privacy, (Erişim Tarihi: 26 Temmuz 2011).

[82] "Workers' privacy Part II: Monitoring and surveillance in the workplace", Conditions of work digest, Volume 12 Number 1 1993, Geneva, International Labour Office, http://www.ilo.org/public/libdoc/ilo/P/09921/09921(12).pdf, (Erişim Tarihi: 27 Temmuz 2011).

[83] Tekergül, M., *İşyerinde Elektronik Gözetim Uygulamaları*, Yüksek Lisans Tezi, Kadir Has Üniversitesi, Hukuk Anabilim Dalı, 2010.

[84] "Protection of workers' personal data", ILO Code of Practice, Geneva, International Labour Office, 1997, http://www.ilo.org/safework/normative/codes/lang–en/docName–WCMS_107797/index.htm, (Erişim Tarihi: 27 Temmuz 2011).

- Kişisel bilgileri, dosya veya bilgisayarlara işleyenler, düzenli olarak eğitilerek yaptıkları işin sorumluluk bilincinde olmaları sağlanmalıdır.
- Toplanan kişisel bilgilerle işçilerin istihdamında ve iş sırasında hukuka aykırı ayrımcılık yapılmamalıdır.
- İşverenler, çalışanlar ve onların temsilcileri, çalışanların özel yaşamına ilişkin bilgilerin korunması politikası geliştirmede işbirliği yapmalıdır.
- Toplanan kişisel bilgilere erişebilen işverenler ve işçi temsilcileri, bu hususta "gizlilik" ilkesine uymak zorundadır.
- Çalışanlar, kişilik haklarını ilgilendiren haklardan feragat edemezler.
- İşveren, işçinin cinsel yaşamı, siyasi, dini ve diğer inançları konusunda bilgi toplayamaz ve işçinin suça eğilimini belirleme amacına yönelik test yapamaz.
- Sağlık açısından, örneğin, önceden bir hastalık geçirip geçirmediğine yönelik sorular ancak, iş için önemli ise ve ulusal mevzuatta iş güvenliği ve işçi sağlığının gerektirdiği ölçüde sorulabilir.
- Yukarıda belirtilen ilkelere aykırı soru sorulursa, aday veya çalışan eksik cevap vermesi halinde işten çıkarılamaz veya disiplin cezası verilemez.
- Çalışanın madde bağımlılığı bulunup bulunmadığına ilişkin testler, ancak ulusal mevzuat kapsamında ve uluslararası standartlar dikkate alınarak uygulanabilecektir.
- İşçi hakkında toplanan bilgilere sadece yetkili olanlar erişebilir. Bu bilgiler, kural olarak üçüncü kişilere, çalışanın izni olmadan verilemez. Ancak cana kast ve sağlığı tehdit eden bir durum söz konusu ise, yasanın elverdiği ölçüde ve çalışma ilişkisinin yönlendirilmesi amacıyla üçüncü kişilere verilebilir. Ayrıca ulusal ceza mevzuatı gerektiriyorsa bu bilgilerin verilmesi mümkündür.

Bu metnin elbette uluslararası bir bağlayıcılığı yoktur ve işyeri gözetimi üzerine yasalar ülkeden ülkeye değişmektedir. Örneğin Avrupa ülkeleri bu metne daha yakın dururken, ABD'de durum çok daha farklıdır.

Örneğin 2007 yılında Amerikan İşletme Vakfı'nın (AMA-*American Management Association*) yayımladığı bir rapora göre[85] ABD'de işverenlerin bilgisayar izlemesi çeşitli şekillerde gerçekleşmektedir. Buna göre işverenlerin %66'sı çalışanların İnternet'te nereye bağlandıklarını izlemektedir, %45'i çalışanların bilgisayarlarında girdikleri içerikleri, bastığı tuşların kaydını ve klavye başında geçirdikleri zamanı izlemektedir, %43'ü çalışanların e-postalarını izlemektedir, %43'ü çalışanların bilgisayarlarındaki dosyaları saklayıp, gözden geçirmektedir,

[85] "The Latest on Workplace Monitoring and Surveillance", 13 Mart 2008, http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx, (Erişim Tarihi: 27 Temmuz 2011).

%12'si İnternet'teki bloglarda firma hakkında ne yazdığını kontrol etmektedir, %10'u sosyal ağları izlemektedir.

2.4. Tüketim ve Tüketici Yapılandırması Alanı

Kişisel bilgilerin ekonomik değer kazanması konusu üzerine Oscar Gandy Jr.'nin yazmış olduğu *The Panoptic Sort* kitabında tüketicilerin sınıflandırılması anlatılmaktadır. Buna göre şirketler ürünlerini daha iyi pazarlayabilmek için kullanıcıların kişisel bilgilerini toplayıp, onları belli özelliklerine göre sınıflandırmaktadır. Bunun yanında tüketici İnternet'te bir sayfaya girip bir alışveriş yaptığında kendisi hakkında bir iz bırakmaktadır. Ancak şirketler yalnız alışveriş sırasında kullanıcıların kişisel bilgilerini toplamakla kalmaz, aynı zamanda kullanıcıların hangi sitelere girdiklerini, sosyal ağlarda nelerden hoşlandıklarını, hangi konuları izlediklerini, e-postalarında hangi kelimelerin kullanıldığını takip ederek bu kullanıcılara göre pazarlama stratejileri geliştirmektedirler. Bu toplanan kullanıcı verilerini şirketler artık yalnız kendileri için kullanmakta, başka şirketlere de satmaktadırlar (Castells, 2001).

Computer Assisted Passenger Pre-Screening Sistemi (CAPPS-II) her hava yolu yolcusunu değişik sınıflara ayrılarak risk değerlendirmesinde bulunarak onlara not vermektedir. CAPPS ilk olarak 1996 yılında bagajlarda patlayıcı madde taraması sistemi olarak başlatılmıştır. İkinci nesil sistem artık hem tehlikeli şeyleri tarayabilmekte, hem de yolcular üzerinde devlet ve ticari kurumların veritabanlarını tarayarak veri-madenciliği algoritması sayesinde tehlikeli olanları ayırabilecek güçtedir[86].

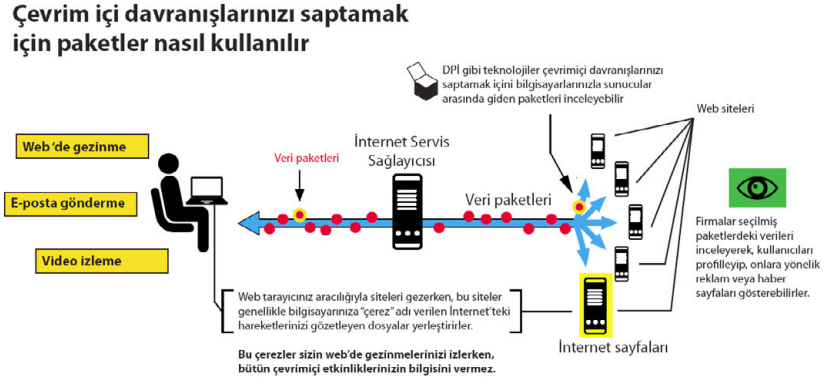
İnternet'te tüketici izlemesi ve profillenmesi konusunda kullanıcıların alışkanlıkları sayısal işaretleyicilerle sağlanmaktadır. Kullanıcı bilgilerini toplamak için web çerezleri, flash çerezleri ve web böcekleri genellikle en çok kullanılan yöntemlerdendir. Çerezler bir web sitesine girdiğinizde bilgisayarınızın sabit diskine yerleşen küçük metin dosyalarıdır. Bu çerez dosyalarında oturum bilgileri ve benzeri veriler saklanır. Bu çerezler yardımıyla web siteleri kullanıcıları yayımladıkları web sayfalarını daha verimli kullanmalarını sağlamaktadır. Örneğin çerezler yardımıyla kullanıcının her seferinde aynı web sayfasına bağlandığında kullanıcı adı ve şifresini girmesi gerekmemektedir. Bu bilgiler çerezlerin içerisinde saklanmaktadır. Ancak web teknolojisi ilerledikçe bilgisayarına yerleştiği kullanıcının web üzerinde dolaşma şekilleri ve web sayfalarında verdiği bilgileri toplamaktadırlar. Web çerezlerinin aksine Flash çerezleri görece kullanıcılar tarafından pek bilinmemektedirler. Bunlar aynı zamanda web tarayıcısının çerez kontrol ayarlarından kontrol edilememektedir. Kullanıcılar her ne kadar bilgisayarlarındaki çerezleri temizlediklerini düşünseler de aslında Flash çerezleri genellikle temizlenmemektedir[87].

[86] Passenger Profiling, *Electronic Privacy Information Center* http://epic.org/privacy/airtravel/profiling.html, (Erişim Tarihi: 10 Temmuz 2011).

[87] Singel, R., "You Deleted Your Cookies? Think Again", *Wired Magazine*, 10 Ağustos 2009, http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/, (Erişim Tarihi: 25 Temmuz 2011).

Web böcekleriyse genellikle web sayfası ya da e-postalarının içerisine kullanıcının göremeyeceği şekilde yerleştirilmektedir. Bunun sayesinde kullanıcının web sayfasını ya da e-postasını görüp görmediği kontrol edilmektedir. Bunlar aynı zamanda çerezleri ve indirilecek uygulamaların gönderilmesi için de kullanılmaktadır. Örneğin kullanıcı web tarayıcısında çerezlere izin vermiyorsa ya da düzenli olarak silse bile web böceklerine izin vermemesi genellikle zordur.

Kullanıcılar hakkındaki toplanan bilgiler genellikle; İnternet Protokolü (IP) adresi; görülen sayfalar; sayfalarda geçirilen zaman; görülen reklamlar; okunan makaleler; yapılan alışverişler; arama yapılan kelimeler ya da sitede girilen bilgiler; kullanılan dil ya da web tarayıcı bilgisi gibi kullanıcı bilgileri; kullanılan işletim sistemi; coğrafi olarak nereden bağlanıldığıdır. Daha fazla veri başka teknolojiler yardımıyla toplanabilmektedir. Örneğin Facebook, MySpace, LinkedIn gibi sosyal ağlarda kullanıcının isteyerek verdiği bilgiler sayesinde, veri madenciliği teknikleri kullanılarak bu toplanan veriler, amaçlar doğrultusunda belli sınıflandırmalara sokulmaktadır.



İnternet'te profilleme nasıl işliyor

Öte yandan İnternette ziyaret ettiğiniz tarayıcızdan bilgisayarınızda hangi fontların yüklendiğini öğrenilebilmektedir. Bunun yanında Adobe Reader, OppenOffice.org, Google Chrome ve Microsoft Silverlight gibi yüklenen kimi programları da öğrenmeleri mümkündür[88]. Hatta son dönemlerde ziyaret ettiğiniz kimi siteleri de öğrenebilmektedirler. Bir kullanıcı İnternet'te gezindiğinde arkasında bıraktığı izlerden web siteleri onun web tarayıcısını tanıyabilir hatta kimi uç durumlarda kullanıcıyı da tanıyabilir[89]. Web tarayıcınızın özellikleri (yüklenmiş olan programlar, fontlar vb.) onun web sitesi tarafından büyük ölçüde tanımasını sağlar[90].

[88] http://browserspy.dk/, (Son erişim tarihi: 8 Mart 2012)

[89] George Lawton, Browser Fingerprints Threaten Privacy, Computing Now, Nisan 2010, http://www.computer.org/portal/web/computingnow/archive/news057, (Erişim tarihi: 8 Mart 2012)

[90] Web tarayıcınızın ne kadar benzersiz olduğunu https://panopticlick.eff.org/ adresinden test edebilirsiniz.

Ancak kimi ülkelerde kullanıcıların bilgileri dışında izlenmesi yasalara aykırıdır. Örneğin İngiltere'de 26 Mayıs 2011'de yürürlüğe giren yeni yasayla kullanıcıların izni olmadan web sitelerinde çerez ya da benzeri aygıtların kullanılması yasaktır[91].

Kanada'da *Kişisel Veri Güvenliği Komisyonu* (*Privacy Commissioner of Canada*)[92] yaptığı araştırma sonucunda Google ve Facebook gibi firmaların kullanıcılar hakkında artan derecede veri topladığını ve kullanıcılarını bu toplanan verilerin ne için kullanılacağına dair düzgün bir şekilde bilgilendirmediğini kaydetmiştir[93]. Bu komisyonun yayımladığı raporda[94] birçok kişinin İnternet'te dolaşırken, sosyal ağları kullanırken ya da cep telefonu gibi taşınabilir cihazlarındaki Google Maps gibi coğrafi konum fonksiyonlarını kullanırken arkalarında bıraktıkları zengin veri yığınının farkında olmadığı belirtilmektedir. Bu raporda Google gibi firmaların politik eğilimlerden, müzik zevkine kadar kullanıcılar hakkında her bilgiyi topladığı ve bu toplanan verilerin pazarlama ya da reklam firmalarına satıldığı ve hatta aramalarda bunlara göre belki de kullanıcının ilgilenmeyeceği web sayfası bağlantı sonuçlarının sunulmakta olduğu belirtilmektedir. Örneğin bir kullanıcı Gmail e-posta hesabı gibi Google firmasının verdiği hizmetlerden birine girdiğinde, firma bu kullanıcının altı aylık İnternet geçmişini kaydetmekte ve bu bilgiyi kullanarak o kullanıcının en çok neler görmek isteyeceğini tahmin etmektedir. Google firmasına göre, bunun nedeni İnternet'te çok fazla bilginin olmasından dolayı kişiye özelleştirilmiş bilgilerin sunulmasıdır.

Örneğin Google'da iki ayrı kullanıcı aynı kelimeyi aradığında farklı sonuçlar elde edebilmektedir. Bu konuda Google firması, kullanıcıya özel ve gereksinime en uygun sonuçlar çıkardığını açıklamıştır. Google firması kullanıcıların dilerlerse geçmiş arama kayıtlarını *http://www.google.com/history/optout* adresinden silebileceklerini de belirtmektedir. Ancak Kanada hükümeti bu açıklamaları yeterli bulmamaktadır. Amazon.com'dan Apple'ın iTunes hizmetine kadar kullanıcıların izlendiğini belirtmişlerdir. Kişisel veri güvenliği komisyonu üyesi Jennifer Stoddart İnternet şirketlerinin kullanıcılara ait verileri nasıl topladıklarını ve bu toplanan verileri nasıl kullandıkları konusunda firmaların daha proaktif olmasını istemektedir.

Amerika'da bir başka gelişmeyse 11 Kasım 2011 tarihinde Cumhuriyetçi Parti'den ABD Temsilciler Meclisi üyesi Michael Rogers ve 111 destekçisi tarafından Siber İstihbarat Paylaşım ve Koruma Yasası (CISPA) adlı yasa tasarısı Beyaz Saray'a sunulmasıdır[95] . Yasa tasarısı ABD'de iş yapan şirketlere, İnternet

[91] "New rules on use of cookies to store and access your data", 26 Mayıs 2011, http://www.direct.gov.uk/en/NI1/Newsroom/DG_197239, (Erişim Tarihi: 23 Temmuz 2011).

[92] Bakınız: http://www.priv.gc.ca

[93] Pileici, V., "Privacy watchdog sets sights on Google - Report raises concerns about how Internet giants track, profile and target us", *The Montreal Gazette*, 19 Temmuz 2011, http://www.montrealgazette.com/technology/Privacy+watchdog+sets+sights+Google/5125124/story.html, (Erişim Tarihi: 19 Temmuz 2011).

[94] "Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing", Mayıs 2010, http://www.priv.gc.ca/resource/consultations/report_201105_e.cfm#toc5a, (Erişim Tarihi: 20 Temmuz 2011).

[95] Cyber Intelligence Sharing and Protection Act, *Wikipedia*, https://en.wikipedia.org/wiki/

kullanıcılarına izlendikleri konusunda bilgi bile vermeyerek, kişisel bilgileri yanında çevrimiçi etkinliklerinin tamamının bütün kayıtlarını toplayıp ABD hükümetine teslim etme yetkisi veriyor. Bunun için herhangi bir yasal izin, bir hukuki gerekçe ya da yasal sürece uygunluk gerekmemektedir. Bunun yanında devlete ve şirketlere özel hayatın gizliliğini ihlal veya başka yasadışı bir fiil gerekçesiyle aleyhlerinde dava açılmasından korunmaları için kapsamlı bir cezasızlık sağladığı da belirtilmektedir[96].

Bu yasa tasarısına göre herhangi bir şirket kendi hak ve mülkiyetlerini korumaya yönelik sibergüvenlik önlemleri alabilmektedir. Yani yasa kullanıcıların bütün e-postalarını ya da Facebook mesajları gibi bütün iletişimlerini şirketlerin izleyebilmesine olanak sağlamaktadır. Öte yandan Tor gibi anonimleştirici hizmetlerin kullanılması, ya da e-postalarınızın şifrelenmesi gibi uygulamalar da tehdit olarak görülmektedir bu yasa tasarısına göre. Bu yasa tasarısı İnternet kullanıcıları arasında o kadar büyük bir tepki yaratmıştır ki uluslararası birçok sivil toplum kuruluşu bu yasa tasarısına karşı kampanya başlatmıştır[97, 98, 99].

Tüketicinin izlenmesi ve profillenmesi konusunda tek ortam elbette İnternet değildir. 2010 yılından itibaren Yakın Alan İletişimi ya da diğer adıyla NFC (*Near Field Communication*) adı verilen yeni nesil kablosuz iletişim teknolojisi de gündelik yaşamda giderek yaygınlaşmaktadır. Bu teknolojiyle elektronik cihazlar arasında yakın mesafeli haberleşme sağlanmaktadır. Böylece kredi kartı ya da nakit para taşımak yerine yalnızca telefonunuzu bir markette ya da mağazada satış noktasına tutmanız yeterli olacaktır. Bu yeni teknolojiyle nasıl kimi pasaportlarda *Radyo Frekansı ile Tanımlama* (RFID) çipleri kullanılıyorsa, gelecekteki kimlik sistemlerinde de NFC çiplerin kullanılabileceğinden bahsedilmektedir.

NFC teknolojisi cep telefonlarında kullanılmaya başlanmıştır. Şu anda Google'ın yeni Android işletim sistemli cep telefonları NFC teknolojisini desteklemektedir ve firma bu pazara büyük ilgi duyduğunu göstermiştir[100]. Google NFC teknolojisi kullanarak mobil ödeme sistemi geliştirilmesi için MasterCard ve Citigroup firmalarıyla ortaklık kurduğunu açıklamıştır. Öte yandan yeni nesil iPhone'larda da NFC teknolojisi bulunacaktır. Microsoft, Amazon gibi firmalar da kendi ürünlerini NFC'ye uyumlu hale getirme konusunda çalışmalarını sürdürmektedir. Ancak burada sorulması gereken bir diğer soru daha vardır: buradan elde edilen gelir ortaklar (şebeke firması, cep telefonu üreticisi, satış yapanlar vs.) arasında

Cyber_Intelligence_Sharing_and_Protection_Act, (Erişim tarihi: 20 Nisan 2012).

[96] Cybersecurity Bill FAQ: The Disturbing Privacy Dangers in CISPA and How To Stop It, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it, (Erişim tarihi: 20 Nisan 2012).

[97] Boone, J., CISPA: The internet finds a new enemy, *GlobalPost*, 9 Nisan 2012, http://www.globalpost.com/dispatches/globalpost-blogs/the-grid/cispa-the-internet-finds-new-enemy-sopa, (Erişim tarihi: 20 Nisan 2012).

[98] Stop Cyber Spying, *Electronic Frontier Foundation*, https://cyberspying.eff.org/, (Erişim tarihi: 20 Nisan 2012).

[99] İnternet gizliliğinin sonu, *AVAAZ.org*, https://secure.avaaz.org/tr/stop_cispa_corporate_global/?cl=1744899201&v=13751, (Erişim tarihi: 20 Nisan 2012).

[100] Eaton, K., "Google's Eric Schmidt Reveals NFC Smartphone Plans: It's All About Advertising", 16 Şubat 2011, http://www.fastcompany.com/1728241/eric-schmidt-gives-away-googles-nfc-smartphone-plans-its-all-about-advertising, (Erişim Tarihi: 23 Temmuz 2011).

nasıl paylaşılacaktır[101]. Bu soru da veri eşleştirmesinin ekonomi politik yönüne işaret etmektedir.

Google firması bugün o kadar reklam odaklı düşünmektedir ki artık yalnızca İnternet üzerinden kullanıcıların arama alışkanlıklarını, e-posta hesap bilgilerini, ajandalarını ve coğrafi konumlarını toplamamaktadır. Aynı zamanda NFC destekli Android telefonları sayesinde kullanıcılarının nereden ve ne zaman alışveriş yaptığı ve ne aldığı konusunda da bilgi sahibi olabilmektedir. Bu nedenle 2010 yılının Aralık ayında Amerikan Federal Ticaret Komisyonu NFC teknolojisi kullanan firmaların tüketicinin kişisel bilgilerinin korunmasına yönelik uyması gereken bir rapor önermiştir[102]. Bu rapor üç temel nokta üzerine odaklanmaktadır: Tasarım olarak kişisel verilerin korunması, basit seçenekler ve daha fazla şeffaflık. Buna göre firmaların tüketicilere kişisel verileri üzerinde basit ve gerçek bir kontrol sağlaması gerekmektedir. Yani tüketiciler kişisel verilerini verirken, bu verilerin pazarlama amaçlı kullanılmaması ve bunun yalnızca anlaşma metninde bulunmaması gerekmektedir. Özetle firmalar kullanıcılara gerçekten haklarında topladıkları verilere ilişkin ne olacağı bilgisini sağlamalıdır.

Google firması son olarak 1 Mart 2012 tarihinden itibaren, kendi ücretsiz hizmetlerinden yararlanan kullanıcılarının önüne, eğer bu hizmetlerden yararlanmayı devam ettirmek istiyorlarsa, onaylamaları gereken yeni bir sözleşme sunmuştur[103]. Bu sözleşmeyle firma, amaçlarının 'gizlilik politikalarını sadeleştirmek' olduğunu belirtmektedir. Bu sözleşmeye göre firma, birçok farklı hizmetini tek bir sözleşme altında toplamaktadır. Öte yandan sözleşmenin 'kişisel bilgilerin korunması' ve 'bilgi transferi' ayağındaki maddelerde, toplanan bilgilerin geniş bir alana yayılıyor olması ve bu verilerin ne zaman ve nerede kullanılacağı açıkça belirtilmemektedir[104]. Nitekim Avrupa Birliği kanun düzenleyicileri bu sözleşmeyle yurttaşlarının kişisel verileri konusundaki olası sonuçları incelemek amacıyla, bu sözleşmeyi durdurmalarını istemiştir[105].

Ancak olay yalnızca tüketici profillenmesiyle sınırlı değildir. Örneğin Google'ın düzenli olarak yayımladığı altı aylık Şeffaflık Raporu'na (Transparency Report) göre, hangi devletin bu firmadan kullanıcı bilgilerini kaç kez istediği ve kaç kez hangi içeriklerin kaldırılmasını talep ettiği gibi bilgiler yayımlamaktadır. Buna göre örneğin, Türkiye devleti, firmadan Ocak-Temmuz 2011 tarihleri arasında

[101] Geiger, H., "NFC Phones Raise Opportunities, Privacy And Security Issues", *Center for Democracy & Technology*, 11 Nisan 2011, http://www.cdt.org/blogs/harley-geiger/nfc-phones-raise-opportunities-privacy-and-security-issues, (Erişim Tarihi: 20 Temmuz 2011).

[102] "Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers", *Federal Trade Commission*, Aralık 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf, (Erişim Tarihi: 20 Temmuz 2011).

[103] "Google Policies & Principles", http://www.google.com/policies/, (Erişim Tarihi: 26 Şubat 2012).

[104] Andaç, Ş., "Derin Google kişisel bilgi avında!", *Milliyet Gazetesi*, 30 Ocak 2012, http://teknoloji.milliyet.com.tr/derin-google-kisisel-bilgi-avinda-/internet/haberdetay/30.01.2012/1495550/default.htm, (Erişim Tarihi: 26 Şubat 2012)

[105] Waugh, R., "EU says Google should 'halt' its upcoming privacy changes that share user details across search, Gmail and YouTube", *Daily Mail*, 3 Şubat 2012, http://www.dailymail.co.uk/sciencetech/article-2095962/EU-says-Google-halt-upcoming-privacy-changes.html, (Erişim Tarihi: 26 Şubat 2012)

269 öğenin kaldırılmasını ve 74 kullanıcı/hesap bilgisi verilerini istemiştir[106].

Bunun dışında bu verilerin saklanmasının başka sakıncaları da vardır. Bunlardan biri çalışanlar tarafından bu durumun istismar edilebilmesi durumudur. Nitekim 2010 yılında Google'da mühendis olarak çalışan 27 yaşındaki David Barksdale'in işteki konumundan yararlanarak, çalıştığı süre boyunca kişisel verilerinin korunmasını ihlal ettiği ortaya çıktı[107]. Bunun üzerine firma Barksdale'i işten çıkardı. Akabinde, Google bunun şirket tarihindeki ikinci olay olduğunu belirmiştir[108]. Ancak on seneden fazla İnternet'te hizmet veren ve en az 20 bin kişinin çalıştığı bir firmada açıklanan benzeri olay sayısı çok azdır. Öte yandan buna benzer başka bir olay da Facebook'ta yaşanmıştır. *The Rumpus*'ta yayımlanan bir makaleye göre, daha önceden Facebook'ta çalışan iki kişi kullanıcıların kişisel verilerinin korunmasını ihlal ettiği gerekçesiyle işten çıkartılmıştır[109]. Ancak Facebook firması bu konuda hiçbir açıklama yapamamaktadır.

Veri depolamanın bir başka tehlikesiyse, bunların bir İnternet korsanı tarafından sistemin kırılarak, tüm bu verilerin ele geçirilmesidir. Çünkü Google bile olsanız sisteminiz kırılmaz değildir. Hatta 2010 yılı Aralık ayında Google firması "çok gelişmiş" ve koordineli bir saldırının kendi kurum bilgisayar ağına gerçekleştirildiğini belirtmiştir[110]. Amerikan Verisign firmasının iDefense biriminde çalışan güvenlik araştırmacıları Aralık ayı içerisinde Google'a yapılan saldırıların, aralarında finans kurumları ve savunma sanayi firmalarının da bulunduğu 33 firmayı da vurduğunu belirtmektedir[111].

Aslında daha önceleri şirketler devlet kurumları kadar vatandaşlar hakkında bilgiye sahip değildi. 1980'lerden beri neoliberal politikalar çerçevesinde süregelen kapsamlı ekonomik deregülasyon, gözetim alanında kamu sektörünün sorumlu olduğu yükün özel sektöre kaymasını sağlamıştır. Örneğin bir zamanlar polis örgütleri tarafından uygulanan işleri özel güvenlik firmaları gibi ticari şirketler üstlenmiştir. Laperriere Quebec modeli çalışmasında 1980'lerin ortasında özel sektörün vatandaşlar üzerinde kamusal sektörden daha fazla veri sahibi olduğunu ve veri takası yaptığını gösteren kanıtlar göstermiştir. Bu çalışmadan sonra özel sektör tarafından toplanan verilere yasal sınırlamalar konmuştur. Ancak 1990'larla beraber yeni piyasa eğilimleriyle özel sektörün sahip olduğu kişisel verilerin

[106] "Google Transparency Report", www.google.com/transparencyreport, (Erişim Tarihi: 26 Şubat 2012)

[107] Chan, A., "GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated)", 14 Eylül 2010, http://gawker.com/5637234/, (Erişim Tarihi: 27 Şubat 2012)

[108] Jason Kincaid, "This Is The Second Time A Google Engineer Has Been Fired For Accessing User Data", *TechCrunch*, 14 Eylül 2010, http://techcrunch.com/2010/09/14/google-engineer-fired-security/, (Erişim Tarihi: 27 Şubat 2012)

[109] Wong, P., "Conversations About the Internet #5: Anonymous Facebook Employee", *The Rumpus*, 11 Ocak 2010, http://therumpus.net/2010/01/conversations-about-the-internet-5-anonymous-facebook-employee/?full=yes, (Erişim Tarihi: 27 Şubat 2012)

[110] Zetter, K., "Google Hack Attack Was Ultra Sophisticated, New Details Show", *Wired Magazine*, 14 Ocak 2010, http://www.wired.com/threatlevel/2010/01/operation-aurora/, (Erişim Tarihi: 27 Şubat 2012)

[111] Zetter, K., "Google Hackers Targeted Source Code of More Than 30 Companies", http://www.wired.com/threatlevel/2010/01/google-hack-attack/, 13 Ocak 2010, (Erişim Tarihi: 27 Şubat 2012)

toplandığı veritabanlarının gelişmesi daha da hız kazanmıştır. Deregülasyonla beraber örneğin giderleri kesmek amacıyla sağlık enformasyon veri tabanlarının yönetim işlevlerini devlet özel sektöre devredebilir hale gelmiştir. Bu da bu bireyin kişisel bilgilerinin özel sektöre satılmasına neden olabilmektedir. Böylece kamusal kurumlar özelleştirmeyle özel sektöre satıldıktan sonra, devlet tarafından toplanmış olan veriler özel sektörün eline bırakılmış olmaktadır.

Günümüzdeyse artık bu dört alan veri eşleştirmesi yoluyla gitgide birine entegre olmaktadır, dolayısıyla bu ayrımlar daha bulanıklaşmaya başlamış durumdadır. Bölümün başlığında belirtildiği gibi bir assemblage şeklinde bütün veritabanları merkezi bir çatı altında toplanmasa da gerektiğinde bu verilerle eşleştirilmenin yapılması teknik olarak mümkün hale gelmektedir. Öte yandan bir sonraki bölümde de görüleceği gibi Türkiye'de devlet yurttaşların devletle ilgili bütün kayıtlarını e-devlet projesiyle tek bir çatı altında toplamaktadır.

III. Bölüm:

TÜRKİYE'DE YURTTAŞLARIN SAYISAL KAYITLANMASI VE GÖZETLENMESİ: ŞECERE KAYITLARINDAN SAYISAL BEDENLENİŞE

3.1. Türkiye'de Yurttaşın Sayısal Kayıtlanmasının Kısa Tarihçesi

Birinci ve İkinci Bölümlerde serimlendiği üzere, yurttaşın kayıtlanması teknikleri hiç kuşkusuz sadece modern devlete özgü bir disipline etme ve denetleme stratejisi değildir. Bu bağlamda, Osmanlı İmparatorluğu'nda da halkın özellikle askerlik hizmeti ve vergi tahsilatı amacı ile kayıtlarının tutulduğu söylenebilir. 1869 yılında Osmanlı Tabiiyet Kararnamesi ile yeni bir düzenlemeye geçilmiş, vatandaş olma koşulu "kan bağına ve toprak esasına" dayandırılmıştır. 1870 tarihli "İdare-i Umumiye-i Vilayet Nizamnamesi" ile, il idaresi şube başkanlıkları kadrosu, emlak ve nüfus memurları kadrosu dahil tahsis edilmiştir. Bu düzenlemede nüfus memurları "il içerisinde emlak ve arazinin ve nüfusa ait kuyudatı düzenlemek ve doğum, ölüm ve yer değiştirmeye ve pasaportlara ilişkin işlemleri" yürütmekle görevli kılınmışlardır.

Bu arada 1836 yılında "Umuru Mülkiye Nezareti" adı altında kurulan ve 1838 yılında "Dahiliye Nezareti" olarak adı değiştirilen bakanlığa bağlı olarak "nüfus hizmetlerini yürütmek üzere" Ekim 1884 tarihinde "Nüfusu Umumiye Müdüriyeti" kurulmuştur. 1889 yılında ise, bu Genel Müdürlüğe "Sicilli Nüfus Ahali İdarei Umumiyesi" adı verilmiştir. Bu dönemde Osmanlı halkına ilk nüfus tezkeresi dağıtılmıştır. Ancak dağıtılan nüfus tezkereleri, herhangi bir nüfus kaydına dayanmaması ve tezkereyi taşıyan kişinin de herhangi bir nüfus kütüğüne kayıtlı olmaması nedeniyle, özel ve resmi işlemlerde pek faydalı olamamıştır. Bunun üzerine, 1905 yılında "Genel Nüfus Yazımı" yapılarak, ilk nüfus kütükleri düzenlenmiştir. Bu sayımda elde edilen kayıtlara dayanılarak, nüfus cüzdanları verilmeye başlanmıştır. Ancak, bu nüfus kütüklerinde, yalnızca Türk vatandaşları kaydedilmiş; kütüğe kayıt edilirken ikamet edilen yer esas alınmış; kayıt sırasında "Şecere" düzenine özen gösterilmiştir. Şecere düzeninde, kütükte her aileye bir bölüm (hane) ayrılmakta; kişinin kimliğine ilişkin bilgilerin yanında mensup oldukları din, meslek, zanaat, okur-yazarlık durumu ve bedensel özürleri de yazılmaktaydı. Bu kütüklerin yazımında Arap harf ve sayıları ile, tarihlerin yazımında Hicri-Kameri ve Şemsi Takvim esası kullanılmış olup; bir hanede misafir durumunda bulunanlar, misafir defterine kaydedilmekle birlikte, asıl kayıtlı oldukları nüfus idarelerine de bu durum bildirilmiştir. Bu nüfus kayıtları yalnızca mahkeme kararıyla düzeltilebilmekte veya değiştirilebilmekteydi. Doğum, ölüm ve yer değiştirme işlemleri için muhtarlarca verilecek belgeler, evlenme ve boşanma işlemleri için imam, papaz veya haham gibi dini örgütlenmelerin temsilcileri tarafından verilecek belgeler kullanılmakta olup, bütün bu işlemlerin ilgili amir ve savcılar tarafından denetlenmesi gerekli kılınmıştır.



Osmanlı devletinde kullanılan şecere kaydı



Arapça harfli kimlik defteri



Atatürk'ün nüfus defteri



Çift renkli nüfus defteri

Türkiye Cumhuriyeti devletinin kurulmasından sonra, 1924 tarihli Teşkilat-ı Esasiye Kanunu ile vatandaşlık hakkı bir esasa bağlanmıştır. Teşkilat-ı Esasiye Kanunu'nun 88. maddesinde "Türkiye ahalisine din ve ırk farkı olmaksızın vatandaşlık itibariyle (Türk) olunur" şeklinde vatandaşlık hakkı tanımlanmıştır. Nüfus defterleri Harf Devrimine değin Arap harfleri ile kayıtlanmış, 01 Kasım 1928 tarihli Harf Devrimnden sonra, kayıtlamalar Latin alfabesi ile yapılmaya başlanmıştır. 1934 yılında her aile ve ailenin fertleri soyadı almış, böylece ünvanlar ve lakaplar kaldırılmıştır. Bundan sonra, 1960 yılında nüfus cüzdanları değerli kağıt niteliğine kavuşmuş ve 1963 yılında 210 sayılı Değerli Kağıtlar Kanunu kapsamında korunmaya alınmıştır. Türkiye Cumhuriyeti yurttaşlarının kayıtlanması için en kapsamlı çalışma, MERNİS projesi ile başlamıştır[112]. Bu projenin fikri, 5 Mayıs 1972 tarihinde 1587 sayılı Nüfus Kanunu ile ortaya çıkmıştır. MERNİS adlı proje 1976 yılında Devlet Planlama Teşkilatı tarafından projelendirilmiş olup, 1980 yılında ODTÜ'ye ihale edilmiştir. 1982 ve 1996 yılları arasında projenin çalışmaları sürmüştür. Bu arada 01 Haziran 1976 tarihinde çok yapraklı nüfus cüzdanları yürürlükten kalkmış, tek yapraklık önlü arkalı, cinsiyete göre ayrıştırılmış (kadınlara pembe, erkeklere mavi renkte) kart uygulamasına geçilmiştir. Ancak 1996 yılında Dünya Bankasından projeye ilişkin olarak özelleştirme ve Sosyal Güvenlik Ağı (PIAL) kapsamında ayrılan 5,5 milyon dolarlık kredinin 3,5 milyon doları kullanılarak, ilçe bazında bilgisayar donanımlarının bir kısmı satın alındı. 1999 yılına gelindiğinde ise, Genel Müdürlük 923 ilçe nüfus müdürlüğünün altyapısını tamamlamıştı. Bu ilçelerde bilgisayar sistemleri kurulmuş ve nüfus kayıtları bilgisayar ortamına aktarılmıştı. Tüm nüfus kayıtlarını içerecek veritabanının kurulacağı ana bilgisayar sistemi Kasım 2000 tarihinde satın alınmıştır. Aralık 2000 tarihinde ana bilgisayar sisteminin kurulumu tamamlanmış, sistem kullanıma açılmıştır. Bunun için 122.145.860 kişinin nüfus bilgilerini içeren uygulama programları yaygınlaştırılmış ve merkezde bir bilgi bankası oluşturulmuştur. 1998-2000 yılları arasında ise, MERNİS uygulama yazılımları geliştirilmiştir. 28 Ekim 2000 tarihinde *Türkiye Cumhuriyeti Kimlik Numarası* tüm nüfus kayıtlarına verilmiştir. Pilot bölge uygulaması ise Ankara ve Kırıkkale illerine bağlı ilçelerde 18 Mart 2002 tarihinde gerçekleştirilmiştir. Kasım 2002 tarihinden itibaren de MERNİS sistemi çevrimiçi olarak çalışmaya başladı.

[112] MERNİS, Merkezi Nüfus İdaresi Sistemi demektir.

Türkiye Cumhuriyeti yurttaşlarının kayıtlanması açısından Türkiye'nin en büyük bilişim projesi olan MERNİS projesi, böylece 2002 yılında uygulamaya geçti. T.C. Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü bu projenin amaçlarını aşağıdaki gibi belirlemiştir:

- Nüfus mevzuatına uygun olarak merkez ve ilçe birimlerinde nüfus işlemlerinin bilgisayar ortamında yapılması ve merkezi veritabanının oluşturulması,
- Türkiye Cumhuriyeti Kimlik Numarasının verilmesi,
- Kolay taşınabilir, kolaylıkla taklit edilemez modern nüfus kimlik kartlarının verilmesi,
- Nüfus ve aile istatistiklerinin hızlı ve sağlıklı bir şekilde alınması,
- Kamu kuruluşlarına ve vatandaşa elektronik ortamda bilgi hizmetlerinin verilmesi.

Bu proje kapsamında T.C. Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü aşağıdaki hedefleri belirledi:

- Nüfus kütükleri üzerinde tam bir denetim kurmak ve nüfus kütüklerini güvenilir belgeler haline getirerek hizmette sürat ve verimliliği sağlamak,
- Merkezde bir bilgi bankası oluşturmak ve bu yoldan nüfus kütüklerindeki bilgileri kamu hizmetleri açısından değerlendirmek,
- Nüfus kütüklerindeki bilgileri istatistik verileri olarak değerlendirerek, nüfus ve aile istatistikleri elde etmek,
- Her vatandaşa bir Türkiye Cumhuriyeti kimlik numarası verilmesi yoluyla, isim benzerliğinden dolayı ortaya çıkan aksaklıkları gidermek ve kamu kuruluşları arasındaki bilgi alışverişini hızlandırmak,
- Mevcut nüfus cüzdanlarını dünya standartlarına uygun şekilde kart şeklinde nüfus cüzdanlarına dönüştürmek.

Bu aşamadan sonra, kamu kurum ve kuruluşlarının gereksinim duyduğu kişi bilgilerine elektronik ortamda hızlı bir biçimde erişim sağlanması amacıyla *Kimlik Paylaşım Sistemi* (*KPS*) projesinin yaşama geçirilmesi çalışmalarına başlanmıştır. KPS, Nüfus ve Vatandaşlık İşleri (NVİ) tarafından, MERNİS ve UAVT[113] veritabanında tutulan bilgileri sınırlandırılmış olarak alıcı kurumlar (kamu kurumları) ve diğer kişiler (diğer tüzel kişilikler) ile ilgili mevzuatta belirlenen esas ve usuller çerçevesinde, güncel ve güvenli bir şekilde, 7 gün 24 saat süreyle, çevrimiçi paylaşılmasını sağlayan bir sistemdir. KPS ile; NVİ'de tutulan nüfus ve adres bilgileri, elektronik ortamda, kamu kurumları ile bunların dışında kalan diğer tüzel kişiliklerin hizmetine sunulmaktadır. Böylece, kurum ve kuruluşların ihtiyaç

[113]UAVT, ulusal adres veritabanı demektir.

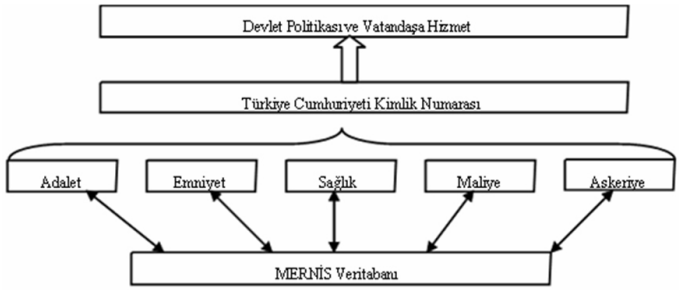
duydukları nüfus kayıt örneği ve yerleşim yeri adresi gibi bilgi ve belgeler ilgili nüfus müdürlükleri ile yazışma yapılmadan veya bireylerden istenmeden doğrudan ve anında KPS'den temin edilebilmektedir.

Daha sonra vergi kimlik numarası almış olan T.C vatandaşlarının vergi kimlik numaraları ile T.C. kimlik numaralarının eşleştirilmesi işlemleri tamamlanıp, 1 Temmuz 2006 tarihinden itibaren vergi dairelerince fiilen Türkiye Cumhuriyeti kimlik numarası kullanılmaya başlanmıştır. Vergi dairelerinin Kimlik Paylaşım Sistemini (KPS) kullanmaları sonucunda; ekonomik ve mali; vergi tahsilâtı ve denetimi kolaylaşmış, kayıt dışı ekonomi kontrol altına alınmaya başlanmıştır. Noter, tapu, bankacılık vb. işlemlerde MERNİS veritabanına erişilerek kişilerin nüfus kayıtlarının doğruluğu tespit edilip dolandırıcılık ve sahtecilik ortadan kaldırılmaya başlanmıştır. Suçların önlenmesi ve suçluların yakalanmasında güvenlik birimleri, aranan kişilerin bilgilerine veritabanından ulaşıp kimlik tespiti yapabilmekte, sahte kimlik kullanımı önleyerek sahte kimlikleri tespit edebilmektedir. Askerlik çağına gelen bireylerin listeleri Askere Alma Daire Başkanlığı (ASAL) tarafından zamanında MERNİS veritabanından alınarak askere alma ve asker kaçaklarının izlenmesi daha kolay olmuştur, Ayrıca yaş gruplarına göre erkek nüfus bilgilerinin kullanılması, Türk Silahlı Kuvvetleri'nin gelecek yıllardaki asker ihtiyacını ve sayısını planlamasına yardımcı olmuştur. Sağlık kuruluşlarında her birey için açılan dosyalarda kimlik numarası kullanıldığından, bilgilerin bir bütün halinde tutulması sağlanmış ve sağlık hizmetlerinden yararlanma standart işlemlere bağlı olmuştur, Sağlık sektöründe yaşanan yolsuzluklar büyük ölçüde engellenmeye başlanmış, var olanlar da ortaya çıkarılmıştır, Sağlık alanında yapılması düşünülen yeni yatırımlar- örneğin hastane ve sağlık ocağı açılması vb.– bundan sonra veritabanındaki bilgilere göre planlanacaktır. Eğitim alanıyla ilgili olarak da; KPS veritabanı kullanımı ile okul çağına gelen çocuklar tespit edilerek okula gitmeleri sağlanmıştır. Sosyal Güvenlik Kurumları da nüfus müdürlüklerinden istemiş oldukları nüfus kayıt örneğine KPS'nin sağladığı bilgi işlem ortamında rahatlıkla ulaşabilmekte ve böylece kurumlar arası yazışma ortadan kalkarak işlemler daha hızlı bir şekilde yürütülebilmektedir. Mahkemelerde davaların görülmesi sırasında kimlik tespiti yapılarak, bireyin verasete ilişkin tüm aile bireyleri belirlenmekte, nüfus kayıt örneği alınabilmekte, böylece davaların daha hızlı şekilde görülmesi sağlanmaktadır. Tüm bunlar MERNİS ve KPS'nin kamu hizmetlerinin işleyiş sürecine sağladığı olumlu katkılardır[114].

KPS ile Hangi Kişisel Veriler Sunulmaktadır?

KPS, aşağıdaki verileri bünyesindeki servisler aracılığı ile sunmaktadır. Bu veriler, aile kütüklerindeki kayıtlar gibi Türk vatandaşlığının ispatında ve belgelendirilmesinde esas olduğu kadar kişinin kimliği, medenî hâli ve aile bağlarının

[114] MERNİS uygulamasını betimleyici düzeyde tanıtan ve kamu hizmetine katkılarını ele alan iki çalışma için bakınız: Özmen, L.A. (2010). *Türk Nüfus Hizmetleri Sistemi ve MERNİS Projesi*. Ankara: Gazi Üniversitesi SBE. Yayınlanmamış Y.Lisans Tezi; Yosuntaş, Ç. (2008). *Sahte Kimlik*. İstanbul: Beykent Üniversitesi SBE. Yayınlanmamış Y.Lisans Tezi. E-devlet uygulamasını ve başarılı olması için temel koşulları değerlendiren bir çalışma için ise bakınız: Ekici, G. (2007). *Kamu Kurumlarının E-Devlet Uygulamalarında Vatandaş Bilgilerinin Güvenliği ve Korunması.* Ankara: Hacettepe Üniversitesi SBE. Yayınlanmamış Y.Lisans Tezi.



belirlenmesinde de hukuken geçerli temel resmi bilgilerdir. Ayrıca, mevzuatta yapılan düzenlemeler ve hizmet gereği duyulacak ihtiyaçlar çerçevesinde KPS'de yer alacak bilgileri belirlemeye İçişleri Bakanlığı yetkilidir.

Kişi bilgileri:

a) Kimlik numarası, adı, soyadı, cinsiyeti, baba adı, anne adı, doğum yeri, doğum ve kütüğe kayıt tarihleri gibi kişisel bilgiler.

b) Medeni hâli, dini ve ölüm tarihi gibi durum bilgileri.

c) İl, ilçe, cilt, mahalle veya köy, aile sıra numarası ve birey sıra numarası gibi nüfusa kayıtlı olduğu yer bilgileri.

Nüfus Cüzdanı Bilgileri:

a) Nüfus cüzdanı üzerinde yer alan bilgiler.

b) 1/6/2000 tarihinden sonra düzenlenen cüzdanlarda seri ve no'su ile verildiği yer ve tarihi.

c) 1/6/2000 tarihinden önce düzenlenmiş cüzdanlarda cüzdan seri, no ve verildiği maliye saymanlığının adı.

Nüfus Olay Bilgileri:

Evlenme, boşanma, soybağının düzeltilmesi veya reddi, ölüm, vatandaşlığın kazanılması veya kaybedilmesi, yerleşim yeri ve diğer adres gibi kişilere ait nüfus olay bilgilerinin tarihi ve açıklamaları.

Adres Bilgileri:

Kişinin bildirdiği mevcut yerleşim yeri adresi ve diğer adresleri.

Ulusal Adres Veritabanında Yer Alan Bilgiler:

Posta kodları, il, ilçe, bucak, köy ve mezra isimleri, mahalle, meydan, bulvar, cadde, sokak isimleri ile sabit tanıtım numarası ve bina numarası gibi adres verileri ile tanımlanan coğrafi konum, kişisel ve kurumsal adres bilgisine ulaşmak için gerekli olan bilgiler.

İstatistik Bilgileri:

Doğum, ölüm, evlenme, boşanma sayıları gibi yerleşim birimi bazında ve belli bir zaman dilimine ait bilgiler.

Tüm bu bilgiler, kurum ve kuruluşların gereksinimlerine göre oluşturulan belli girdi parametrelerine karşılık belirli çıktılardan oluşan KPS web sayfaları ve hizmetleri şeklinde sunulmaktadır. Sunulan hizmetlerin listesi KPS ana sayfasından güncel olarak yayınlanmaktadır. Halen 70 kurum ücretsiz, 47 kurum ücretli olmak üzere toplam 117 kurum yapılan ikili anlaşmalar çerçevesinde KPS'den bilgi erişimi yapabilmektedir.

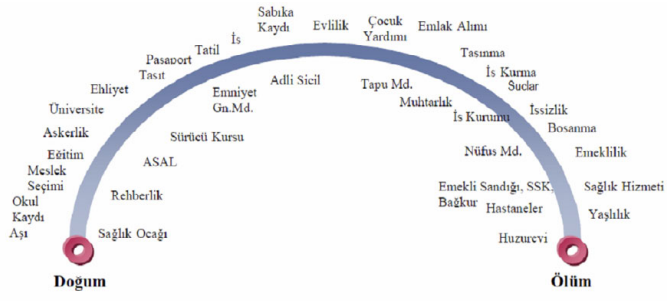
MERNİS ve KPS uygulamasına yönelik sosyal bilimler alanında eleştirel bakış açısı ile değerlendirmeler sınırlı sayıdadır. İlk olarak, Çağatay Topal "Global Citizens and Local Powers: Surveillance in Turkey" (2005) adlı makalesinde[115], MERNİS projesinin dijital gözetim boyutuna dikkat çekmiştir. KPS veritabanı aracılığı ile bir "gözetim assemblage"ı (2005:89) oluşturulmaktadır. Özellikle MERNİS dolayımı ile KPS de toplanan veriler ve çalışmanın bundan sonraki kısmında ayrıntılı olarak ele alınacak olan e-devlet kapısı uygulamaları ile e-kimlik kartı göz önüne alındığında, Türkiye'de yurttaşın doğumdan ölüme, gündelik yaşamın her alanında dijital olarak kayıtlandığı, sınıflandırılabileceği gerçeği ortaya çıkmaktadır. Alanur Çavlin Bozbeyoğlu da "Türkiye'nin Biyometrik Elektronik Kimlik Kartı Sistemi" adlı çalışmasında[116], Türkiye'de nüfus sayımlarının nüfusu etnik köken ve mezhebe göre ayırmada kullanıldığına dikkat çekmekte, T.C. Kimlik Numarası kullanımı ile yurttaşın yaşamının her anında ve alanında denetime tabii tutulduğunu belirtmekte, e-kimlik kartlarının dağıtılmasıyla da benzeri bir siyasi, toplumsal ve kültürel ayrımcılık politikalarına hizmet edebileceği şeklindeki kaygılarını dile getirmektedir.

TÜBİTAK UEKAE[117] tarafından e-kimlik kartı projesinin yürütüldüğünü ve pilot uygulamanın 2010 yılında Bolu'da gerçekleştirildiğini belirelim. Yüksek Planlama Kurulu'nun 11 Temmuz 2006 tarih ve 2006/38 no'lu kararı ile "Bilgi Toplumu Stratejisi Eylem Planı" kabul edilmiş ve 28 Temmuz 2006 tarih ve 26242 sayılı Resmi Gazete'de yayınlanmıştır. Bu Eylem Planının 46. madde-

[115] Bakınız: Çağatay Topal (2005). "Global Citizens and Local Powers: Surveillance in Turkey", *Social Text* 83, 23(2): 85-93.

[116] Alanur Çavlin-Bozbeyoğlu (2011). "Türkiye'nin Biyometrik Elektronik Kimlik Kartı Sistemi", *Toplum ve Bilim*, S.122. syf. 53-74.

[117] UEKAE, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nün kısaltmasıdır.



sinde "Vatandaşlık Kartı: Pilot Uygulaması ve Yaygınlaştırılması ile biyometrik unsurlar içeren elektronik vatandaşlık kartının kimlik doğrulama için kullanımının sağlanması ve tüm kimlik doğrulama fonksiyonlarının tek bir elektronik kartta toplanması" öngörülmüştür (Kubilay, Adalıer ve Karademir, 2010: 8)[118]. TÜBİTAK UEKAE tarafından yürütülen "Elektronik Kimlik Doğrulma Sistemi" (EKDS), diğer bir deyişle e-kimlik kartı projesinde "Çağdaş kimlik kartı, MERNİS Projesini tamamlayacak bir uygulama olacak" denilmektedir (Kubilay, Adalıer ve Karademir, 2010: 8). Başbakan Recep Tayyip Erdoğan da 12 Haziran 2011 tarihli Genel Seçimi takiben, yeni hükümet programını açıklarken

> "Kamu hizmetlerinin sunumu sırasında vatandaşlarımızdan diğer kamu kurumlarında bulunan bilgi ve belgeler artık istenmeyecek. Bugün vatandaşlarımız devlet ile olan işlerinin büyük bir kısmını internet üzerinden kolaylıkla yapabiliyor. Okul kaydından vergi ödemelerine, araç satışından tapu muamelelerine, ihracat, ithalattan trafik işlemlerine kadar birçok hizmeti elektronik ortamda verilebilir hale getirdik. Kamudaki işlemlerin resmi olarak elektronik ortamda gerçekleşmesine imkan sağlayan "elektronik imza" uygulamasını hayata geçirdik. Tüm vatandaşlarımıza "elektronik vatandaşlık kartı" dağıtımını gerçekleştireceğiz. Elektronik vatandaşlık kartı, kamu hizmetlerinin sunumunda kimlik doğrulama işlemleri için kullanılacak. Böylece vatandaşlarımızın kamu hizmetlerine 7 gün 24 saat evlerinden veya işyerinden ulaşabilecek."[119]

şeklinde açıklama yapmıştır.

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanı Binali Yıldırım da E-Devlet kapısının mevcut durumu üzerine bilgi verdiği bir görüşmede, 9.6 milyon kullanıcının olduğunu ve 276 kamu hizmetinin bu kapı üzerinden verildiğini belirtmiş ve e-Devlet kapısının kamu kaynaklarının daha verimli kullanılmasını sağlayacağı ve

[118]M. Aydın Kubilay, Oktay Adalıer ve Apti Karademir (2010) "Türkiye'nin E-Kimlik Yolculuğu", *UEKAE Dergisi*, 2(4): syf. 6-25.

[119]Konuşmanın tam metnine AKP'nin web sitesinden erişebilirsiniz: http://www.akparti.org.tr/site/haberler/basbakan-erdoganin-hukumet-programini-sunus-konusmasinin-tam-metni/10899

kamu yönetiminin şeffaflığını ve hesapverebilirliğine katkıda bulunacağını iddia etmiştir[120]. Yıldırım'ın söylemi analiz edildiğinde, Türkiye'de e-Devlet kapısının ve e-Kimlik uygulamasının yönetişim modeli içerisinde tanımlandığı açık bir şekilde ortaya çıkmaktadır.

Oktay Adalıer TÜBİTAK BİLGEM'de "T.C. Kimlik Kartı (eKimlik)" başlıklı 20 Haziran 2011 tarihinde yaptığı sunumda, "eKimlik" kapsamında mevcut durumu açıklamıştır: "eKimlik" uygulamasına bir ilde başlanacak, yedi bölgede birer şehirde dağıtıma devam edilecek ve yurtdışında iki yerde uygulamaya başlanacaktır." demiştir. Ayrıca Adalıer, "T.C. Kimlik Kartı, alternatifsiz bir sistem olup e-Devlet açınımında vatandaşın kurumlara ulaşımında anahtar vazifesi görecektir" vurgusunu da yapmaktadır. Adalıer sunumun son kısmında e-Kimlik kartı uygulamasında "mahremiyet konrolü" başlığı ile, e-Devlet kapısı ve e-Kimlik kartı çipleri içinde toplanan verilerin güvenliği sorununa da kısmen olsa da dikkat çekmiştir. Kamuoyuna örnek olarak sunulan e-Kimlik kartı görseli incelendiğinde Bozbeyoğlu'nun yukarıda bahsedlen çalışmasında dile getirdiği kaygıları haklı gösterecek bir olguyu ortaya çıkmaktadır: E-Kimlik kartı çeşitli şekillerde yurttaşı "muteber" ve "muteber olmayanlar" şeklinde ayırt edecek, sınıflandıracak veritabanı ve veri eşleştirmesine zemin oluşturmaktadır. Kartın arka yüzeyinde "Din Hanesi" nin yazması aynı zamanda Şubat 2010 tarihli AİHM'in T.C. nüfus cüzdanlarında din ibaresinin yer almasının Avrupa İnsan Hakları Sözleşmesi'nin 9.maddesine aykırı olduğu ve kalkması gereği yönündeki kararıyla da çelişkilidir.[121]

3.2. Araştırmanın Yöntemi: E-devlet Kapısı Üzerinde Yurttaşın Sayısal Bedenlenişinin Topografyasını Çıkartmak

Bilgisayar Dolayımlı İletişim (BDİ) (*computer mediated communication*) araştırmaları dünyada yirmi yılı aşkın bir süredir devam etmektedir, buna karşın Türkiye'ye BDİ üzerine yürütülen araştırmalar son 10 yıl içerisinde önem kazanmıştır. Bu alandaki araştırmalarda genel olarak uzam (uzamın kullanım şekilleri ve toplumsal aktörlerin bu uzamda neler yaptığı, uzamı alımlama pratikleri) ve metin (sanal uzamda bedenin geride bırakılarak, ortamın kendisinin bir metin olarak ele alınması) incelemeleri yapılmaktadır (Binark, 2005: 182). BDİ üzerine yapılan araştırmaların kendine özgü özellikleri vardır; öncelikle araştırma bilgisayar kullanılarak yürütülmekte ve elde edilen bilgilerin büyük çoğunluğu İnternet üzerinden edinilen verilere dayanmaktadır. Buna ek olarak, incelenen metin sürekli bir değişim halindedir, gerek kullanıcılar tarafından kesintisiz bir şekilde ve çok sayıda yeni metinlerin eklenmesi, gerekse ortamın/arayüzeyin

[120] Bakınız: *İctMedia*, Ekim 2011, syf. 16-17.

[121] Işıl Cinmen, "Yeni Kimliklerimiz Yne 'Dini' Yine 'Medeni'!", *Bianet.org*, http://www.bianet.org/bianet/diger/134618-yeni-kimliklerimiz-yine-dini-yine-medeni (Erişim tarihi: 09 Aralık 2011).

sıklıkla tasarımcılar tarafından geliştirilmesi/değiştirilmesi araştırmacılar tarafından alanın/metnin takip edilmesini zorlaştırmaktadır. Hızla değişim gösteren bu ortamda araştırma süresi de büyük önem kazanmaktadır, sürekli yeni bilgilerin eklenmesi araştırmacının elde ettiği bilgilerin günceliğini etkilemektedir. Bu nedenle İnternet araştırmalarında istenen bilgiye kısa bir sürede ulaşmak ve araştırma süresini doğru belirlemek büyük önem kazanmaktadır. Bir başka önemli nokta ise, araştırmacının yerinde inceleme yapmasıdır. Oluşan veri yığını içerisinde bağlantıları doğru saptayabilmek için araştırmacının söz konusu ortamın içerisine dahil olması gerekmektedir, bu nedenle BDİ alanında yürütülen araştırmalarda "sanal etnografi", yöntemine çoğunlukla başvurulmaktadır (Toprak vd, 2009: 89). Sanal etnografi çalışmalarında araştırmacı incelenen sanal uzama dahil olmakta, ortamı deneyimlemekte ve tıpkı diğer kullanıcılar gibi arayüzey ile etkileşime girmektedir. Bu sayede araştırmacı, arayüzeyin yapısını, çevrimiçi toplulukların davranışlarını ve tepkilerini inceleyerek birçok veriye anında ulaşabilmektedir (Binark, 2005: 184). Bu araştırmada da T.C. kimlik numarasının kullanıldığı sanal uzamlara –burada E-devlet kapısına- kullanıcı olarak dahil olunmuştur. İnternet incelemelerinde bir başka önemli araştırma yöntemi de sanal topografya çalışmalarıdır. Chris Nunes sanal topografyayı, siber uzamda belirlenmiş nokta ve hatlar arasında düzenlenmiş bağlantılar sistemi olarak tanımlamaktadır (aktaran Bayne 2004: 304). Deleuze ve Guattari'ye göre de sanal topografya, sanal uzamda bir noktadan başka bir noktaya bağlanan yolları ve yörüngelerin oluşturduğu damarlı ağ yapısını ortaya çıkarmaktadır (aktaran Nunes, 2006: 17). Bu bağlamda dijital gözetim olgusunu incelemek ve yurttaşın sayısal bedenlenişini daha iyi kavrayabilmek için, T.C. kimlik numarasının sanal uzamda kullanımının topografyasının çıkarılması büyük önem taşımaktadır.

Bu çalışmada da, T.C. kimlik numarasının sanal uzamda hangi hatlar üzerinden nereden nereye nasıl bağlandığının topografyasını çıkartmak için, E-devlet kapısı 12.5.2011 ile 15.7.2011 tarihleri arasında gözlemlenmiş[122], E-devlet kapısı uygulaması bir metin gibi incelenmiştir. Araştırma kapsamında, ilk olarak E-devlet şifresi alındıktan sonra www.turkiye.gov.tr adresinde oturum açılmış, E-devlet kapısının yapısı ve link verdiği bazı devlet kurumlarının İnternet sayfaları incelenmiştir. İkinci olarak, T.C. kimlik numarası üzerinden işlem yapan diğer potansiyel kayıtlayıcılar (İnternet üzerinden satış yapan ticari İnternet sayfaları, siyasi partiler, STK'lar) bu topografyaya dahil edilmiştir. Yurttaşın sayısal bedenlenişinin topografyasını çıkartmayı amaçlayan bu araştırmanın son kısmında ise, tüm Türkiye'de uygulamaya geçecek olan Elektronik Kimlik Doğrulama Sistemi (EKDS) sistemi incelenmiştir. Araştırmadan çıkan bulgular doğrultusunda T.C. kimlik numarasının sanal uzamdaki kullanım alanları, potansiyel kayıtlayıcıları, kurum ve kuruluşlar arasındaki paylaşımı incelenmiş, ve böylece Türkiye'de yurttaşın sayısal bedenlenişinin sanal topografyası ortaya konmuş bulunmaktadır.

[122] E-devlet kapısı bu çalışma yayına hazırlanırken tekrar gözlemlenmiş, E-devlet arayüzeyindeki uygulama değişiklikleri (yeni hizmetler, linkler, sayfa tasarımı, güvenlik vb. ögelerin kullanımı) veya güncellemeler üzerinden yurttaşın sayısal bedenlenişine ilişkin hazırlanan topografya yenilenmiştir.

3.3. Türkiye'de Yurttaşın Sayısal Bedenlenişinin Topografyası

Yukarıda kısaca bahsedildiği üzere, MERNİS projesi kapsamında 122.145.860 kişiye T.C. kimlik numarası verilmiştir, projenin tamamlanmasıyla birlikte 28 Ekim 2000 tarihinden sonra verilen nüfus cüzdanlarında T.C. kimlik numarası yazılmaya başlanmıştır. Vatandaşlar sahip oldukları T.C. kimlik numarasını üç farklı şekilde öğrenebilmektedir; Nüfus İdaresi Daire Başkanlığı'nın İnternet sayfasından (www.tckimlik.nvi.gov.tr) nüfus cüzdanı bilgileri girilerek, il ve ilçe nüfus idarelerine başvurularak, ya da yeni bir nüfus cüzdanı alarak öğrenilebilmektedir. T.C. kimlik numarası uygulaması başlamasından 2008 yılına kadar geçen 8 yıl zarfında, 58.000.000 kişi T.C. kimlik numarasını öğrenmiştir: bu kişilerin numaralarını öğrenmek için en çok kullandıkları yöntem ise, kamu kurum ve kuruluşları aracılığı (21.000.000 kişi); nüfus kayıt örneği aracılığı ile (15.000.000 kişi) ve İnternet aracılığı ile (10.000.000 kişi) şeklinde sıralanabilir (NVİ, 2008).

Çalışmanın bu kısmında T.C. kimlik numarası ile dahil olunan E-devlet kapısının kullanımı ve arayüzeyin kendisi incelenecektir. E-devlet kapısı, Türkiye'deki tüm devlet kurumlarını sanal uzamda tek bir adres üzerinden temsil etme niteliğini taşıyan bir İnternet sitesidir. 18 Aralık 2008 tarihinde www.turkiye.gov.tr adresinden erişime açılan E-devlet kapısı halihazırda 12.123.846 kayıtlı kullanıcıya ulaşmıştır. Kapının genel amacı kamu hizmetlerini, yurttaşlara ve kamu kurumlarına İnternet üzerinden sunmaktır (E-devlet kapısı, 2012). E-devlet uygulamalarını kullanmak için, www.turkiye.gov.tr adresinden dört farklı elektronik imza[123] yönteminden birini kullanarak sisteme girmek olanaklıdır. Bu yöntemler: (1) e-devlet şifresi kullanmak, (2) mobil imza kullanmak, (3) e-imza kullanmak ve (4) T.C. kimlik kartı kullanmak. Bu yöntemleri kısaca açıklayacak olursak;

- **E-devlet Şifresi:** E-devlet kapısında T.C. kimlik numarası ve e-devlet şifresi kullanılarak oturum açılmaktadır. E-devlet şifresi PTT merkez müdürlüklerinden şahsen başvuru ile üzerinde T.C. Kimlik numarası bulunan kimlik belgesi gösterilerek alınmaktadır. Şifre ilk defa alındığında işlem bedeli olarak 1 TL. alınmaktadır, ancak şifrenin kaybedilmesi, unutulması vb. durumlarda PTT'den alınacak her yeni şifre için 10 TL. ücret ödenmektedir. Bu işlem masrafı dışında herhangi bir yıllık ücret istenmemektedir (E-devlet kapısı, 2012).

- **Mobil İmza:** Mobil elektronik imza cep telefonu ve GSM SIM kart kullanılarak uygulanan bir sistemdir. Dijital ortamda atılan bu imza ıslak imzanın dijital ortamdaki temsili niteliğindedir ve eş değerde hukuksal geçerliliğe sahiptir. Mobil elektronik imzayı kullanılabilmek için GSM operatöründen

[123] Elektronik imza, ıslak imzanın dijital ortamda yerini almaktadır; temel amacı, veriyi kullanan kişinin kimliğini tespit etmektir. 5070 sayılı Elektronik İmza Kanunu, elektronik imzayı şu şekilde tanımlanmaktadır: "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" (BTK, 2012).



Çipli kimlik kartının ön yüzü

(Turkcell veya Avea) hizmetin satın alınması gerekmektedir (E-devlet kapısı, 2012). Hizmet bedeli olarak her imza başına ücret alınmakta ya da GSM operatörü tarafından belirlenen aylık sabit bir ücret ödenmektedir. Kullanım şeklini şöyle açıklayabiliriz; ilk aşamada, www.turkiye.gov.tr İnternet sayfasındaki Mobil imza bölümüne T.C. kimlik numarası ve cep telefonu numarası girilmektedir. İkinci aşamada, cep telefonuna kısa mesaj yoluyla onaylanması istenen işlemin ismi gelmektedir, SMS deki şifre ile web sayfasındaki şifre kullanıcı tarafından karşılaştırılıp aynı olup olmadığı anlaşıldıktan sonra kullanıcı mobil imza şifresini cep telefonuna girerek işlemi onaylamaktadır. Bu onaydan sonra E-devlet kapısında oturum açılmaktadır.

- **Elektronik İmza:** Elektronik imza ile giriş yapmak için kullanılan bilgisayara bazı ek donanımın tedarik edilmesi ve bazı ek yazılımların kurulması geremektedir. Öncelikle kullanılan bilgisayara bir adet kart okuyucu takılmaktadır, daha sonra sözü geçen kart okuyucuya okutulan ve kimlik tanımlanması için kullanılan bir akıllı kart gerekmektedir, son olarak da bu donanımların kullanılabilmesi için gerekli yazılımın bilgisayara yüklenmesi gerekmektedir. Bu donanımlar ve yazılımlar BTK'nın belirlediği Sertifika Hizmet Sağlayıcı firmalar tarafından ücret karşılığında satın alınmaktadır (E-devlet kapısı, 2012).

- **T.C. Kimlik Kartı:** T.C. Kimlik kartı, nüfus cüzdanının yerini alacak elektronik bir kimlik kartıdır. Bu kart şu anda pilot uygulama olarak sadece Bolu ilinde kullanılmaktadır. T.C. Kimlik Kartı ile E-devlet kapısına giriş yapabilmesi için iki yöntem bulunmaktadır:

  a) Standart Kart Okuyucu ile giriş: T.C Kimlik Kartı ve şifre (PIN) kullanarak ile giriş yapılabilmektedir. Bunun için bilgisayarınızda standart bir kart okuyucu ve UEKAE tarafından geliştirilen AKİS (Akıllı Kart İşletim Sistemi) yazılımı kurulu olmalıdır.

  b) Kart Erişim Cihazı ile giriş: Kullanılan bilgisayara ek donanım olarak KEC (kart erişim Cihazı) Sürücüsü ve OYA (Otomasyon Yazılım Arabirimi) kurulu olmalıdır. Sisteme girişi Kart, Şifre (PIN) ve Parmak İzi üçlüsü kullanılarak yapılması öngörülmektedir (E-devlet kapısı, 2012).



Çipli kimlik kartının arka yüzü

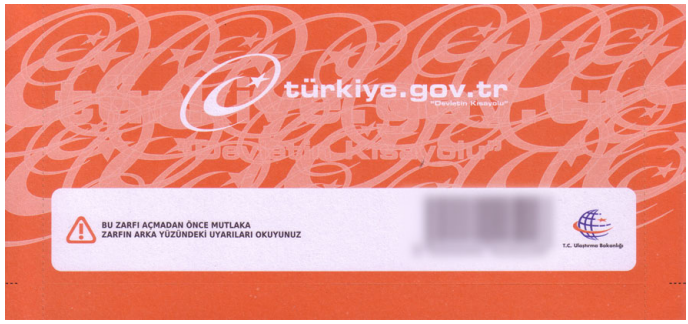


Kart erişim cihazı

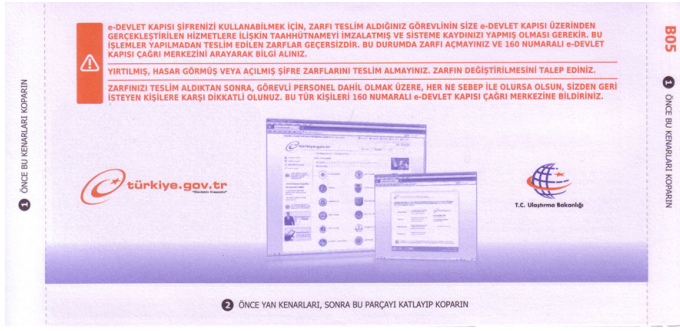
E-devlet Kapısından İçeri Girmek ve Topos'u Keşfetmek

Bu bölümde E-devlet kapısında oturum açma işlemi ve www.turkiye.gov.tr sayfasının genel yapısı incelenmiştir. Araştırma boyunca, elektronik imza yöntemi olarak sadece e-devlet şifresi ile sisteme giriş yapıldığını da belirtelim. Araştırma kapsamında E-devlet kapısında oturum açmak için gerekli olan E-devlet şifresi PTT'nin Ankara Yenişehir şubesinden 1 TL. karşılığında satın alınmıştır. İşlem, 5 farklı aşamadan oluşmaktadır: (1) PTT yetkilisi araştırmacıdan üzerinde T.C. kimlik numarası bulunan bir kimlik belgesi istemiştir. (2) araştırmacın sahip olduğu T.C. kimlik numarası ve kimlik bilgileri sisteme girilmiştir. (3) Kapalı zarfın üzerinde bulunan barkod, barkod okuyucuya okutularak kapalı zarfta bulunan e-devlet şifresi araştırmacının T.C. kimlik numarasıyla eşleştirilmiş ve şahsa özel hale getirilmiştir. (4) Araştırmacıya e-devlet kapısı üzerinden gerçekleştirilen hizmetlere ilişkin taahhütname imzalatılmıştır (bu belgenin üzerinde işlem tarihi, e-devlet şifre zarfının üzerinde bulunan barkodun aynısı, araştırmacının T.C. kimlik numarası / adı soyadı ve yasal uyarılar yer almaktadır) (5) İşlem sonunda araştırmacıdan 1 TL istenmiş ve kapalı zarf içerisinde e-devlet şifresi teslim edilmiştir (Bakınız: Şekil "PTT'den alınan e-devlet sifresinin oldugu zarfın ön yüzü" ve Şekil "PTT'den alınan e-devlet sifresinin oldugu zarfın arka yüzü").

E-devlet kapısından sisteme bağlanmak için www.turkiye.gov.tr adresinden



PTT'den alınan e-devlet şifresinin olduğu zarfın ön yüzü



PTT'den alınan e-devlet şifresinin olduğu zarfın arka yüzü

"*Sisteme Giriş*" bölümüne girilmiştir, bu bölümdeki dört farklı elektronik imza seçeneğinden e-devlet şifresi ve T.C. Kimlik numarası kullanılarak giriş yapılmıştır. Sisteme ilk defa giriş yapıldığında bir sefere mahsus olarak "*Hoşgeldiniz Sayfası*" açılmaktadır ve kullanıcıdan yeni bir şifre oluşturmasını istenmektedir. Bu işlemin ardından PTT şubesinden alınan E-devlet şifresi işlevliğini yitirmektedir. Mecburi şifre değişikliğinden sonra *Onay ve Güvenlik Uyarısı* sayfası açılmaktadır. Bu sayfada e-devlet şifresi hakkında güvenlik uyarıları ve alınması gereken önlemler belirtilmektedir. Bu aşamalar geçildikten sonra www.turkiye.gov.tr sayfasındaki uygulamalar kullanıma açılmaktadır.

Bu noktada, www.turkiye.gov.tr ilk hizmete açıldığında iki ana bölümden oluşmakta olduğunu belirtelim: (1) kamu hizmetleri konusunda bilg¬ilendirme amaçlı "Vatandaş", "Devlet" ve "İş" bölümleri, (2) elektronik devlet hizmetlerin verildiği bölüm. 1 Mart 2012 tarihli arayüzey incelemesindeyse e-devlet kapısının arayüzeyinin ve bölümlerinin yeniden tasarlandığı görülmüştür. Bu yeni tasarım beş ana bölümden oluşmaktadır: (1) Kurumlardan bilgi almak için kurulan *sorgula* bölümü. (2) Kurumlardan alınacak hizmet, kurumlar için yapılacak iş ve sınav başvuruları için *başvur* bölümü. (3) Denizcilik Müsteşarlığına yapılacak ödemeler için Öde bölümü. (4) "Öğren" başlığı altında bulunan vatandaşları bilgilendirme amaçlı *Vatandaş rehberi* bölümü. (5) Bilgi edinme başvuruları için *iletişime geç* bölümü. Bu ana bölümlerin dışında birçok ek bölüm bulunmakta-

[redacted]

TC Kimlik No : [redacted]

18.01.2011

E- DEVLET KAPISI ÜZERİNDEN GERÇEKLEŞTİRİLEN HİZMETLERE İLİŞKİN TAAHHÜTNAME

İşbu taahhütname, 20.04.2006 tarihli ve 26145 sayılı Resmi Gazete'de yayınlanarak yürürlüğe giren 2006/10316 sayılı "e-Devlet Kapısı'nın Kurulması, İşletilmesi ve Yönetilmesine İlişkin Bakanlar Kurulu Kararı" hükmü gereği, Vatandaş tarafından, e-Devlet Kapısı'na erişim ve e-Devlet Kapısı üzerinden sunulacak hizmetler hususunda, e-Devlet Kapısı'na cezai, idari, yasal ve hukuki sorumluluk yükletilemeyeceğine ilişkin gayrikabili rücu olarak kabul, beyan ve taahhüd edilmesini düzenlemektedir.

Bu taahhütnamede geçen şifre tanımlaması vatandaşın kendisi tarafından tanımlanmış parolasını, sisteme kendisi tarafından yüklenmiş bilgilerini ve e-Devlet Kapısı tarafından kendisine verilmiş veya kendi belirlediği şifreyi ifade etmektedir.

VATANDAŞ,

1. e-Devlet Kapısı'nda, şifresini kullanmak suretiyle kendisince verilen talimatların yazılı talimatı yerine geçeceğini,
2. e-Devlet Kapısı uygulamalarının içerik ve kapsamında önceden haber verilmeksizin değişiklik yapılabileceğini,
3. İşbu taahhütname çerçevesinde e-Devlet Kapısı tarafından verilecek hizmetlerden yararlanma hakkının vatandaşın münhasıran kendisine ait olduğunu,
4. Şifresini vekili dahi olsa herhangi bir üçüncü kişiye veya e-Devlet Kapısı görevlilerine açıklamayacağını, veya kullanılmasına izin vermeyeceğini, kullanılması durumunda sonuçlarından e-Devlet Kapısı'nın herhangi bir cezai, idari, yasal ve hukuki vb. yönlerden sorumlu olmayacağını, e-Devlet Kapısı'nın işlem yapan kişilerin kimliklerini araştırma yükümlülüğünün olmadığını,
5. e-Devlet Kapısı'nın sunduğu hizmetlerde kullanılan şifrenin gizli kalması için gerekli dikkat ve özeni göstereceğini, yazılı olarak saklamayacağını, kendi kontrolü dışında üçüncü şahısların eline geçmesi halinde derhal e-Devlet Kapısı'na yazılı ihbarda bulunmayı, yazılı ihbarda bulunulan tarihe kadar kullanılması durumunda sonuçlarından e-Devlet Kapısı'nın sorumlu olmayacağını,
6. Kendisine ait şifrenin unutulması, kaybedilmesi, yanlış bir şifrenin kullanılması ve/veya ulaşım kayıtları bilgilerinin e-Devlet Kapısı görevlilerine yanlış olarak beyan edilmesi durumunda ve/veya e-Devlet Kapısı'nın güvenlik açısından gerekli görmesi halinde, işlemi durdurmak, hesabı dondurmak/işlemi yapmamak/şifreyi iptal etmek/şifreyi vatandaşa haber vermeksizin iptal etmek ve/veya değiştirilmesini talep etmek ve/veya iş bu protokolü iptal etmek haklarına sahip olduğunu, bu durumda zararlarından, kayıplarından ve gecikmelerden e-Devlet Kapısı'nın sorumlu tutulamayacağını,
7. e- Devlet hizmetlerini kullanırken ortaya çıkabilecek cihaz arızası, iletişim kesintisi, iletişim yavaşlığı, hat yoğunluğu vb. teknik nedenlerden dolayı hizmetin yerine getirilememesi durumunda e-Devlet Kapısı'nın herhangi bir sorumluluğunun olmayacağını,
8. e-Devlet Kapısı tarafından izah ve tavsiye edilen güvenlik önlemlerini uygulamayı, güncellemeyi, uygulamak istemediği takdirde, e-Devlet Kapısı'nın, sunduğu işlemlerin niteliğinde ve niceliğinde kısıtlamalara gidebileceğini,

Yukarıdaki arz ve izah edilen neden ve gerekçeler ile e-Devlet Kapısı'na herhangi bir cezai, idari, yasal ve hukuki sorumluluk yüketemeyeceğini, bu konularda hangi nam altında olursa olsun e-Devlet Kapısı'na karşı hiç bir talep ve iddiada bulunamayacağını ve e-Devlet Kapısı'nın söz konusu işlemlerden doğacak zararlardan herhangi bir sorumluluğunun bulunmadığını gayrikabili rücu olarak kabul, beyan ve taahhüt ederim.

Başvuran kişinin ismi

18.01.2011

--İmza--

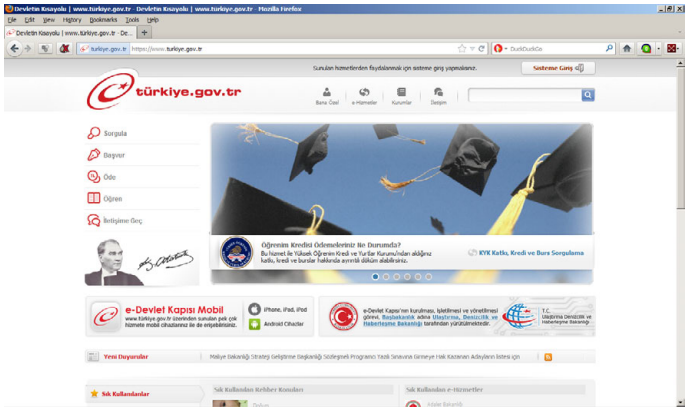
E-devlet Kapısı Taahhütname



E-devlet Şifresi Değiştirme Uyarı Sayfası



E-devlet Şifresi Değiştirme Sayfası



E-devlet Kapısı

dır: kullanıcıların kimlik bilgilerinin görüntülendiği *kişisel bilgilerim ve ayarlarım* bölümü, *mesajlarım* bölümü, *ödemelerim* bölümü, *bilgi paylaşımı* bölümü, kullanıcın e-devlet kapısı arayüzeyinin görünümünü değiştirebileceği *görünüm ayarları* bölümü, kamu kurumlarının listesi, *yardımcı sayfalar* (*yardım merkezi, iletişim, sıkça sorulanlar, mobil devlet, site haritası*) ve son olarak da *güvenlik*, *gizlilik*, *yasal bildirim* ve *hakkımızda* bölümleri bulunmaktadır.

E-devlet kapısı üzeriden verilen hizmetler toplamda 236 devlet kurumunu temsil etmektedir. Bu kurumlardan, 29 kurum entegre olarak E-devlet kapısı içinde hizmet vermektedir. Söz konusu ana kurumlara ait toplam 568 hizmet amaçlı link bulunmaktadır. Bu linklerin dağılımı ise şu şekildedir:

- 480 adet *entegre hizmet* (Bunlar E-devlet kapısı üzerinden vatandaşlara verilen hizmetlerdir),
- 88 adet *e-hizmet* (E-devlet kapısından çıkılarak, söz konusu kuruma ait İnternet sitesi üzerinden sunulan hizmetlerdir). E-hizmet bağlantısı E-devlet kapısı sistemi içerisinde hizmet vermemektedir. Bu linkler sadece kurumların kendi web sayfasına yönlendirmektedir, işlemler ve hizmetler kurumun kendi geliştirdiği sistem üzerinden devam etmektedir. Topografya çalışması sırasında araştırmacı e-hizmet bağlantısına tıkladıktan sonra aşağıdaki uyarıyla karşılaşmıştır: "Şu anda www.türkiye.gov.tr'yi terk ederek (. . .) sitesine gidiyorsunuz. Yönlendirildiğiniz sitedeki hizmet ve içerik ile ilgili E-Devlet Kapısı'nın sorumluluğu bulunmamaktadır. Kabul ediyorsanız Tamam'a tıklayınız. Bu sayfada kalmak için İptal'e basınız."

Yukarıda belirtilen bağlantıların bir kısmı çalışır vaziyette olup, bir kısmı bozuk bağlantılardır. Bozuk olan linklere basıldığında "Yararlanmak istediğiniz hizmet, yaşanan bir teknik aksaklık nedeni ile geçici olarak hizmet dışıdır. Lütfen daha sonra tekrar deneyiniz" ya da "Asal AdresDogrulama1, geçici olarak kullanılamıyor" şeklinde uyarı vermektedir. Bazı linkler ise sadece mobil imza ya da

elektronik imza ile kullanılan linklerdir, bu nedenle söz konusu linklere araştırma sırasında erişilememiştir. Kurumların E-devlet kapısı üzerinden verdikleri elektronik hizmetlerin listesini Ek 1 de bulabilirsiniz.

E-devlet uygulamaları T.C. kimlik numarası üzerinden işlemektedir, bu nedenle Türkiye'de yurttaşın sayısal bedenlenişinin başlıca temsili olan bu numaralar elektronik ortamda stratejik bir öneme sahiptir. Bunun nedeni, yurttaşların çevrimdışı dünyada sahip oldukları kimliklerin çevrimiçi dünya içerisinde de tek bir numaraya (T.C. kimlik numarasına) dönüşmüş olması ve devasa bir kimlik paylaşım sistemi içine "veri" olarak dahil edilmeleridir. Sanal uzamda sayısal veriye dönüşen bu kimlikler çok daha rahat kayıtlanabilir, çoğaltılabilir ya da izlenebilir hale gelmektedir. Kişisel verilerin yasal olmayan şekillerde toplanmasını önlemek ya da dijital gözetimi engellenmek için yüksek güvenlik önlemlerinin alınmasının gerektiğinin bu noktada altını çizelim. Türkiye'de E-devlet uygulamalarında hukuksal boyutta önemli eksikliklerin bulunduğunu da belirtelim. Yurttaşlar E-devlet kapısı üzerinden 29 farklı devlet kurumuyla ilgili elektronik işlem yapabilmektedir. Elektronik ortamda e-Devlet kapısından yürütülen bu işlemlerin temel amacı, devletin kırtasiye masraflarını azaltmak, daha hızlı, verimli ve güvenli bir şekilde hizmet vermek şeklinde açıklanmaktadır (E-devlet kapısı, 2011). Ancak genel olarak tüm E-devlet uygulamalarına bakıldığında yukarıda sayılan bu hedeflerin bazılarına ulaşılamadığı görülmektedir. E-devlet kapısı içerisinde bulunan hizmet amaçlı linklerin %15'inde E-devlet kapısından çıkılarak, kullanıcı diğer devlet kurumlarına ait İnternet sayfalarına yönlendirilmekte ve işlemler kurumun yönettiği İnternet sayfası üzerinden yürütülmektedir[124]. Bu aşamada E-devlet uygulamalarında standartların büyük oranda değiştiği gözlemlenmektedir. Bu noktada E-devlet kapısı uygulamasına ilişkin topografya incelemesinin sonuçlarından yararlanak şu saptamalarda bulunulabilir:

(a) E-devlet kapısından kurumlara ait İnternet sayfasına link verildiğinde, bazı durumlarda kullanıcı doğrudan ilgili e-hizmet sayfasına değil kurumun ana sayfasına yönlendirilmektedir. Bundan ötürü kullanıcı istediği bilgiyi ya da yapmak istediği işlemin bağlantısını tekrardan aramak zorunda kalmaktadır.

(b) Bazı kurumların kendi web sayfalarının görsel olarak karmaşık bir arayüzey tasarımına sahip olmasından dolayı aranan bilgi kolay bulunamamaktadır.

(c) Kurumun İnternet sayfası içerisinde T.C. kimlik numarası ya da bir başka şifrenin girilmesi gerektiğinde sanal klavye uygulamasının bulunmaması ve/veya HTTPS (Güvenli Soket Katmanı) özelliğinin bulunmaması güvenlik açığı oluşturmaktadır.

Sonuç olarak E-devlet kapısı *Bilgi Toplumu Stratejisi ve Eki Eylem Planı* kapsamında hazırlanan *kamu kurumları internet siteleri standartları ve önerileri* içerisinde belirlenen standartlarına uymaktadır. Ancak, diğer kurumların İnternet

[124]Bu oran, E-devlet kapısı topografyasının ilk incelendiği Temmuz 2011 tarihinde %24 oranındaydı.

sayfaları yukarıda belirtilen standartlara uymamakta bu nedenle hızlı, etkin ve güvenli bir iletişim sağlanamamaktadır.

T.C. kimlik numarasının kullanımı sadece devlet kurumları bünyesinde yapılan işlemlerle sınırlı kalmamaktadır. Bir çok firma İnternet üzerinden satış yaparken, üyelik işlemleri sırasında, indirim kartı ya da benzeri uygulamalar esnasında müşterilerinden T.C. kimlik numarası isteyerek kendi kayıtlarını oluşturmaktadır. Bu durum belirli hizmetler satın alındığında daha da önemli bir boyut kazanmaktadır. Ticari kayıtlayıcılar dışında da bir çok kurum ve kuruluş (siyasi partiler, STK'lar, belediyeler, üniversiteler, eczaneler, hastaneler, mağazalar) da bir çok işlem için T.C. kimlik numarası talep etmektedir. Bu konuda bir çok farklı örnek vermek mümkündür:

- Ulaşım alanında, İnternet üzerinde satın alınan biletlerde T.C. kimlik numarası istenmektedir.
- İnternet hosting firmaları, alan adı kaydı, sunucu kiralama gibi bir çok hizmet esnasında T.C. kimlik numarası istemektedir.
- Bankalar, tüm işlemlerini T.C. kimlik üzerinden yürütmektedir, bazı bankalar yurttaşlara cep telefonundan "kredim" ve T.C. kimlik numaralarıyla bankaya mesaj atmaları halinde kefilsiz kredi vermektedir.
- Bir çok süpermarket zinciri müşterilerine verdikleri indirim kartlarında T.C. kimlik numarası talep etmektedir.
- Bazı üniversitelerin kütüphanelerine girmek için kapıda bulunan bilgisayarlara T.C. kimlik numarasının girilmesi şart koşulmaktadır, yanlış TC kimlik numarası girildiğinde, sistem uyarı vermekte ve kapı açılmamaktadır.
- Telefon aboneliği yaptırmak istendiğinde, alt yapıyı kontrol etmek için eve geden görevli, imzalattığı kağıda müşterinin adını, soyadı ve T.C. kimlik numarasını yazıp imzalamasını talep etmektedir.
- Siyasi partiler, parti haberlerinin cep telefonuna gelmesini isteyen yurttaşlardan, kişinin adını soyadı ve T.C. kimlik numarasını cep telefonu mesajı olarak partinin belirttiği telefon numarasına göndermesini istemektedir.
- Kargo firmaları aracılığıyla paket gönderilebilmesi için, müşterilerin firmaya T.C. kimlik numarasını beyan etmeleri gerekmektedir. Kargo firmaları KPS ile entegre olarak çalıştıklarından yanlış T.C. kimlik verildiğinde sistem otomatik olarak bu numarayı reddetmekte ve kargo gönderilememektedir.

E-devlet uygulamaları, öncelikli olarak yurttaşların devlet dairelerindeki işlemlerinin hızlandırılması, vergi işlemlerinin kolaylaştırılması, nüfus bilgilerinin daha kolay tutulabilmesi ve sağlık hizmetlerin daha etkin olarak verilebilmesi için geliştirilmiştir. Ancak günümüzde T.C. kimlik numarası, yurttaşların yapmak istediği her türlü işlem için zorunlu olarak kullanılması gereken bir anahtar haline

gelmiştir. Bu durum kişisel veri olarak, T.C. kimlik numarasının gizliliğinin sağlanmasının önem ve gereğini daha da arttırmıştır. Ancak gerek yasal mevzuattaki boşluklar, gerek denetim mekanizmalarının düzgün işlememesi nedeniyle T.C. kimlik numaraları kişisel veri olarak korunamamakta ve kamusal alanda, özellikle sanal uzamda bir çok farklı yoldan teşhir edilmekte/sergilenmektedir.

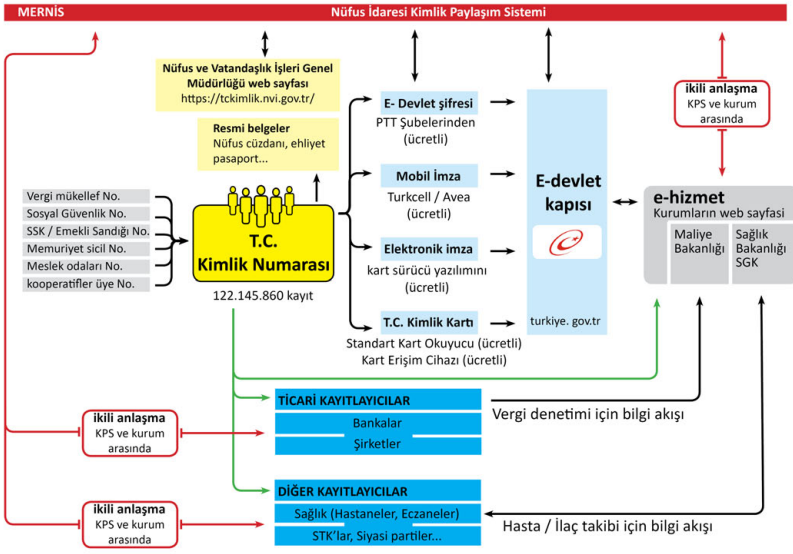
- Örneğin, bazı üniversiteler, öğrencilerinin sınav sonuçlarını isim, soyadı ve T.C. kimlik numaralarıyla birlikte İnternet sayfalarından yayınlamaktadır.

- Örneğin, Emniyet Genel Müdürlüğü Pasaport Hizmetleri Biriminden kargo aracılığıyla başvuru sahiplerine gönderilen pasaportların bulunduğu zarfların üzerinde, başvuru sahibinin adı, soyadı, adresi, cep telefonu, ve T.C. kimlik numarası yazmaktadır. Bu şekilde pasaport alıcıya ulaşana kadar bu kişisel veriler bir çok kişi tarafından görülebilir, okunabilir ve kayıtlanabilir hale gelmektedir.

Sonuç olarak, MERNİS projesi kapsamında geliştirilen ve dağıtılan T.C. kimlik numaraları, aslında bir çok devlet kurumu tarafından yurttaşlara ayrı ayrı numaraların verilmesini önlemek ve tek bir numara üzerinden kamu hizmetleri işlemlerinin yapılabilmesi için geliştirilmiştir. Buradaki asıl amaç, kamu hizmetlerinde işlemlerin hızlandırılması ve daha güvenilir bir hale gelmesini sağlamaktır. Bu bağlamda T.C. kimlik numaralarının paylaşılabilmesi için bu çalışmada daha önce anlatılan, Kimlik Paylaşım Sistemi (KPS) kurulmuştur. KPS birçok kurumu birbirine bağlayan bir alt yapı görevi görmektedir. Ayrıca E-devlet uygulamaları geliştirilmiş ve E-devlet kapısı üzerinden bir çok işlem yapılabilir hale gelmiştir. T.C. kimlik numarasının sanal uzamda kayıtlama hatları üzerinde bu denli entegre olarak işlemesinin ve işletilmesinin sonucunda devlet dışında birçok kayıtlayıcı da (örneğin, ticari kayıtlayıcılar, hastaneler, eczaneler, üniversiteler, siyasi partiler, STK'lar) yurttaşların T.C. kimlik numaralarını toplayan ve kayıtlayan veri bankaları konumuna gelmiştir. Şekil "TC Kimlik Numarası ve E-Devlet Kapısından Veri Eşleştirmesi Topografyası"nda görünen topografya çalışması bu entegre yapıyı en iyi şekilde özetlemektedir.

T.C. kimlik numarası üzerinden bir çok işlemin entegre bir şekilde yapılabilir hale gelmesi, bu sayısal kodun önemini giderek arttırmıştır. Bu bağlamda da bazı temel soruların sorulması gereği ortaya çıkmıştır. Bunları sıralayacak olursak; MERNİS projesiyle kapsamında E-devlet hizmetlerinde kullanılan verilere, kimlerin erişim izni vardır? Bu erişimler nasıl denetlenmektedir? E-devlet kapısı haricindeki kurumların İnternet sayfalarında "Bilgi Toplumu Stratejisi ve Eki Eylem Planı" kapsamında hazırlanan *kamu kurumları internet siteleri standartları ve önerileri* neden uygulanmamaktadır? vb.

E-devlet kapsamı dışında her türlü kurum, ticari firma, STK vd. işlem sırasında T.C. kimlik numarası isteyebilmekte ve kendi veri bankasını oluşturabilmektedir. Bu kurumların İnternet sayfalarından T.C. kimlik numarası dahil olmak üzere kişisel veriler girilirken güvenlik önlemlerinin bulunmaması nedeniyle, bu veriler



TC Kimlik Numarası ve E-Devlet Kapısından Veri Eşleştirmesi Topografyası

işlem anında üçüncü kişiler tarafından izlenebilmektedir. Bu noktada, kullanıcıların verilerinin işlem anında çalınması ya da oluşturulan bu veri bankalarından veri sızdırılmasının olası sonuçları nelerdir; oluşturulan bu veri bankalarına kimlerin erişim izni bulunmakta, bu erişim nasıl denetlenmekte, bu erişimler ne amaçla kullanılmaktadır, yeni soruların da kişisel veri olarak T.C. kimlik numarasının güvenliğinin korunması tartışmasına eklenmesi gerekmektedir.

Bu aşamada Türkiye'de yürütülen uygulamaların denetlenmesine yönelik veya yurttaşların uygulamalar hakkında bilgilendirmesi için gerekli hukuki çerçevenin bulunmaması temel sorunlardan birini oluşturmaktadır. Fransa'da oluşturulan *Ulusal Enformatik ve Özgürlükler Komisyonu*'nun (CNIL - Commission Nationale Informatique et Libertés[125]) bu amaca yönelik iyi bir örnektir. Komisyonun temel amacı yurttaşları özgürlükleri, hakları, sorumlulukları ve alabilecekleri güvenlik önlemleriyle ilgili bilgilendirmeyi hedeflemektedir. Tamamen bağımsız bir yapısı olan komisyon, kişisel verilerin kullanımını denetleme ve düzenleme yetkisine sahiptir (CNIL, 2012).

Yukarıda sıralanan tüm örnekler ve bulguların sonucunda, Türkiye'de sanal uzamda ve bilişim alanındaki uygulamaları insan hak ve özgürlükleri temelinde düzenleyen, yurttaşları bu yönde bilgilendiren özerk ve bağımsız bir kuruma ihtiyaç

[125] CNİL (www.cnil.fr): Fransız hukukundaki enformatik ve özgürlükler yasası kapsamında oluşturulan bağımsız bir komisyondur. Denetim ve cezai yaptırım yetkisine sahiptir. Komisyonun temel amacı gelişen yeni teknolojilerin insan hak ve özgürlüklerini kısıtlamasını engellemektir. Bu bağlamada altı temel misyonu bulunmaktadır: (1) Kişileri hak ve yükümlülükleri hakkında bilgilendirmek, (2) Denetlemek, (3) Düzenlemek, (4) Cezai yaptırımlarda bulunmak, (5) Yurttaşları korumak, (6) Öncülük etmek.

duyulduğunu söyleyebiliriz. Bilişim alanındaki yasaların yetersizliği alanın hukusal boyutta incelenmesini ve yasaların insan hak ve özgürlükleri temelinde düzenlenmesini gerekli kılmaktadır. Çalışmanın bundan sonraki Dördüncü Bölümünde bu sorun hukuki boyutu ile ele alınacaktır.

IV. Bölüm:
TC KİMLİK NUMARASI:

HUKUKSAL BİR DEĞERLENDİRME*

*Kitabın bu bölümü Yrd.Doç.Dr. Elif Küzeci tarafından yazılmıştır.

4.1. Giriş

"Bilme" isteği belki de insanlık tarihinin kendisi kadar eskidir. Bunun bir uzantısı olarak, farklı nedenlerle farklı kişilere yönelik olsa da, eşler, akrabalar, arkadaşlar; cemaat, dernek gibi çeşitli topluluklar ve hem modern öncesi, hem de modern dönemde yöneticiler her zaman diğerlerini bilmeyi istemişlerdir. Daha öncesinde farklı ve sınırlı bir şekilde yaşama geçen bu istek, modern devletin ve modern kapitalist işletmelerin ortaya çıkması ile bir dönüşüme uğrar. Gerçekten bürokratik kollarıyla hüküm sürdüğü toprakların en ücra köşelerine kadar ulaşmayı hedefleyen bu yeni devlet yapılanması, üzerine düşen görevleri yerine getirebilmek için kişisel bilgilere daha önce hiç olmadığı oranda büyük bir gereksinim duyar[126].

Bu gereksinimin tam anlamıyla karşılanmasında ikinci büyük dönüm noktasının ise 1950'li yıllardan itibaren bilgisayarların ve merkezi veri bankalarınn gelişmesiyle yaşandığı söylenebilir. Bu zamandan günümüze, bilişim teknolojileri, kayıtların kolay, ucuz, kapsamlı bir şekilde tutulmasına, işlenmesine ve farklı kaynaklardan toplanan bilgilerin ilişkilendirilmesine olanak tanıyacak şekilde hızla gelişmiştir. Türkiye'de, kamusal tartışma alanlarında ayrıntılı incelemelere konu olmaksızın, uygulamaya geçirilen on bir haneli kimlik numaralarını, bu gelişimi dikkate alarak değerlendirmek gerekir. Nitekim, pek çok farklı kaynaktaki bilgilerin ilişkilendirilmesinde, adeta bir anahtar olan bu numaraya neden ihtiyaç duyulduğunu, kullanımının temel hak ve özgürlükler bakımından ne gibi sorunlar yaratabileceğini ortaya koymadan, Türkiye'de konuya ilişkin hukuksal düzenlemeleri sağlıklı bir şekilde değerlendirebilmek de olanaklı değildir.

Bu nedenle aşağıda öncelikle modern devlet yapılanmasında yurttaşların bilgilerine duyulan gereksinimin nedenleri kısaca açıklanmış, ardından gözetim teknolojilerindeki gelişmeler dolayısıyla duyulan kaygının giderilmesi yönünde hukuksal alanda tanınan güvenceler ana hatlarıyla değerlendirilmiştir. Bu noktada karşımıza çıkan temel alanın "kişisel verilerin korunması" olduğunun altı çizilmelidir. Nitekim aşağıda da görüleceği üzere, devletin kişisel bilgileri elektronik ortama aktarma süreçlerinde uyması gereken temel ilkeler bu kapsamda belirlenmiştir. TC kimlik numaralarının hukuksal alanda değerlendirilmesinde de temel dayanak noktası önemi her geçen gün biraz daha artan kişisel verilerin korunması hakkı olmalıdır.

[126] Modern devletin yurttaşlarını kayıtlamaya duyduğu gereksinim Birinci Bölümde ayrıntılı olarak tartışılmıştır.

4.2. Modern Devletin "Veri Açlığı" ve Hızla Şeffaflaşan Bireyin Hukuksal Kalkanı

16. yüzyılda başlayan ve 20. yüzyılda dünyanın tamamına yayılan bir süreç olarak modernliğin en önemli bileşenlerinden biri kuşkusuz modern devlettir. "Aralarında eşgüdüm sağlanmış çok sayıda görevin hizmetindeki tek bir merkezden gelen bilgiyle harekete geçen ve o merkezce yönetilen bir makine" (Poggi, 2002:119) olarak tasarlanan bu yapı, ilk ortaya çıktığı günden beri hep bilgiye gereksinim duymuştur. Bu, modern toplumda değişimin ve rasyonelliğin kaçınılmaz bir sonucu (Bygrave, 2002:98) olduğu gibi, kural koyma, bunlara uymaya zorlama, düzeni sağlama, vergi toplama, kamu hizmetleri sunma, özel teşebbüsler için sosyal ve ekonomik yapıyı oluşturma, kısaca devletin modern dünyada ticari, diplomatik ve askeri gücünü geliştirme gibi hedeflerinin de bir gereğidir (Whitaker, 1999:40-41; Küzeci, 2010:20-21). Bu hedefler, bilgiye daha önce hiç olmadığı oranda gereksinim duyulmasına neden olmuş ve bilgi toplama kanalları ile bunları değerlendirme teknikleri de her geçen gün biraz daha gelişmiştir. Karşılıklı olarak birbirini besleyen bu iki durum, gözetimdeki farklılaşmayı da beraberinde getirmiş, modern devletin gelişimi ile birlikte merkezi gözetim de güçlenmiş ve yaygınlaşmıştır (Küzeci, 2010:21).

20. yüzyılda bilgisayar teknolojisinin ve merkezi veri bankalarının gelişmesi ise modern devletin "veri açlığı"nın giderilmesinde adeta bir devrim yaratmıştır. 1950'li yıllardan günümüze, devletler yurttaşlarına ilişkin kişisel bilgileri, artan oranda ve hızla, arşivlerin tozlu raflarından bilgisayarların ve ağların dijital koridorlarına aktarmaya başlamıştır. Bu zamana kadar çoğunlukla kişisel güven ilişkisi içerisinde arkadaşa, aileye, hekime aktarılan pek çok bilgi, artık soyut yapılanmalar içerisinde, kimlikleri bilinmeyen kişi ya da kurumlara elektronik ortamda iletilmektedir. Bu kişiler ya da çeşitli sistemler bizleri "veri imge"miz üzerinden kavrarlar (Lyon, 1997:36). Pek çok kaynaktan edinilen bilgileri ilişkilendirebilmek ve "veri imge"leri yaratabilmek için ise sayılara başvurulduğu görülür. Bunun kaçınılmaz sonucu, 21. yüzyıl sakinlerinin artık yalnızca adları ile değil, kendilerini niteleyen pek çok sayı ile tanımlanmasıdır. Kimlik numarası, pasaport numarası, ehliyet numarası, okul numarası, banka hesap numarası, pek çoklarının yanında, yalnızca bir kaç örnektir (Schaar, 2009:98).

Bütün bu gelişmeler, özellikle demokratik toplumlarda haklı bir tedirginliğe neden olur. İnsan onuru, özel yaşamın gizliliği hakkı, bireysel özerklik gibi temel değerler başta olmak üzere, kişiler, hak ve özgürlüklerinin elektronik ortama aktarılan bilgileri dolayısıyla tehlikeye düştüğünü kavrarlar. Bilgisayarların ve veri tabanlarının kişisel bilgileri kayıt etme amaçlı olarak ilk aşamada yalnızca devletler tarafından kullanılması, ilk tepkilerin de devletlere yönelmesine neden olur. Devlet, "büyük birader"e benzetilir ve bireyler dijital kimliklerinin özel yaşamın gizliliği hakkını koruyan kalkanı şeffaflaştırmaması için tepki gösterir. Hemen bu noktada belirtmek gerekir ki, kısa zamanda, "büyük birader" yanında gözetime oldukça istekli "küçük kardeşler" olarak adlandırabileceğimiz özel teşebbüslerin kişisel verileri işleme süreçleri de gözlemlenir ve bireysel şeffaflaşmaya tepki devlet

yanında özel teşebbüslere karşı da gelişir.

Kamusal tepkinin hukuksal düzenlemelere yansıması ilk kez Almanya ve İsveç gibi ülkelerde 1970'li yıllarda görülmüştür. Bu elbette, ne zaman, ne de mekan açısından tesadüftür. II. Dünya Savaşı'na götüren süreç içerisinde tanık olunan ve yönetimin yurttaşlarına ilişkin bilgileri nasıl kullanabileceğini ortaya koyan dehşet verici olayların hatıraları, bu dönemde, henüz tazedir. Avrupa'nın yakın tarihindeki acı tecrübelerin, yurttaşlara ilişkin bilginin, yeni gelişen teknolojiler yardımıyla daha önce görülmeyen ölçüde kolay, ucuz ve hızlı bir şekilde, kaydına, başka bilgiler ile ilişkilendirilmesine ve aktarılmasına olanak tanıyan yeni projeler ile birleşmesi, temel hak ve özgürlüklere yönelik ciddi ve haklı bir tedirginliğin oluşmasına neden olmuştur. Nitekim bu tedirginlik, 1970 yılında Almanya'nın Hessen eyaletinde ilk veri koruması yasasının kabul edilmesini doğrudan etkilemiştir. Bu düzenlemeyi ilk ulusal yasa olan ve 1973 yılında yürürlüğe giren İsveç Veri Koruma Yasası izler. 1980'li yıllara gelindiğinde İngiltere, İrlanda ve İtalya hariç Batı Avrupa devletlerinin hemen hemen tamamında konuya ilişkin yasal düzenlemeler tamamlanmıştır. Ayrıca yeni anayasalarında Portekiz, İspanya, Avusturya, Macaristan gibi ülkelerin kişisel verilerin korunmasını anayasal güvencelere bağladığı da görülür (Early,1993:809-810).

Bu düzenlemeleri uluslararası alanda kabul edilen önemli metinler takip eder. 1980 yılında OECD'nin Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verilerin Sınırötesi Akışının Düzenlenmesine İlişkin Rehber İlkeleri yayınlanmasından kısa bir süre sonra, 1981 yılında Avrupa Konseyi bünyesinde, kısaca AK Veri Koruma Sözleşmesi olarak adlandırabileceğimiz, 108 sayılı Kişisel Verilerin Otomatik Yollarla İşlenmesi Hususunda Bireylerin Korunması Sözleşmesi kabul edilir. 1990 yılında Birleşmiş Milletler'in, 2004 yılında ise APEC'in konuya ilişkin çerçeve nitelikteki ilkeleri belirleyen metinleri yayınlanır. Bütün bu gelişmeler esnasında özellikle 1995 yılından itibaren Avrupa Birliği de önemli yönergeler benimseyerek, üye ülkelerdeki düzenlemelere yol gösterir.

Kısaca özetlemeye çalıştığımız bu süreç içerisinde, konu demokratik devletlerin tamamında tartışma alanına girmiş, büyük bir bölümünde ise yasal düzenlemeler ile olası tehlikeler önlenmeye çalışılmıştır. Kanada, Japonya, Yeni Zelanda, İsrail gibi dünyanın çeşitli bölgelerindeki ülkeler kişisel verilerin korunmasını hukuksal güvencelere bağlamıştır. Bu noktada ayrıca işaret etmek gerekir ki yurttaşların özel yaşamlarına müdahale etmeyi, onları gözetlemeyi ve sürekli takibi yönetim pratiği haline getiren devletlerde kişisel verilerin korunması, hukuksal düzeyde, ya hiç tanınmamıştır ya da mevzuatta yer alan konuya ilişkin hükümler fiilen uygulanmamaktadır.

Türkiye Cumhuriyeti Kimlik Numaralarının değerlendirilmesine geçmeden önce, konunun hukuksal alandaki önemini saptayabilmemizde, belirtilen gelişmeler kapsamında gözlenen birkaç husus bize yardımcı olabilir. Öncelikle kişisel verilerin korunmasına ilişkin ilk ulusal düzenleme olan İsveç Veri Koruma Yasası'nın kabulünde ulusal kimlik numaralarına ilişkin tartışmanın etkili olduğu belirtilmelidir. İsveç'te 1947 yılında her yurttaşa, cinsiyet ve doğum tarihi bilgilerini içeren on haneli bir kimlik numarası verilmesini öngören bir sistemin oluşturulması,

tartışmaları gündeme taşımış; 1960'lı yılların ortalarında nüfus sicili, vergi sicili ve verilerin kaydedileceği ortak bir veri bankasının oluşturulması yönünde çalışmaların başlaması (Bennett, 1992:49-50), hukuksal güvence gerekliliğini açıkça ortaya koymuştur. Görüldüğü gibi kişisel verilerin korunmasının hukuksal düzenlemelerin konusu haline gelmesinde nüfus bilgilerinin merkezi veri bankalarında tutulmasının etkisi bulunmaktadır.

İşaret edilmesi gereken bir diğer önemli gelişme, 1983 yılında Alman Anayasa Mahkemesi'nin verdiği Nüfus Sayımı Kararıdır (BverfGE, 65, 1-Volkszählung). Bu kararda ortaya konan felsefenin hukuksal düzenlemelere etkisi, yalnızca Almanya'da değil, Avusturya, Norveç, Hollanda, Maceristan, Finlandiya gibi ülkelerde de görülmüştür (Jóri, 2007). Bugün halen Alman Anayasa Mahkemesi'nin belirtilen kararda geliştirdiği "bilgilerin geleceğini belirleme hakkı"nın (*informationalle selbst-bestimmung*) konuya ilişkin tartışmalarda bize yol gösterdiğini söyleyebiliriz (Wohlgemuth, Gerloff, 2005:12).

Mahkeme, belirtilen kararında Alman parlamentosunun her iki kanadının oy birliği ile kabul ettiği, ancak devletin "veri açlığı"nı ortaya koyduğu gerekçesi ile yoğun bir şekilde eleştirilen ve bireysel başvuru yolu ile Mahkemenin önünde gelen Nüfus Sayımı Yasasını (Volkszählung Gesetz) Anayasaya aykırı bulmuştur. İptal edilen yasanın yoğun eleştirilere maruz kalmasının nedeni, bu yasa ile nüfus sayımı sırasında yurttaşlara bazı bilgilerin açıklanması yükümlülüğünün getirilmesidir (Simitis,184:398-405). Anayasa Mahkemesi yaptığı inceleme neticesinde yasanın dayanağı olan gerekçeleri tek tek çürütmüş, devletin kişisel verilerle olan ilişkisini ayrıntılı bir şekilde resmetmiş ve Anayasanın 1/1 ve 2/1 madde hükümlerini bir arada değerlendirerek, "*bilgilerin geleceğini belirleme hakkı*"nı (*informationalle Selbstbestimmung*) türetmiştir. Hemen belirtelim Federal Almanya Cumhuriyeti Anayasası'nın karara dayanak olan hükümleri şöyledir: "İnsan onuru dokunulmazdır. Tüm devlet güçleri ona saygı göstermek ve onu korumakla yükümlüdür"(m.1/1); "Herkes başkalarının haklarını ihlal etmemek, Anayasal düzene veya ahlak kurallarına aykırı düşmemek koşuluyla kişiliğini serbestçe geliştirme hakkına sahiptir"(m.2/1). Görüldüğü gibi mahkemenin kararı temel olarak "insan onuru" ve "kişiliğin korunması" ilkelerine dayanmaktadır. Bu ilkeler, pek çok demokratik devletin temel prensipleri arasında yer alır. Türkiye Cumhuriyeti Anayasasının da Başlangıç 6. Paragrafında ve 17/1 hükmünde kişinin maddi ve manevi varlığını geliştirme ve koruma hakkı tanınmış, ayrıca Anayasanın 5. Maddesinde "Devletin temel amaç ve görevleri" arasında "insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak" düzenlenmiştir. İnsan onuru, ise kişinin maddi ve manevi varlığını geliştirme hakkı yanında, diğer hak ve özgürlüklerin de ortak temelini oluşturur (Kaboğlu,2002:25). Nitekim Alman Anayasa Mahkemesi de bu duruma işaret etmiştir. Mahkemeye göre, anayasal düzenin merkezinde toplumun özgür bir üyesi olan kişinin onuru bulunur. Son dönemde görülen teknik gelişmeler ve buna bağlı olarak ortaya çıkan tehlikeler karşısında kişiliğin korunması ise özel bir önem kazanmaktadır. Kendisine ilişkin hangi bilgilerin edinildiğini, bu bilgilerin kimler tarafından kullanıldığını bilmeyen kişinin kararlarını özgürce verebilme olanağı zarar görür. Özellikle otomatik araçlar ile verilerin sınırsız bir şekilde kaydedilebilmesi, bunlara

kolaylıkla ulaşılabilmesi ve kişinin ayrıntılı profillerinin çıkarılabilmesi ciddi bir tehlike olarak ortaya çıkmaktadır. Bunun sonucunda kişinin psikolojik baskı hissetmesi ve kamusal yaşama katılımının etkilenmesi olanaklıdır. Nitekim sürekli kayıt altına alındığını ve bundan dolayı çeşitli mağduriyetler yaşayacağını düşünen kişi, çeşitli kamusal haklarını kullanmaktan vazgeçebilir. Bu kişinin, toplumsal yaşamda kişiliğini özgürce belirleyememesi, kendinden beklenen davranış tarzına göre hareket etmesi de olasıdır. Bu durum, yalnızca bireyin kendi kişiliğini geliştirme hakkını zedelemekle de kalmaz, ayrıca kamu çıkarlarına da zarar verir, çünkü özgürlükçü bir demokrasinin işlemesi topluma katılma ve toplum içerisinde işlev görme becerisine bağlıdır. Bu nedenle, kişiliğin serbestçe gelişebilmesi ve demokratik toplum yapısının sürekliliği için devlet tarafından kişisel verilerinin toplanılması, kaydedilmesi, kullanılması ve devredilmesi karşısında bireyin korunması bir gerekliliktir. Ayrıca yaşam ilişkilerinin açığa çıkacağı zamana ve bunun sınırına da kişi kendisi karar vermelidir. Nitekim bilgilerin geleceğini belirleme hakkı, ilke olarak bireyin kendi kişisel verileri üzerinde karar verme hakkını tanır (BverfGE 65,1,42 vd; Gola,Schomerus,2007,77; Küzeci, 68).

Bunun yanında Alman Anayasa Mahkemesinin işaret ettiği önemli hususlardan bir diğeri, verilerin işlenmesi sırasında çeşitli kaynaklardan edinilen bilgilerin ilişkilendirilebilmesi sebebiyle, ilk aşamada önemsiz gibi görülen verilerden hareketle kişinin davranış tarzının belirlenmesinin olanaklı olduğudur. Buna göre kişiye ilişkin bilgilerin önemli ya da önemsiz olarak ayırmak yanıltıcı olacaktır. Nitekim başka bilgilerle bağlantı kurularak yeni veriler yaratılması her zaman olanaklıdır (BverfGE 65,1,45;Şimşek,2008:116). Son olarak Alman Anayasa Mahkemesi'nin çeşitli kararlarında işaret ettiği "obje formülü"ne deyinmemiz konumuz açısından yararlı olabilir. Mahkemeye göre, eğer insan kamusal organların etkinlikleri karşısında basit bir obje, ya da başka bir anlatımla bir araç haline indirgeniyorsa insan onurunun ihlali söz konusu olur. Devletin insanın kişiliğini kayıt altına alması da bu bağlamda incelenmelidir (BverfGE 45,187; Şimşek,2008:130).

Bu hususlar, kanımızca, kimlik numaralarının hukuksal değerlendirilmesinde de mutlaka dikkate alınmalıdır. Nitekim TC kimlik numarası aracılığıyla kişilere ilişkin pek çok bilginin ilişkilendirilmesi ve değerlendirilmesi mümkündür. İlk başta önemsiz gibi görülen bilgilerin, başkaları ile bağlantısının kurulmasının ardından, temelde insan onurunun ve ayrıca özel yaşamın gizliliği hakkının zarar görmesi söz konusu olabilir. Bu ilişkilendirmeler sırasında kişinin bilgileri ile arasındaki bağlantının kopması, bilgilerinin nasıl kullanıldığını öğrenme olanağının bulunmaması, bilgilerin işlenmesinde hakim olacak temel ilkelerin belirlenmemesi ise kamusal otoritelerin karşısında özneden nesneye doğru evrilmesi tehlikesini beraberinde getirecektir.

Bu noktada kişisel verilerin korunmasının ve bilgilerin geleceğini belirleme hakkının, yurttaşın kişilik haklarının korunması ile resmi makamların ve işletmelerin bilgilendirilmesi arasında bir denge unsuru olduğu da belirtilmelidir (Creifelds ve diğ.,1997:277). Bir başka anlatımla, bilgilerin geleceğini belirleme hakkı, ilgilinin kişisel verileri üzerinde sınırsız bir hakka sahip olduğu anlamına gelmez. Ancak sınırlamalar yalnızca belirli durumlarda söz konusu olmalı ve mutlaka yasal temele

dayanmalıdır. Bu sınırlamaların koşulları ve kapsamı yurttaş için açık ve anlaşılır bir şekilde saptanmalı ve temel haklar rejiminin ilkelerine uyulmalıdır (Gola, Schomerus,2007:78).

Türkiye'de ulusal kimlik numarası özelinde kişisel verilerin korunmasının hukuksal temellerine ilişkin incelemelere geçmeden önce, son olarak konunun Almanya dışında çeşitli ülkelerde de Anayasa Mahkemesinin önüne geldiğini belirtmek isteriz. 1998 yılında Filipinler Supreme Court'unun ulusal kimlik sisteminin, 1991 yılında ise Macaristan Anayasa Mahkemesinin çok amaçlı kullanım için tasarlanan bireysel kimlik kartının anayasalarının özel yaşamın gizliliği hakkına ilişkin hükümlerini ihlal ettiği yönünde kararları burada örnek olarak gösterilebilir. Ayrıca 1997 Portekiz Anayasasında çok amaçlı ulusal kimlik numarası kullanımı yasaklayan bir hükmün bulunması da konuya ilişkin dikkat çekici bir başka örneği oluşturur(EPIC-Privacy and Human Rights Report 2006).

4.3. Elektronik Devlet, Sayısallaştırılmış Yurttaş

Devletin, modern yapılanma içerisinde üzerine düşen görevleri yerine getirmek üzere, yurttaşa ilişkin bilgileri, toplaması, kayıt etmesi ve kullanması yaşamının tamamını kapsar ve hatta denilebilir ki, doğumundan önce başlayıp ölümünden sonra da bir süre daha devam eder. Bu niteliğiyle devletin, özel teşebbüsler gibi güçlü rakipleri bulunmasına karşın, halen en büyük bilgi tekeline sahip olduğu söylenebilir. Bu, devletin en temel görevlerin biri olan ve en genel şekliyle "*(s)iyasal organlar tarafından kamuya yararlı kabul edilen, bir kamu kuruluşunun ya kendisi ya da yakın denetimi ve gözetimi altında özel kesim tarafından yürütülen faaliyetler*" olarak tanımlanabilecek kamu hizmetinin (Günday, 269) yerine getirilebilmesi için önemli bir gerekliliktir. Yukarıda da işaret ettiğimiz gibi idarenin kişisel bilgilere gereksinim duymasında modern devletin ortaya çıkması ve gelişmesi adeta bir dönüm noktası olmuş, ikinci büyük değişim ise teknolojideki gelişim sonucunda yaşanmıştır. Teknolojideki gelişim, bir sonraki aşamada, elektronik devlet olarak ifade edilen yeni bir projenin gündeme gelmesine neden olur. Gerçekten ülkemizde de özellikle 2000'li yıllardan itibaren tartışma ve uygulama alanına giren "elektronik devlet" kamu hizmetlerinde önemli bir değişimin habercisidir (Arifoğlu, 2004). Bu noktada TC kimlik numaralarını da kapsayan pek çok önemli uygulamanın Türkiye'de e-devlet projelerinin bir parçası olarak geliştiğini belirtmek gerekir.

Elektronik devlet, ya da kısaca e-devlet, yurttaşlara devlet tarafından sunulan hizmetlerin elektronik ortama taşınmasını ifade eden ve devlet hizmetlerinin yurttaşa kolay ve etkin yoldan, kaliteli, hızlı, kesintisiz ve güvenli bir şekilde ulaştırılmasını hedefleyen bir proje olarak tanımlanabilir. Bu ortamda kamu kuruluşları, özel sektör ve yurttaşlardan oluşan üç unsur buluşturulmaktadır.

Üçüncü Bölümde de serimlendiği üzere e-devlet uygulamalarının oldukça geniş bir alana yayıldığı söylenebilir. Türkiye'de e-devlet projesinin önemli ayaklarından biri olan ve bütün kamu hizmetlerine tek bir noktadan erişim olanağı sağlayan

bir İnternet sitesi olarak kurgulanan e-devlet kapısı (http://www.turkiye.gov.tr) 18 Aralık 2008 günü açılmıştır. Kapı'nın amacı kamu hizmetlerini, vatandaşlara, işletmelere, kamu kurumlarına bilgi ve iletişim teknolojileriyle etkin ve verimli bir şekilde sunmak ve bürokrasinin hantal kolları arasından sıkışmış bireyi biraz olsun rahatlatmaktır. Bunun yanında Merkezi Nüfus İdaresi Sistemi (MERNİS), Kimlik Paylaşım Sistemi, Vergi Daireleri Otomasyonu Projesi (VEDOP I-II), Ulusal Yargı Ağı Projesi (UYAP), Gümrük İdaresinin Modernizasyonu Projesi (GİMOP), Polis Bilgi Ağı (POLNET), Saymanlık Otomasyon Sistemi (Say2000i), e-Bildirge ve Başbakanlık Mevzuat Bilgi Sistemi yaygın olarak hizmet veren başlıca e-devlet uygulamaları arasında sayılabilir. Bu uygulamalar içerisinde konumuz açısından merkezi öneme sahip olan MERNİS projesidir. Bu proje, "*tüm Ahvali Şahsiye bilgilerini elektronik ortama aktaran ve Ahval-i Şahsiye bilgilerinde meydana gelen her tür değişikliğin ülkenin her tarafına dağılmış 957 merkezden anlık güncellenmesini ve bir ağ üzerinden güvenle paylaşımını*" sağlamak üzere geliştirilmiştir (http://www.nvi.gov.tr) ve e-devlet çalışmalarının en önemli bileşeni olarak kabul edilebilir. Öte yandan bu sistemin kişisel verilerin korunmasında hakim olan temel ilkelerle uyumlu bir şekilde işlemesi son derece önemlidir. Üçüncü Bölümde sunulan topografya çalışmasında ortaya konduğu üzere böylesine bir merkezi nüfus sistemi çerçevesinde önemli kişisel verilerin işlendiği açıktır. Ayrıca, yukarıda da belirttiğimiz gibi, ilk kişisel veri koruma yasalarının kabulünde benzeri merkezi nüfus sistemlerinin yaratabileceği olası tehlikeden korunma düşüncesi etkili olmuştur. 1972 yılından beri süren bir çalışmanın ürünü olan MERNİS, 2006 yılında yeni Nüfus Hizmetleri Kanununun (kanun no.5490, t. 25 Nisan 2006; RG. t. 29 Nisan 2006, S. 26153) kabulü ile tam olarak uygulamaya geçmiştir. Yasanın uygulamasını göstermek için, kısa bir süre sonra, Nüfus Hizmetleri Kanununun Uygulanmasına İlişkin Yönetmelik (Bakanlar Kurulu Kararı t. 29 Eylül 2006, S. 2006/11081, RG. t. 23/11/2006, S. 26355) yürürlüğe girmiştir.

Yasa uyarınca MERNİS, "*Merkezî veri tabanı ve Kimlik Paylaşımı Sistemini de kapsayan Merkezî Nüfus İdaresi Sistemini*" ifade eder(m.3/n). Buradan çıkarılacak sonuç, merkezi veri tabanı ve kimlik paylaşım sisteminin MERNİS'in temel iki bileşeni olduğudur. Yasaya göre merkezi veri tabanı, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünde elektronik ortamda tutulan aile kütüğü kayıtlarını; kimlik paylaşım sistemi ise "*Genel Müdürlükçe merkezî veri tabanından ayrı olarak elektronik ortamda tutulan, Kimlik Paylaşımı Sisteminden yararlanacak kurumların istifadesine sunulan ve sınırlandırılmış bilgiler ihtiva eden aile kütüğü kayıtlarını*" ifade eder(m.3/k,m). MERNİS'in temel hedefi ağır ve aksak işleyen bürokrasiye ilişkin bazı sorunların giderilmesidir. Nitekim MERNİS'in amaçları arasında doğru, hızlı ve verimli hizmet sunmak yer alır. Bu kapsamda nüfus kayıtlarına ilişkin yanlışlıklar ve bu yanlışlıklar ile ilgili sorunların giderilmesi de merkezi önemdedir. Bu türdeki uygulamaların yaygınlaşmasının pek çok yararı olduğu açıktır. Her şeyden önce maliyet ve zaman tasarrufu sağlanacağı düşünülmektedir. Gerçi belirtmek gerekir ki MERNİS uygulamaya geçtikten sonra da hedeflenen sorunlar tam anlamıyla çözülememiştir. Sistem uygulamaya geçtikten kısa bir süre sonra, MERNİS'te yurttaşların T.C. kimlik bilgilerinin yüzde yirmi beşinin hatalı olduğunun belirlendiğine ilişkin haberler bunun göstergesi olarak kabul

edilebilir ("Mernis Skandalı", Milliyet, 11 Aralık 2006). Diğer yandan MERNİS kapsamında her yurttaşa on bir haneli T.C. kimlik numarası verilmesi ile isim benzerliğinden dolayı ortaya çıkan aksaklıkları gidermek ve kamu kuruluşları arasındaki bilgi alışverişini hızlandırmak da hedeflenmiştir[127].

MERNİS öncesinde de Türkiye'de çeşitli veri tabanlarında kişilere ilişkin bilgiler tutulmaktaydı. Bu projeyi önemli kılan ise birbirinden farklı veri tabanlarındaki bilgilere tek yerden ulaşma olanağı sağlamasıdır. Ancak kişisel verilerin korunmasına yönelik ilkeler belirlenmeden böyle bir sistemin uygulamaya geçmesi ciddi tehlikelerin ortaya çıkmasına neden olabilir. Federal Almanya Anayasa Mahkemesinin yukarıda da işaret edilen Nüfus Sayımı kararında da belirtildiği gibi, veriler arasında ilişki kurabilme olanağından dolayı, ilk başta önemsiz gibi görülen bilgilerden hareketle ayrıntılı kişilik profilleri çıkarılabilir. Bu noktada sistem üzerinde ne tür bilgilerin tutulduğuna kısaca değinmek gerekir. Kimlik Paylaşımı Sistemi Uygulama Yönetmeliği'nin (İçişleri Bakanlığından, RG. t. 10 Temmuz 2005; S. 25871) 8. Maddesi uyarınca bu sistemde toplanan bilgiler şöyle gruplanabilir:

- Kişi bilgileri: Kimlik numarası, adı, soyadı, kızlık soyadı, cinsiyeti, baba adı, anne adı, doğum yeri, doğum ve kütüğe kayıt tarihleri gibi kişisel bilgiler; medeni hali, dini ve ölüm tarihi gibi durum bilgileri; İl, ilçe, cilt, mahalle veya köy, aile sıra numarası ve birey sıra numarası gibi nüfusa kayıtlı olduğu yer bilgileri.

- Nüfus Cüzdanı Bilgileri: Nüfus cüzdanı üzerinde yer alan bilgiler, 1 Haziran 2000 tarihinden sonra düzenlenen cüzdanlarda seri ve numarası ile verildiği yer ve tarihi, 1 Haziran 2000 tarihinden önce düzenlenmiş cüzdanlarda cüzdan seri, no ve verildiği maliye saymanlığının adı.

- Nüfus Olay Bilgileri: evlenme, boşanma, soybağının düzeltilmesi veya reddi, ölüm, vatandaşlığın kazanılması veya kaybedilmesi gibi kişilere ait nüfus olay bilgilerinin tarihi ve açıklamaları.

- İstatistik Bilgileri: Doğum, ölüm, evlenme, boşanma sayıları gibi bilgiler.

Görüldüğü gibi sistem içerisinde oldukça kapsamlı bilgiler tutulmaktadır.

[127] Nitekim T.C. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün resmi İnternet sitesinde (http://www.nvi.gov.tr) MERNİS projesinin hedefleri şöyle belirlenmiştir: "(i)Nüfus kütükleri üzerinde tam bir denetim kurmak ve nüfus kütüklerini güvenilir belgeler haline getirerek hizmette sürat ve verimlilik sağlamak; (ii) Merkezde bir bilgi bankası oluşturmak ve bu yoldan nüfus kütüklerindeki bilgileri kamu hizmetleri açısından değerlendirmek; (iii) Nüfus kütüklerindeki bilgileri istatistik verileri olarak değerlendirerek, nüfus ve aile istatistiklerini elde etmek; (iv) Her vatandaşa bir Türkiye Cumhuriyeti kimlik numarası vermek suretiyle isim benzerliğinden dolayı ortaya çıkan aksaklıkları gidermek ve kamu kuruluşları arasındaki bilgi alışverişini hızlandırmak; (v) Mevcut nüfus cüzdanlarını dünya standartlarına uygun şekilde kart şeklinde nüfus cüzdanlarına dönüştürmek". Ayrıca yasanın Geçici 1. maddesi uyarınca "(k)urumlar ve tüzel kişiler bu Kanunun yayımı tarihinden itibaren iki yıl içinde mevzuatlarını bu Kanun hükümlerine uygun hale getirerek işlemlerinde kimlik numarasını kullanmak zorundadırlar".

Bunlar arasında kişinin dini gibi, hassas nitelikteki kişisel veriler de bulunmaktadır. Hemen hatırlatalım, aile kütüklerinde ve nüfus cüzdanlarında din hanesinin bulunma zorunluluğu 1587 sayılı eski Nüfus Kanununda da bulunmaktaydı ve yoğun şekilde eleştirilen bu hüküm, kanunun yürürlüğü sırasında iki kez Anayasa Mahkemesi'nin önüne götürülmüştü. Ancak her iki başvuru neticesinde verdiği kararda da Mahkeme, bu zorunluluğu din ve vicdan özgürlüğüne aykırı görmemiştir(AYMK, E. 1979/9, K.1979/44, t. 27 Kasım 1979; AYMK, E. 1995/17, K.1995/16, t. 21 Haziran 1995). Kanımızca belirtilen hüküm Anayasa'ya aykırıdır. Nitekim Anayasanın kimsenin dini inanç ve kanaatlerini açıklamaya zorlanamayacağı hükmü karşısında, dinin ne olduğunu açıklamanın yasal zorunluluğa bağlanması din özgürlüğünü zedeleyecektir. Bunun yanında kişinin dini inancı sağlık bilgileri, etnik köken, cinsel yaşam gibi oldukça hassas nitelikteki bilgilerdendir. Kişisel verilerin korunmasını ulusal hukuklarının bir parçası haline getirmiş ülkelerin önemli bir bölümünde bu türdeki bilgiler özel bir koruma rejimine tabidir. Ayrıca dini inanca ilişkin bilgiler özelinde baktığımızda bu bilginin kayıt altına alınmasının makul bir yararı olmadığı gibi, kötüye kullanımının ciddi sakıncalara neden olabileceği de açıktır. 5490 sayılı Nüfus Hizmetleri Kanunu yürürlüğe girmeden önce de söz konusu olan bu tartışmalar, MERNİS projesinin uygulamaya geçmesiyle kanımızca daha da ciddi bir boyuta taşınmıştır. Nitekim artık Kimlik Paylaşım Sistemi kapsamında yer alan bu bilgilere daha fazla sayıda kişinin daha kolay ulaşabilmesi ve bu bilgilerin başka kaynaklardan edinilen bilgiler ile ilişkilendirilebilmesi olanaklıdır. Ayrıca belirtmek gerekir ki nüfus cüzdanlarından din hanesinin çıkarılması 2000 yılında MERNİS projesinin ve daha sonra 2006 yılında yürürlüğe giren yeni Nüfus Hizmetleri Kanununun hazırlanma sürecinde gündeme gelmiş, ancak bu yaklaşım benimsenmemiştir (Esen, Gönenç, 2008: 584-587). Günümüz temel hak ve özgürlükler anlayışında bu uygulama, kabul edilemez bir nitelik taşır. Kaldı ki kişisel verilerin korunmasına ilişkin standartların henüz belirlenmediği bir ortamda ortaya çıkabilecek tehlikenin boyutu da artmaktadır.

4.4. "Ben" ya da On Bir Hanelik Kimlik Numaram...

E-devlet projelerinin önemli bir ayağını oluşturan Türkiye Cumhuriyeti kimlik numarasının hukuksal temelini 5490 sayılı Nüfus Hizmetleri Kanununun 46 ve 47. Maddelerinde bulduğunu görüyoruz. Yasanın "Kimlik numarası" kenar başlıklı 46. Maddesi şu hükmü içerir:

> "(1) Kimlik numarası, Türkiye Cumhuriyeti vatandaşlarının nüfus kayıtları arasında bağ kurmak, kişilerin kaydına ulaşmak ve kamu kuruluşlarında tutulan kayıtlar arasında ilişki sağlamak amacını taşıyan bir numara sistemidir. Türkiye Cumhuriyeti kimlik numarası kişiye bir defa verilir ve değiştirilemez. (2) Türkiye'de kaydı tutulan yabancılara da Bakanlığın tespit edeceği esaslar içerisinde bir kimlik

numarası verilir".

Görüldüğü gibi TC kimlik numarası sistemine geçilmesinin temel amacı yurttaşların "nüfus kayıtları arasında bağ kurmak, kişilerin kaydına ulaşmak ve kamu kuruluşlarında tutulan kayıtlar arasında ilişki sağlamak"tır. Bir başka anlatımla her bir Türkiye Cumhuriyeti yurttaşına bir kez verilen ve değiştirilemeyen on bir haneli TC kimlik numarası çeşitli kayıtlarda adeta onu niteler şekilde, onun adının yerine kullanılan ve farklı kayıtlar arasında ilişki kurmaya yarayan bir anahtardır. TC kimlik numarası aracılığıyla ilişkilendirilen bilgilerin ne kadar çeşitli olduğu numaranın kullanımına ilişkin hususları düzenleyen 47. Maddenin ifadesinden açıkça anlaşılmaktadır. Belirtilen hükme göre:

> "(1) Kişiler adına düzenlenecek olan her türlü form, beyanname, kimlik kartı, vergi kimlik kartı, sürücü belgesi, pasaport gibi bütün tanıtıcı belgelerde Türkiye Cumhuriyeti kimlik numarasına yer verilir. (2) Türkiye Cumhuriyeti kimlik numarası kurumlar ile diğer gerçek ve tüzel kişilerin her türlü işlem ve kayıtlarında esas alınır. (3) Kimlik numarasının uygulanmasında ortaya çıkan sorunlar ile tereddüt edilen hususlarda Genel Müdürlüğün görüşü alınır".

Böylelikle kimlik numarasının kullanım zorunluluğu oldukça geniş bir alanı kapsar şekilde belirlenmiştir. Bu noktada kişisel verilerin korunması açısından bir değerlendirme yapmak gerekir. Nitekim, yukarıda da belirtildiği gibi, kişisel verilerin korunmasının hukuksal düzenlemelerin konusu olmasının önemli nedenlerinden biri de gelişen teknoloji sayesinde pek çok farklı yerde tutulan bilginin ilişkilendirilebilir hale gelmesidir. TC kimlik numarasının sağlık hizmetinden, vergilendirmeye kadar kamuyla yapılan her türlü işlemde esas alınacağını unutmamak gerekir.

Hemen belirtelim TC kimlik numarasının kullanıldığı her durumda kişisel veri oluşmaktadır. Bu, her şeyden önce kimlik numarasının kendisinin kişisel veri olmasından kaynaklanır. Nitekim kişisel verinin genel kabul gören karşılığı "belirli ya da belirlenebilir bir kişiye ilişkin her türlü bilgi"dir. Herhangi bir işlemde kimlik numarasına yer verilmesi, doğrudan ilgili kişiyi belirlenebilir kılacağından "kişisel veri"nin söz konusu olması kaçınılmazdır. Ayrıca, aşağıda üzerinde durulacak olan, Kişisel Verilerin Korunması Kanun Tasarısının gerekçesinde de TC kimlik numarasının kişisel veri niteliğinde olduğuna açıkça yer verilmiştir. O halde TC kimlik numarasının kullanıldığı durumlarda kişisel verilerin korunmasında hakim olan temel ilkelere uygun hareket edilmelidir.

Buna göre kişisel verilerin korunmasına yönelik uluslararası metinlerde ve çeşitli ulusal düzenlemelerde kabul edilen ilkelerin başlıcaları şöyle sıralanabilir (Bkz. 95/46/AT sayılı AB Yönergesi, m. 6; 108 sayılı AK Sözleşmesi, m. 5, BM Rehber İlkeleri par. 1,3, OECD Rehber İlkeleri, par. 7,9, APEC Çerçeve Belge, par. 18.:

Kişisel veriler;

- hukuka ve dürüstlük kurallarına uygun işlenmeli,

- belirli, açık ve meşru amaçlar için toplanmalı,
- toplanma ve daha sonra işlenme amaçlarına uygun, ilgili bulunmalı ve aşırı olmamalı,
- doğru ve eğer gerekli ise güncel tutulmalı,
- amacın gerektirdiğinden daha uzun süre tutulmamalıdır.

Ayrıca kişisel verilerin ancak yasadan kaynaklanan durumlarda veya ilgilinin rızasının bulunması halinde üçüncü kişilere aktarılabileceği de genel kabul gören temel bir ilkedir. Böylece kişisel verilerin açıklanmasına bir sınırlama getirildiği belirtilmelidir (AB Yönergesi, m.6,7,8; 108 sayılı AK Sözleşmesi, m. 5,6; OECD Rehber İlkeleri, par. 10). Bu, oldukça önemlidir. Nitekim meşru amaçlarla toplanmış ve kayıt edilmiş kişisel bilgilerin başkaları ile paylaşılmasına herhangi bir sınırlama getirilmemesi, bu ilkeleri uygulamada anlamsız kılacaktır.

Türkiye'de ise, kısaca belirtilen temel ilkeler açısından, hukuksal alanda ciddi bir eksikliğin bulunduğu dikkat çekmektedir. Gerçi bu konuda ülkemizde de çalışmalar yapılmaktadır. Ancak kişisel verilerin korunmasıyla ilgili çerçeve nitelikte ve kapsayıcı bir yasa hâlâ mevcut değildir. Kişisel Verilerin Korunması Kanun Tasarısı ise, TBMM'de ilgili komisyonun önünde beklemektedir. Tasarının metni kaleme alınırken temel olarak 95/46/AT sayılı AB Yönergesinden yararlanıldığını belirtmek gerekir. Bunun yanında 108 sayılı AK Sözleşmesi, Türkiye tarafından 28 Ocak 1981 tarihinde imzalanmış olmasına karşın, konuya ilişkin yasal düzenleme henüz yapılmadığından, onaylama işlemi tamamlanamamakta, dolayısıyla bağlayıcı sonuçları hukuk sistemimiz açısından söz konusu olamamaktadır.

Buna karşın, özellikle son dönemde çıkarılan yasalarda kişisel verilerin korunmasına yer verildiği görülmektedir. Türk Ceza Kanununun (TCK) ilgili hükümleri (m. 135 vd.) bunun en açık örneğidir. Gerçekten yeni TCK'nın 135. maddesi "kişisel verilerin kaydedilmesi"ne, 136. maddesi "verileri hukuka aykırı olarak verme, yayma veya ele geçirme"ye, 138. maddesi ise "verileri yok etmeme"ye ilişkin kuralları ceza hukuku açısından düzenlemektedir. TCK'nın "Özel hayata ve hayatın gizli alanına karşı suçlar" başlıklı dokuzuncu bölümünde düzenlenen bu hükümler mevzuatımızda kişisel verilerin korunmasına yönelik en önemli düzenlemeleri oluşturmaktadır. TCK'nın 135. Maddesi uyarınca:

> "(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir. (2) Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır".

136. Madde hükmü ise şu düzenlemeyi getirmektedir:

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

Görüldüğü gibi TCK uyarınca yalnızca kişisel verileri "hukuka aykırı olarak kaydetme" değil, bunun yanında kişisel verileri hukuka aykırı olarak başkalarına iletme, yayma ya da bunları ele geçirme de suç olarak düzenlenmiştir. Bu yaklaşım yukarıda işaret ettiğimiz kişisel verilerin korunmasına yönelik temel ilkeler ile uyumludur. Bununla birlikte hükümlerin uygulama alanının belirlenmesi ancak "kişisel veri" kavramının açıkça tanımlanması ile olanaklıdır. Bu noktada çerçeve bir yasanın gerekliliğine bir kez daha dikkat çekmek gerekir. Öte yandan TC kimlik numarası özelinde konuya yaklaştığımızda bu numaranın ve onunla ilişkili tutulan diğer bilgilerin kişisel veri olup olmadığı hususunda herhangi bir tereddütün bulunmadığını bir kez daha belirtmeliyiz. Dolayısıyla hukuka aykırı olarak TC kimlik numarasını kayıt eden, başkalarına veren, yayan ya da ele geçiren veya kanunlarda belirtilen sürelerin geçmesine karşın TC kimlik numarası ile ilişkili kayıtları yok etmeyen kişi, TCK'nın belirtilen hükümleri çerçevesinde ceza yaptırımı ile karşılaşabilir.

TCK'nın ilgili hükümleri yanında konuyla doğrudan ilişkili olmayan bazı temel metinlerde de kişisel verilerin korunmasına yönelik güvencelerin bulunduğu belirtilmelidir. Bu kapsamda Türk Medeni Kanunu'nunda (MK) sınırlı da olsa kişisel verilerin korunmasına yönelik bazı hükümlerin bulunduğu söylenebilir. Bu bağlamda, örneğin MK'nın 24-25. maddelerinde ve Borçlar Kanununun 49. maddesinde kişinin gizli alanına sızarak sırlarını öğrenme, teknik aygıt ve araçlarla kaydetme, resmini, filmini çekme, ayrıca bunları aktarma ve yayma gibi, kişilik haklarına yönelik saldırılara karşı koruyucu hükümler yer almaktadır. Ayrıca yeni Borçlar Kanunu (BK) işçinin kişisel verilerinin korunmasına yönelik bir hüküm öngörmektedir. 1 Temmuz 2012 tarihinde yürürlüğe girecek yeni BK'nın Hizmet Sözleşmesine ilişkin altıncı bölümünde yer alan 419. maddesi uyarınca;

> "(1)İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. (2)Özel kanun hükümleri saklıdır".

Bu noktada belirtilen hükümler çerçevesinde korumanın sınırlı kaldığını belirtmeliyiz. Bunun temel nedeni ise yine kişisel verilerin korunmasına yönelik çerçeve bir yasanının bulunmamasıdır. Örneğin Türkiye'de medeni hukuk alanındaki önemli etkisi açık olan İsviçre Medeni Kanunu'nda hemen hemen aynı düzenlemeye yer verilmiş olmasına karşın, İsviçre'de ayrıca bir kişisel verilerin korunması yasasının da kabul edilmesinin nedeni budur. Kişisel verilerin korunması yasaları MK, BK gibi temel metinler ile karşılanamayan bir korumayı getirmekte, bir anlamda onları tamamlamaktadır. Bu nedenledir ki İsviçre, Almanya gibi medeni hukuk sistemimizi yakından etkileyen ülkelerde kişilik haklarına ilişkin açıklamalarda kişisel verilerin korunmasına sıklıkla atıfta bulunulmaktadır (Münchener Kommentar zum Bürgerlichen Gesetzbuch, 2001:267-268). Temel hukuksal

metinler yanında kişisel verilerin korunmasına ilişkin bir yasanın gerekliliği, böylesine bir düzenlemenin konuya ilişkin önleyici bir koruma sağlaması açısından da önemlidir. Nitekim TCK'nın hükümleri suç sayılan bir fiil gerçekleştikten sonra uygulanacağı gibi, MK ve BK hükümleri de, büyük oranda, zarar ortaya çıktıktan sonra uygulama alanı bulabilecektir. Oysa çerçeve bir yasa ile temel ilkelerin belirlenmesi, bunlara uygun pratiklerin geliştirilmesine ve böylelikle de zarar ya da suç oluşmadan kişisel verilerin korunmasına hizmet edecektir. TC kimlik numaraları açısından bu hususu değerlendirecek olursak şöyle söyleyebilmemiz olanaklıdır: TCK'nın ilgili hükümleri TC kimlik numarasının hukuka aykırı işlenmesi durumunda bu faaliyetleri gerçekleştirenlerin cezalandırılmasını öngörmektedir. Bu elbette yerinde bir yaklaşımdır. MK ve BK hükümleri ise hukuka aykırı kullanımlar dolayısıyla zarar gören kişinin zararının giderilmesini hedefler. Bu düzenlemelerin de önemli kazanımlar sağladığı açıktır. Öte yandan çerçeve bir yasanın yürürlüğe girmesi, pek çok kişi ya da kurumun, TC kimlik numaralarını toplarken, kayıt ederken, kullanırken ve üçüncü kişilere aktarırken daha ihtiyatlı olmasını sağlayacaktır. Böylelikle henüz zarar ortaya çıkmadan önlenmesi olanaklı bulunacaktır.

Türkiye'de kişisel verilerin korunmasına ilişkin son dönemde gözlenen belki de en önemli gelişme ise 2010 yılında gerçekleşen Anayasa değişiklikleriyle, kişisel verilerin korunması hakkının Anayasanın 20. maddesi hükmüne dahil edilmiş olmasıdır. Böylelikle söz konusu korumanın anayasal bir temel hak olması konusunda hiçbir tereddüt kalmamıştır. Değişikliklerden sonra Anayasanın 20. maddesinin son fıkrası şu düzenlemeyi getirmektedir:

> "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir".

Anayasadaki bu değişiklikle birlikte, mevzuatta konuya ilişkin daha ayrıntılı düzenlemelerin yapılması ve özellikle çerçeve yasanın kabulü de bir zorunluluk haline gelmiştir. Anayasada yer alan belirtilen düzenlemenin içeriğine ilişkin değerlendirmeye geçmeden önce, işaret edilmesi gereken bir diğer konu ise kişisel verilerin korunmasının, bu değişikliğin öncesinde de anayasal güvenceden yoksun olmadığıdır. Nitekim bu önemli hakkın, başta özel yaşamın gizliliği (m.20) ve kişinin maddi ve varlığını geliştirme hakkı (Başlangıç, par.6; m. 5; m. 17/1) olmak üzere, haberleşme hürriyeti (m.22), düşünce ve kanaat hürriyeti (m.25) gibi çeşitli temel hak ve özgürlükleri düzenleyen hükümlerle yakından ilişkisi bulunmaktadır. Ancak bu dönemde belirtilen ilişki belki gözden uzak tutulabilmişse de Anayasanın 20/son hükmü ile kişisel verilerin etkin korunmasına kayıtsız kalınması olasılığı ortadan kalkmıştır. Artık konuya ilişkin yeni düzenlemeler yapılması, mevcut düzenlemelerin gözden geçirilmesi ve uygulamada da bu konuda

gereken hassasiyetin gösterilmesi bir zorunluluktur. Bu noktada, "Anayasa'nın bağlayıcılığı ve üstünlüğü" kenar başlıklı 11. maddesini de dikkatten kaçırmamak gerekir. Nitekim belirtilen hüküm uyarınca:

> "Anayasa hükümleri, yasama, yürütme ve yargı organlarını, idare makamlarını ve diğer kuruluş ve kişileri bağlayan temel hukuk kurallarıdır. Kanunlar Anayasaya aykırı olamaz".

O halde Anayasa'da açıkça yer aldığı üzere kişilerin kendileri ile ilgili bilgilerin korunmasını isteme hakkı bulunmaktadır. Bunun istisnası, kişinin rıza göstermesi ya da yasanın açıkça öngörmesi durumlarıdır. Bu noktada, oldukça olumlu olan bu gelişmeyi değerlendirirken, iki sorunun varlığını da göz ardı etmemek gerekir. Bunlardan birincisi, Anayasa tekniği açısından söz konusudur. Anayasamızın 13. maddesi uyarınca "Temel hak ve hürriyetler ... yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ... sınırlanabilir". Oysa 20. maddeye eklenen bu hüküm ile, sınırlama sebepleri yasa koyucuya bırakılmıştır. Ancak unutulmamalıdır ki yasa koyucu, her durumda yine 13. maddede kaynağını bulan sınırlamanın sınırlarına uymak zorunluluğundadır. Ayrıca temel hak ve özgülükler ile ilişkili konularda istisnaların her zaman dar yorumlanması gerekliliği de dikkatten kaçmamalıdır. Aksi durum, Anayasa'da yer alan bu hükmü, adeta kâğıttan bir kaplana dönüştürür. Bunun sonucunda yasal düzenlemeler ile belirlenen ölçüsüz sınırlama nedenleri, hakkın tanınmasını anlamsız kılabilir (Küzeci, 2011:142-149).

Anayasanın 20. maddesine eklenen hükümde dikkat çeken bir diğer husus ise kurallara uyulmasını denetleyen bağımsız bir kurumun oluşturulmasına burada yer verilmemiş olmasıdır. Oysa daha önce hazırlanan kimi Anayasa taslaklarında bu hususa yer verildiği gibi, Kişisel Verilerin Korunması Yasa Tasarısı'nda da-önemli bazı eksikliklere karşın-böyle bir kurulun oluşturulmasına dair esaslar belirlenmiştir. Bu yaklaşım, 1 Aralık 2009'dan itibaren hukuksal açıdan bağlayıcılığa kavuşan Avrupa Birliği Temel Haklar Şartı'nın (ABTHŞ) 8/3 hükmünün de bir gereğidir. Nitekim bu maddede kişisel verilerin korunmasında hakim olan temel ilkelere uygun hareket edilip edilmediğini denetleyecek bağımsız bir makamın oluşturulması bir zorunluluk olarak öngörülmüştür. ABTHŞ'nın 8. maddesi ile oldukça benzeşen Anayasanın 20/son hükmünde bağımsız denetim organı oluşturulmasının neden dışlandığını anlamak güçtür. Elbette Anayasa'da bağımsız denetim organına ilişkin bir ifadenin yer almaması bunun oluşturulamayacağı anlamına gelmez. Ancak, kanımızca, bu eksikliğin yasal düzenlemeler ile mutlaka giderilmesi gerekir.

Ayrıca Anayasa'nın 20. Maddesi'ne eklenen hükmün ışığında kişisel verilerin korunmasına yönelik hukuksal düzenlemeler geliştirilirken Avrupa İnsan Hakları Sözleşmesi (AİHS) ve Sözleşmenin öngördüğü yargı organı olan Avrupa İnsan Hakları Mahkemesi (AİHM) kararları da dikkate alınmalıdır. Anayasa'nın 90. maddesi uyarınca bu bir zorunluluk. Nitekim 90. maddenin son fıkrası uyarınca usulüne göre yürürlüğe konulmuş antlaşmalar, yasa hükmündedir. Bunlar hakkında Anayasa'ya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz. Bunun yanında belirtilen hükme, 2004 yılında şu kural da eklenmiştir:

> "Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşma hükümleri esas alınır".

Hemen belirtelim: AİHS'de kişisel verilerin korunması, ayrı bir hak alanı olarak düzenlenmemiştir. Ancak AİHM verdiği kararlarla, kişisel verilerin korunmasında temel ilkelerin büyük bir bölümünü, Sözleşme'nin 8. maddesi kapsamında tanımaktadır (Küzeci, 2011a:7-61). Bununla birlikte Türk Anayasa Mahkemesi'nin konuya yaklaşımının AİHM'nin kararlarından oldukça farklılaştığını belirtmek gerekir. Mahkeme, kişisel verilerin korunmasına ilişkin temel ilkeleri Anayasanın özel yaşamın gizliliğine ilişkin 20. Maddesi çerçevesinde yorumlamada biraz isteksiz görünmektedir. Yukarıda da işaret ettiğimiz, ve kanımızca din özgürlüğü kadar özel yaşamın gizliliği hakkı ile de ilişkili olan, nüfus cüzdanlarında din hanesinin bulunmasını Anayasaya aykırı görmeyen kararı bunun bir işareti olarak kabul edilebilir.

Anayasa Mahkemesinin konuya ilişkin bir diğer önemli kararı ise 1774 sayılı Kimlik Bildirme Kanununa ilişkindir. Belirtilen kanuna eklenen bir hüküm ile genel kolluk kuvvetlerinin bilgisayarlarında kişisel bilgilerin toplanma yetkisini, bu yetki kullanılırken hangi kurallara uyulması gerektiği belirlenmeden, tanıyan hükmü Anayasaya aykırı bulmamıştır (AYMK E. 1996/68, K. 1999/1, k.t. 6 Ocak 1999). Buna karşılık Mahkeme 2008 yılında, 5429 sayılı Türkiye İstatistik Kanununun hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşların yetkililerinin, kendilerinden istenen veri veya bilgileri, vermekle yükümlü olduklarına ve bu yükümlülüğe uymayanların para cezası ile cezalandırılacaklarına ilişkin hükmü oyçokluğu ile Anayasaya aykırı bulmuştur (AYMK, E. 2006/167, K. 2008/86, k.t. 20 Mart 2008). Konusu itibariyle yukarıda açıkladığımız Alman Anayasa Mahkemesinin Nüfus Sayımı kararı ile benzerlikler taşıyan bu kararda Türk Anayasa Mahkemesi Türkiye İstatistik Kanununun 8 ve 54/2,b hükümlerini değerlendirirken, kişisel verilerin korunmasına ilişkin önemli saptamalarda bulunmuştur. Mahkemeye göre:

> "Maddede açıklayıcı bir düzenleme bulunmadığı için, "kişisel veri" veya "isteme bağlı veri" olarak adlandırılan, belirli veya belirlenebilir kişilerle ilgili her türlü bilgilerin istenebileceği kuşkusuzdur. İstatistiki birimlerin kendilerinden istenen bilgileri belirlenen şekil ve sürede eksiksiz ve hatasız olarak vermek zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmış olmasına karşın, istenilecek veri ve bilgilerin kapsamı ya da sınırlarının ne/neler olacağına, başka bir anlatımla, temel hak ve özgürlüklere müdahale niteliğinde olan veri ve bilgilerin bu zorunluluk kapsamında bulunup bulunmadığına ilişkin herhangi bir düzenlemeye rastlanmamaktadır. Dolayısıyla, istatistiki birimler kendilerinden istenildiği takdirde her türlü bilgiyi temel hak ve özgürlüklerine müdahale niteliğinde olsa bile vermek zorundadırlar. Anayasa'nın 20. maddesinde herkesin özel hayatına ve aile yaşayışına

> saygı gösterilmesini isteme hakkına sahip olduğu; 25. maddesinde de herkesin düşünce ve kanaat özgürlüğüne sahip olduğu, her ne sebep ve amaçla olursa olsun kimsenin düşünce ve kanaatlerini açıklamaya zorlanamayacağı hüküm altına alınmıştır. 20. madde gerekçesinde, özel hayatın korunmasının her şeyden önce bu hayatın gizliliğinin korunması, resmi makamların özel hayata müdahale edememesi anlamına geldiği belirtilmiştir. AİHM kararlarında da belirtildiği gibi, özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililer hakkında rızası olmaksızın bilgi toplamasının her zaman söz konusu kişinin özel hayatını ilgilendireceği kuşkusuzdur. Anket formlarında yer alan bazı sorular özel yaşamın gizliliği ile düşünce ve kanaatin açıklanması sonucunu doğurabilir. Bir ülkede en güçlü veri tekeli idaredir. Bu gücün sınırlandırılması özel yaşamın ve düşünce ve kanaat özgürlüğünün korunması bakımından önemlidir. Anayasa'nın 20. ve 25. maddelerinde yer alan güvencelere rağmen itiraza konu 8. madde hükmüyle kişiler, bilgi toplama, saklama, işleme ve değiştirme tekeli olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamanın sınırlarına yasal düzenlemede yer verilmemiştir. Açıklanan nedenlerle itiraz konusu kuralların Anayasa'nın 20. ve 25. maddelerine aykırı olduğundan iptali gerekir".

Kişisel verilerin korunması açısından oldukça umut verici bu kararın ardından Yasa koyucu oluşan boşluğu gidermek amacıyla Türkiye İstatistik Kanununun 8. maddesini yeniden düzenlemiştir. Hükmün yeni şekli şöyledir:

> "İstatistikî birimler, ülkenin ekonomi, sosyal, demografi, kültür, çevre, bilim, teknoloji ve ihtiyaç duyulan diğer alanlardaki resmi istatistikleri üretmek üzere, **Anayasa'da belirlenen temel haklar ve ödevler çerçevesinde**, kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle yükümlüdür".

Her ne kadar düzenlemenin yeni şeklinde kapsam öncekine göre sınırlandırılmış gibi gözükse de, aslında hükmü yeni şekline eklenen ifade uygulamada ciddi bir değişiklik getirmemektedir. Nitekim hükümde sözü edilen alanlar sınırlayıcı olmadığı gibi, eğer öyle olsaydı da neredeyse her türlü veriyi kapsayabilecek genişlikte kavramlardır. Bu nedenle istatistiki birimlerden hemen hemen her konuda bilgi istemek olanaklıdır. Ayrıca Anayasada belirlenen temel hak ve özgürlükler, herhangi bir yasada açıkça belirtilmemiş olsa bile, dikkate alınması zorunlu hükümleri oluşturur. Ancak, iyimser bir yorumla, hükümde temel hak ve ödevlerin hatırlatılması dolayısıyla kişilerin kendilerinden istenen özel bilgileri vermemekte direnmesine yardımcı olabileceği söylenebilir. Nitekim benzer yaklaşımlar dolayısıyla, yasanın yeni şekli de Anayasa Mahkemesinin önüne gitmiştir.

Gerçekten belirtilen hüküm 2010 yılında "...anket kapsamında bireyleri belli konularda sorulacak sorulara cevap vermeye zorlamak herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu; herkesin vicdan, dini inanç ve kanaat hürriyetine sahip olduğu ve bu dini inanç ve kanaatlerini açıklamaya zorlanamayacağını; herkesin düşünce ve kanaat hürriyetine sahip olduğu, her ne sebep ve amaçla olursa olsun kimsenin düşünce ve kanaatlerini açıklamaya zorlanamayacağına ilişkin" Anayasa hükümlerine aykırı olduğu gerekçesi ile itiraz yolu kullanılarak tekrar Anayasa Mahkemesinin önüne götürülmüştür. Ancak Anayasa Mahkemesi yaptığı inceleme sonucunda, bu kez itiraz edilen 5429 sayılı İstatistik Kanununun 8. ve 54/2,a hükümlerinin Anayasaya aykırı olmadığı sonuç ve kanaatine ulaşmıştır (AYMK, E. 2010/2, K. 2011/135, k.t. 12 Ekim 2011). Anayasa Mahkemesine göre:

> "(...) İtiraz konusu kurallarla istatistiklerin kamu yararı için önemi dikkate alınarak bireylere mecburi ve ücretsiz kamusal bir külfet yüklenmiştir. Karşılaştırmalı hukukta da bazı ülkelerde bireylere istatistik amaçlı bilgi verme yükümlülüğü getirildiği görülmektedir. Modern bir devlette kamu hizmetlerinin planlanması ve kamu güvenliğinin sağlanabilmesi için bireylerin kendileriyle ilgili pek çok bilgiyi kamu otoritelerine verme yükümlülüğü bulunmaktadır. Bu bilgilerin istatistik amacıyla toplanmış olması bilgi toplamayı kendiliğinden Anayasa'ya aykırı hale getirmez. (...) 5429 sayılı Kanunun 54. maddesinin ikinci fıkrasında, istatistiki birimlerin kendilerinden istenen bilgileri geçerli bir mazereti olmaksızın belirlenen şekil ve sürede, eksiksiz ve hatasız olarak verme zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmıştır. Bu durumda dava konusu iki hüküm birlikte değerlendirildiğinde bireylerin temel haklarının korunmasının idari ve adli makamların sorumluluğuna bırakıldığı görülmektedir. İdari makamlar bireyin temel haklarını ihlal edecek şekilde bilgi talep etmeme yükümlülüğündedirler. İdari makamların bu ödevini yerine getirmemesi halinde istatistiki birimler haklarını yargı makamları önünde arayabileceklerdir. Bu durumda itiraz konusu kurallarla bireyin hakları ile kamu yararı arasında makul bir denge kurulduğu ve bireyin haklarına ölçüsüz bir müdahalaye izin verilmediği anlaşıldığından Anayasanın 2. Maddesindeki hukuk devleti ilkesine aykırılık görülmemiştir".

İstatistiki bilgilerin devletin üzerine düşen görevleri en iyi şekilde yerine getirmesinde oldukça önemli olduğu açıktır. Ancak Anayasa Mahkemesinin bu noktada geliştirdiği yoruma katılmak mümkün değildir. Nitekim istatistiki bilgiler toplanırken kişilerin temel hak ve özgürlükleri mutlaka dikkate alınmalı, dengeli uygulamalar geliştirilmelidir. Kanımızca Mahkemenin incelediği hükümler bu dengeyi bireyin hak ve özgürlükleri aleyhine bozmaktadır. Bu noktada Alman Anayasa Mahkemesinin Nüfus Sayımı kararında geliştirdiği "bilgilerin geleceğini belirleme hakkı"nı hatırlamak gerekir. Öte yandan Mahkemenin, kararını verdiği sırada yürürlükte olan ve kişisel verilerin korunmasını açıkça anayasal hak

durumuna getiren Anayasanın 20/son hükmüne ilişkin tamamen sessiz kalması da dikkate değerdir. Gerçekten Mahkemenin kararında bu hükümden hiç bahsedilmemiş, kişisel verilerin korunması açısından bir yorum da geliştirilmemiştir. Nitekim bu hususa yalnızca Anayasa Mahkemesi Başkanvekili Serruh Kaleli ile Mahkeme üyesi Erdal Tercan'ın karşı oy yazılarında değindikleri görülmektedir.

4.5. Dijital Çağda Bireysel Özerklik Nasıl Sürdürülebilir?

Türk hukuk sisteminde yürürlükte bulunan düzenlemeler ve Anayasa Mahkemesinin konuya yaklaşımı incelendiğinde kişisel verilerin korunması alanında açıkça bir boşluğun bulunduğunu belirtmek gerekir. Bu nedenle TC kimlik numaralarının, yaratabileceği riskler dikkate alınmadan, adeta sınırsız kullanımı endişe verici niteliktedir. Kişisel verilerin korunmasına dair ilkeler yaşama geçmeden Türkiye Cumhuriyeti yurttaşlarının kamusal otoriteler karşısında, yalnızca sayılarla belirlenmiş nesnelere dönüşmeleri tehlikesi mutlaka dikkate alınmalıdır.

Unutulmamalıdır ki, idare hukuku açısından da, idarenin üzerine düşen görevlerin niteliği gereği kaçınılmaz olan bilgi toplama ve bunları kullanma süreçlerinin bireysel hakları koruyacak nitelikte olması gerekir (Akıllıoğlu: 2004). Bu anlamda idare, bu bilgileri kişisel verilerin korunmasında hakim olan ilkelere uygun bir şekilde işlemelidir. Bu, idarenin kanuniliği ilkesinin ve keyfilikten uzak olması koşulunun da bir gereğidir. Ancak böylelikle idari usul hukukunun iki temel amacının, yani yönetimin tam ve etkin işleyişi ile yurttaşın temel haklarının korunması bir arada gerçekleşebilir. Ayrıca unutulmamalıdır ki günümüzde devlet ile birey arasındaki ilişkide bireyin konumu o devletin yönetim sistemini belirleyen en önemli ölçütlerden biri olarak kabul edilmektedir.

Uygulamaya baktığımızda e-devlet projeleri çerçevesinde kişisel verilerin çeşitli kurumlarca işlenmesi ve bu bilgilerin İnternet ortamında yer alması, özellikle veri güvenliğine ilişkin bazı sorunların görülmesine neden olmuştur. Kişisel verilere yalnızca ilgili kişilerin erişimini sağlamak için kurum ve kuruluşlar bazı önlemler almaya çalışmaktadır. Ancak her kurumun kendi başına belirlediği önlemler hedefin, yani kişisel verilerin korunmasının, gerçekleştirilebilmesi için yeterli değildir. Nitekim bir İnternet sitesinde yer alan bilgi, diğerindeki verilere erişimin anahtarı olabilir. Bu sakıncanın giderilmesi için bütün kurum ve kuruluşların uyacakları ortak standartların belirlenmesi gerekir. Bu standardı sağlayabilecek olan ise konuya ilişkin uluslararası metinlerle uyumlu bir kişisel verilerin korunması yasasının yürürlüğe girmesidir.

Bu noktada adı "Kişisel Verilerin Korunması Kanunu" olan herhangi bir düzenlenmenin yeterli olmadığının altı çizilmelidir. Ancak gerçek anlamıyla kişisel verilerin ve bunun sonucunda insan onurunun, bireysel özerkliğin, kişiliği geliştirme hakkının korunacağı bir düzenleme mevcut tehlikeleri bertaraf etmeye yarayabilir. Böylelikle bir yandan kamu hizmetlerinin doğru, hızlı, etkin, düşük

maliyetli bir şekilde yurttaşlara ulaştırılması, diğer yandan da yurttaşların temel hak ve özgürlüklerinin korunması olanaklı olabilir. Çağdaş, demokratik bir devletten beklenen "denge" de ancak böyle sağlanabilir.

V. Bölüm:

GENEL DEĞERLENDİRME

5. Genel Değerlendirme

Görüldüğü üzere Türkiye'de yurttaşlar gerek MERNİS projesi sonucunda gerekse e-devlet kapısı uygulamasıyla artık sayısal olarak bedenleşmiştir. E-kimlik kartı üzerindeki parmak izi, damar kesiti vb. güvenlik uygulamaları ile Türkiye'de yurttaş bio-iktidara ve bio-politikaya tabi kılmaktadır. KPS ile olsun, UAVT ile olsun, e-devlet kapısı ile olsun verilerin otomatik güncellemesiyle yurttaş üzerinde bir denetim sistemi oluşturulmuştur. Veri eşleştirmesi sürekli yapılmakta ve güncellenmektedir. E-devlet uygulamaları, güvenlik, verimlilik, hızlılık, şeffaflık gibi söylemlere dayanan neoliberal politikalar ile yönetişim olgusundan beslenmekte ve yönetişim olgusu üzerinden meşru kılınan bu uygulamalar dolayımıyla yurttaşın kayıt altına alınması süreklilik arz ederek gerçekleşmektedir. Bu işlemde, iktidar ve bilgi alma süreçleri birlikte işlemektedir. Foucault'u izleyerek söyleyecek olursak, KPS ve e-devlet kapısı ile merkezsizleşmiş, ancak sürekli işleyen veri gözetimi ve denetimi söz konusudur. Böylece MERNİS'ten e-kimlik kartına doğru uzanan/gelişen yurttaşın sayısal bedenlenişi sürecinde, yurttaş görünmez bir gözün her yerdeki iktidarını dijital gözetim teknolojileri üzerinden meşru ve doğal görmeye, dolayısıyla veri gözetimini kanıksamaya ve içselleştirmeye başlamaktadır.

Bedenin sayısal konumlanışını, kişisel verilerin gözetimini ve veri eşleştirmesini teknik-sosyal-siyasal ve ekonomik sorunlar olarak ele alırsak, ivedilikle bu sorunların çözümüne yönelik birtakım politikaların geliştirilmesi gereği ortaya çıkmaktadır. Bu çalışma kapsamında geliştirilen politika ve çözüm önerilerimizi aşağıdaki/şu şekilde sıralayabiliriz:

- Uluslararası insan hakları standartlarına ilişkin farkındalığın ve kimlik kayıtlarındaki verilerinin kişiye özel hassas veri olarak gizliliğinin korunması hakkının arttırılması gereği;
- Kişisel verilerin korunması konusunda Türkiye'de gözetim ve veri eşleştirmesini denetleyecek bağımsız ve özerk bir kurumun oluşturulması gereği;
- Türkiye'de dijital verilerin izlenmesi ve veri gözetimi konusunda bir kamu politikasının geliştirilmesi ve bu politikada öncelikle yurttaşların veri bütünlüğünün korunmasına vurgu yapması gereği;
- *Kişisel Verilerin Korunması Kanunu*'nun temel insan hakları temelli çıkartılması gereği,
- *Kişisel Verilerin Korunması Kanunu*'nun zaruriliği konusunda başta yürütme erki olmak üzere, ilgili tüm sivil toplum örgütlerini akademik ve disiplinlerarası bir çerçevede bilgilendirme gereği;

- Kimlik kartları dolayımı ile yurttaşın gözetlenmesi ve denetlenmesi, veri eşleştirmesi konusunda, özellikle de Türkiye'de T.C. kimlik numarası ve e-kimliklerin kullanım pratiklerinin irdelenmesine ilişkin akademik ve disiplinlerarası kapsamlı bilgi üretilerek, bu bilginin her türlü hak örgütü ile paylaşılması gereği;
- Ayrımcılığa karşı ve insan hakları konusunda çalışan sivil toplum örgütleri ile birlikte EMO gibi yeni iletişim teknolojileri, gözetim ve kişisel verilerin korunması gibi konularda da çalışmalar yürüten toplumsal örgütlemelerin bu konudaki farkındalıklarının arttırılması, desteklenmesi gereği;
- Medyayı dijital gözetim, veri eşleştirmesi ile e-devletin mevcut altyapısındaki sorunlar hakkında bilgilendirme ve yurttaşın kimlik kayıtlarının kişiye özel hassas veri olarak gizliliğinin korunmasına yönelik bazı hukuksal ve toplumsal çözümlerin geliştirilmesi gereği;
- Türkiye'de yurttaşı dijital bedene indirgeyen ve dijital kimliklenmeye dönüştüren, e-kimlik uygulamasının "disipline edici ve denetleyici" yönünün/olasılığının farkında olunması gereği;
- E-kimlik ve e-devlet uygulamalarında merkezi iktidarın gücünün arttırılması ve yurttaşın dijital olarak denetlenmesi amacının başat amaç olmaktan çıkarılarak, insan haklarını temel alan e-devlet uygulamasının amaç olması gereği;
- E-devlet kapısı uygulamasının ödev ve sorumluklarını yerine getiren yurttaş yerine; haklarına erişen ve kullanabilen yurttaş odaklı olması gereği;
- Bireylerin "kendi verilerinin geleceğini tayin hakkı"nın ("information self-determination") sağlanması gereği;

Peter Shields (2006: 34) iletişim içeriği ve iletişim veri trafiği arasındaki çizginin giderek silindiğini, devletin gözetim gücünün bireylerin hakkını gaspettiğine dikkat çekmiştir. Frank Webster da "Information Warfare, Surveillance and Human Rights" (2003:90-111) adlı makalesinde devletlerin "bilgi savaşçılarına" dönüştüğünü iddia eder. Örneğin AWACS (*Airbone Warning and Control Systems*) uçakları birçok ülkeyi havadan gözlemlemekte, vurulacak hedefi tespit etmektedir. Webster, bu enformasyon temelli/beslenen savaş tekniklerinin insan hakları ihlali ile olan ilişkisine değinmektedir. Bu izlekte devam edersek, veri gözetiminin insan hakları ihlali sorununu ortaya çıkardığını da görmekteyiz. David Lyon da (2007:161-170) yönetişim olgusu tartışılırken, insan hakları ve sivil özgürlükler ile dijital gözetimin birlikte tartışılması gerektiğini belirtir.

Thomas Hammarberg *Avrupa'da İnsan Hakları* (2012) adlı çalışmasında, bu çalışmanın Birinci Bölümü'nde dikkat çektiğimiz güvenlikleştirme söyleminin insan hakları ihlalini nasıl meşru kıldığını tartışmaktadır. Hammarberg demokrasileri "teröre karşı savaş" uygulamalarında terörizmle terörist yollarla mücadele etmemesi için uyarmaktadır: "Demokrasiler, ciddi insan hakları ihlallerini önleyecek ya da cezalandıracak eylemde bulunmamayı mazur göstermek üzere gizlilik

doktrinlerinin kullanılmasını asla kabul etmemelidir. Güvenlik güçlerinin de hesap vermeleri gerektiği herkes tarafından bilinmelidir ve bu alanda parlemento araştırmaları ve hukuki soruşturmalar yapılmalıdır. "Teröre karşı savaş" sırasında yapılan hatalardan çıkarılacak bir ders de, ulusal güvenlik teşkilatlarını daha etkili bir biçimde demokratik denetim altında tutma gereği olmuştur" (2012: 240).

Hammarberg'in bu uyarısının Türkiye'de yakın zamanlarda kamuoyunun, siyasetin ve yargının gündemini meşgul eden MİT Başkanı ve Başkan Yardımcılarının Özel Yetkili Cumhuriyet Savcıları tarafından "sanık" sıfatı ile ifade vermeye çağrılmasından[128] sonra yaşanan gelişmeler anımsanacak olursa, ne kadar önemli olduğu ortaya çıkar. Bu uyarının yurttaşların kişisel kayıtlarının gizliliğinin korunması konusuna da taşınması gereklidir.

Hammarberg bu konuda şu şekilde devam etmektedir: "Gözetleme teknolojisi nefes kesen bir hızla gelişmektedir. Bu trend, terörle ve organize suçlarla mücadelede kıymetli birtakım yeni araçlar yaratmasına karşın, bireylerin mahremiyet hakkıyla ilgili bazı temel sorunlara yol açmaktadır. Bireyler, özel hayatlarına izinsiz olarak girilmesi ve verilerin uygunsuz şekilde toplanması, kaydedilmesi, paylaşılması ve kullanılmasına karşı korunmalıdır" (2012:250). Özellikle gözetim teknolojilerini kullanan siyasi iktidar sahipleri ile emniyet ve istihbarat güçleri "gizlenecek bir şey yoksa bu tedbirlerden korkulması" gerekmediğini kamuoyunda dile getirmektedir. Örneğin, 28 Ocak 2009 tarihinde gazetecilerin Türkiye'de yasadışı telefon dinleme iddialarını yanıtlayan Ulaştırma Denizcilik ve Haberleşme Bakanı Binali Yıldırım, "Yanlış, yasal olmayan bir işiniz yoksa dinlenmekten korkmayın. Dinlenmek istemiyorsanız konuşmayın" demiştir[129].

Bu retorik, Hammarberg'in deyişiyle sorumluluğu yanlış tarafa yüklemektedir (250). Ona göre, "... yeni gözetleme olanaklarının polis ve güvenlik güçleri tarafından kullanılması, gelişmiş bir demokratik ve hukuki denetim gerektirmektedir" (251). Kişisel verilerin korunması devletin yurttaş karşısında temel bir sorumluluğudur. Özellikle yurttaşın devasa veri tabanlarında birleştirilen ve işlenen kimlik kayıtlarının ırk, etnik köken, dini inanç, cinsel kimlik yönelimi, siyasi görüş, ekonomik konum ve statüye göre ayrıştırılarak, bu veri sınıflandırmasına dayanılarak "biz" ve "ötekiler" temelinde ayrımcı, dışlayıcı, hatta yok sayıcı toplumsal-siyasal ve ekonomik politikaların yaşama geçirilmesinin önüne geçilmesi gerekmektedir. Uluslararası ve ulusal güvenlileştirme politikaları ile bu politikaların "tehdit, kaygı ve olası risklerin bertaraf edilmesi" ve "suçun gerçekleşmeden kontrolü" şeklinde dile getirilen hakim söylemsel pratikler, yurttaşın dijital olarak kayıtlanmasını ve kimliklenmesini denetleme ve düzenleme politikasının bir aracı olarak dijital gözetim teknolojilerini uygulamaya sokmaktadır. Bu uygulamalar, bireylerin "ideal ve sorunsuz" ve "risk taşıyan ve sorunlu"

[128] Bu konuda ayrıntılı bilgi için bakınız: http://t24.com.tr/yazi/25-soruda-mit-krizi/4614, (Erişim tarihi: 19 Mart 2012).

[129] http://arsiv.ntvmsnbc.com/news/473678.asp, (Erişim tarihi: 20 Mart 2012); http://www.milliyet.com.tr/yildirim–yasal-olmayan-bir-isiniz-yoksa-dinlenmekten-korkmayin/siyaset/sondakika/28.01.2009/1052784/default.htm, (Erişim tarihi: 20 Mart 2012); http://bianet.org/bianet/ifade-ozgurlugu/112267-dinlenmekten-korkmayin-diyenler, (Erişim tarihi: 20 Mart 2012).

olarak ayrılmasına kadar gidebilecek/giden ayrımcı, dışlayıcı sınıflandırmalardır. Gerek askeri, emniyet, istihbarat amaçlı, gerekse tüketici yapılandırması, gerekse işverenin işyeri denetimi amacıyla gerçekleştirdiği veri gözetimi, veri eşleştirmesi ve diğer tüm dijital kayıtlamalar son kertede yurttaşların birbirinden farklılıklarına göre ayırt eder; farklılıkları tektipleştirmeye, "aynılaştırmaya" çalışır. Bundan ötürü de gündelik yaşamın her alanında yaygınlaşan dijital gözetim tekniklerinin uygulanması temel insan haklarından biri olan özel yaşamın gizliliğine aykırıdır. Mevcut haliyle de e-devlet kapısı ile e-kimlik kartı uygulaması özünde iktidar merkezlidir. Bizim bu çalışmadaki tüm saptamalarımız ışığında ivedi önerimiz, Türkiye'de e-devlet kapısı ve e-kimlik kartı uygulamasının yurttaş odaklı olarak söylem ve pratik düzeyinde, karşılılıklılık ilkesi temelinde işletilmesi gereğidir. Son olarak, artık dijital olarak konumlanan/konumlandırılan yurttaşın kişisel kayıtlarının korunmasındaki temel sorumluluğun devlet ve diğer kayıtlayıcılarda olduğunun ve buna ek olarak kişisel verilerin bütünlüğünü ve korunmasını talep etmenin de temel bir yurttaşlık hakkı[130] olduğunun altını çizelim.

Son söz olarak, bu çalışmanın hiç kuşkusuz Türkiye'de dijital gözetim olgusu üzerine kapsamlı tartışmalar ile farklı gözetim uygulamaları incelemeleri için bir başlangıç niteliği taşımakta olduğunu belirtelim. T.C. kimlikten e-Kimliğe uzanan çizgide Türkiye'de yurttaşın sayısal bedenlenişi olgusunun irdelenmesinin bu çalışmanın bıraktığı yerden devam ettirilmesi, yurttaşın e-devlet kapısı uygulamasında çoğunlukla "sorumluluk" sahibi olarak konumlandıran egemen söylemin "yurttaşa" biçtiği edilgen ve itaatkâr rolün daha derin tartışmalara açılması gerekmektedir. Umarız, bu çalışmanın üzerine dijital gözetim uygulamalarının temel insan hakları, özel yaşamın gizliliği ve insan onuru ile çatışması durumu ile Türkiye'deki diğer dijital gözetim uygulamaları -askeri ve istihbarat alanlarından, iş yerlerine ve ticari kayıtlamalara, veri madenciliği olgusuna değin- tartışmaya başlanır.

---

[130] Thomas Humphrey Marshall, yurttaşlık kavramını ilk olarak 1949 yılında yazmış olduğu "Citizenship ve Social Class" (Yurttaşlık ve Toplumsal Sınıflar) makalesinde ele almaktadır. Marshall, yurttaşlığın tarihsel açıdan üç farklı eksenin bir araya gelmesiyle oluştuğunu söylemektedir: *Medeni haklar, siyasal haklar ve sosyal haklar* (Marshall, 2006: 8). Marshall medeni ve siyasal hakları şu şekilde tanımlar: "Medeni haklar eksenini oluşturan unsurlar bireysel özgürlük, konuşma özgürlüğü, düşünce ve inanç özgürlüğü, mülk edinme ve sözleşme yapma özgürlüğü ve adalet hakkı gibi hak ve özgürlüklerdir. Siyasal haklar ekseni ise siyasal karar alma sürecine seçmen ve seçilen olarak katılma hakkını ifade eder" (Marshall, 2006: 8). Marshall, sosyal hakları ise şöyle açıklar: "Sosyal haklar ekseni ile ifade edilen şey ise yaşadığımız toplumun standartları ölçüsünde ekonomik refah ve sosyal güvenlik gibi haklara sahip olmaktan, çağdaş bir birey gibi yaşayabilme hakkına değin uzanan geniş bir haklar dizinidir. Eğitim hakkı ve sosyal hizmetler bu çerçevede değerlendirilebilir" (2006: 8-9). Marshall'ın yurttaşlığın bu eksenlerine ilişkin tartışmasına yakın zamanlarda etnik kimlik/temelli haklar da eklenmiştir. Bu çalışmada altını çizmek istediğimiz husus, kişisel verilerin bütünlüğünün sağlanması ve korunması gereğinin, kişinin kendi verilerinin geleceğine sahip çıkma talebinin artık temel bir yurttaş hakkı olduğu konusudur. Türkiye'de yurttaşın sadece ödevler ve sorumluluklar ekseninde konumlandırılması, haklar ve özgürlükler ekseninde eyleyiciliğinin ve iradesinin süregelen bir şekilde siyasi iktidarlar ve devlet kurum-kuruluşları tarafından görmezden gelinmesi, sindirilmesi ve bastırılması aslında "yurttaş hakları" tartışmasındaki asıl ve asli sorundur. Türkiye'de yurttaşın konumuna ilişkin bir diğer sorun da "yönetişim" veya "iyi yönetişim" modeli temelinde de yurttaşın tüketici konumunun altının çizilmesi, neoliberalizmin yurttaşı "sen tükettiğin kadar varsın"a indirgemesi, sürekli tüketime çağırmasıdır.

Ek-1

Kurumlar Listesi

- Adalet Bakanlığı
- Başbakanlık
- Bilgi Teknolojileri ve İletişim Kurumu
- Cumhurbaşkanlığı
- Çalışma ve Sosyal Güvenlik Bakanlığı
- Çay İşletmeleri Genel Müdürlüğü
- Çevre ve Şehircilik Bakanlığı
- Denizcilik Müsteşarlığı
- Devlet Meteoroloji İşleri Genel Müdürlüğü
- Dışişleri Bakanlığı
- Emniyet Genel Müdürlüğü
- Gelir İdaresi Başkanlığı
- Gümrük ve Ticaret Bakanlığı
- İçişleri Bakanlığı
- İŞKUR
- Kıyı Emniyeti Genel Müdürlüğü
- KOSGEB
- Mahalli İdareler Genel Müdürlüğü
- Maliye Bakanlığı
- Merkezi Kayit Kurulusu

- Millî Savunma Bakanlığı
- Milli Eğitim Bakanlığı
- Nüfus Vatandaşlık İşleri Genel Müdürlüğü
- PTT
- Sağlık Bakanlığı
- Sivil Havacılık Genel Müdürlüğü
- Sosyal Güvenlik Kurumu
- Tapu ve Kadastro Genel Müdürlüğü
- TBMM Başkanlığı
- T.C. Merkez Bankası
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
- Yüksek Öğrenim Kredi ve Yurtlar Kurumu Genel Müdürlüğü

Hizmet Listesi

Adalet Bakanlığı

- Adalet Bakanlığı Mahkeme Dava Dosyası Sorgulama
- UYAP Portali Avukat Girişi
- UYAP Portali Baro Girişi
- UYAP Portali Kurum Girişi
- UYAP Portali Vatandaş Girişi

Başbakanlık

- Başbakanlık İletişim Merkezi Yeni Başvuru
- Başbakanlık İletişim Merkezi Başvuru Sonucu Sorgulama
- Başbakanlık Kamu Hizmet Envanteri Giriş Uygulaması

Bilgi Teknolojileri ve İletişim Kurumu

- IMEI - MSISDN Eşleşme Sorgulama
- IMEI Sorgulama

Cumhurbaşkanlığı

- Cumhurbaşkanına Yazın

Çalışma ve Sosyal Güvenlik Bakanlığı

- İş Sağlığı ve Güvenliği Yönetim Hizmetleri
- Yabancıların Çalışma İzinleri Otomasyon Sistemi

Çay İşletmeleri Genel Müdürlüğü

- Budama Desteği Sorgulama
- Üretici Cari Detay Bilgileri Sorgulama
- Üretici Cari Hesap Listesi Sorgulama
- Üretici Destekleme Sorgulama
- Üretici Sorgulama
- Üretici Tanitim Karti Bilgileri Sorgulama
- Üretici Yillik Alimlar Sorgulama

Devlet Meteoroloji İşleri Genel Müdürlüğü

- 3 Günlük Hava Tahmini
- Deniz Suyu Sıcaklıkları
- Dış Merkezler Hava Tahmini
- Günlük Hava Tahmini

Dışişleri Bakanlığı

- Akredite Misyonlar
- Diplomatik Liste
- Fahri Konsolosluklar
- Geçici İşgüderler
- Uluslararası Kuruluşlar
- Yurt Dışındaki Temsilciliklerimiz
- E-Konsolosluk Hizmeti

Emniyet Genel Müdürlüğü

- Emniyet Genel Müdürlüğü e-Pasaport Gönderi Takibi
- Toplum Destekli Polislik (TDP)
- Toplum Destekli Polislik Mahalle Polisi Hizmeti

- ASBIS Araç ve Sürücü Bilgi Sistemi (Test Uygulaması)
- Trafik Şube
- Araç Sorgulama
- Sürücü Belgesi Ceza Puanı Sorgulama
- Sürücü Belgesi İptal Bilgisi Sorgulama

Gelir İdaresi Başkanlığı

- e-Vergi Levhası Sorgulama

Gümrük ve Ticaret Bakanlığı

- Online Tüketici Şikayet sorgulama
- Gümrükler Genel Müdürlüğü e-Dilekçe
- Tüketici Portali - Tüketici Şikayeti Uygulaması
- Tüketici İşlemleri
- Garanti Belgesi
- Kullanım Kılavuzu
- Satış Sonrası Hizmet Yeterlilik Belgesi
- Tüketici Kuruluşları Sorgulama
- Tüketici Sorunları Hakem Heyeti Sorgulama

İçişleri Bakanlığı

- Kaymakam Adaylığı Sınav Başvurusu
- İçişleri Bakanlığı e-İçişleri Projesi Evrak Takibi

İŞKUR

- Is gücü İnsan Gücü Planlama Sistemi Giriş Uygulaması
- Kriterlere Göre Açık İş Sorgulama ve İş Başvurusu
- Meslek Kursu Sorgulama
- Profile Göre Açık İş Sorgulama ve İş Başvurusu
- Türk Meslek Sözlüğü
- İŞKUR'a Olan Borcu Sorgulama
- İş Başvuru Sonucu Sorgulama

- İşsizlik Ödeneği Başvurusu
- İşsizlik Ödeneği Ödemesi

Kıyı Emniyeti Genel Müdürlüğü

- Kıyı Emniyeti Borç Sorgulama
- Kıyı Emniyeti Deniz Ruhsatı Borç Sorgulama
- Kıyı Emniyeti Hava Ruhsatı Borç Sorgulama
- Kıyı Emniyeti Kara Ruhsatı Borç Sorgulama
- Kıyı Emniyeti Amatör Telsiz Sınav ve Belge Ücreti Sorgulama
- Kıyı Emniyeti Inmarsat Aktivasyon Borç Sorgulama
- Kıyı Emniyeti Deniz Haberleşme Fatura Sorgulama
- Kıyı Emniyeti Donatan Acente
- Kıyı Emniyeti Donatan ve Acente Bilgi Doğrulama
- Kıyı Emniyeti INMARSAT Abonelik İşlemleri
- Başvuru İptal
- Başvuruları Listele
- Numara Tahsis Başvuru
- Kıyı Emniyeti Seyir Planı1(SP1)
- Boğaz Geçiş Sorgula
- SP1 Başvurumu Güncelle
- SP1 Başvurumu İptal Et
- SP1 Başvurumu Sil
- SP1 Başvurumu Sorgula
- SP1 Ekle
- Kıyı Emniyeti Sınav İşlemleri
- Kıyı Emniyeti Amatör Telsizcilik Sınav Başvuru
- Kıyı Emniyeti Amatör Telsizcilik Sınav Durum Sorgulama
- Kıyı Emniyeti Amatör Telsizcilik Belge Sonuç Sorgulama
- Kıyı Emniyeti Telsiz Ruhsat İşlemleri

- Deniz Ruhsat Sorgula
- Kıyı Emniyeti Yerleşim Planı
- Kıyı Emniyeti Yerleşim Planı

KOSGEB

- İşletme Durum Sorgulama

Maliye Bakanlığı

- e-Yolluk Uygulaması
- Maliye Bakanlığı e-Bordro Hizmeti

Merkezi Kayıt Kurulusu

- Merkezi Kayıt Kuruluşu

Millî Savunma Bakanlığı

- ASAL Hizmetleri
- ASAL Adres Bilgileri Teyidi ve Güncellenmesi
- ASAL Son Yoklama Bilgi Formu
- ASAL Celp Dönem Tercihi
- Yedeklik Yoklama Hizmetleri
- Sevk Edilecek Eğitim Merkezi
- Personel Seferberlik Hizmetleri
- Personel Seferberlik Tatbikat Sorgulama
- Personel Sefer Görev Emri Sorgulama
- Lojistik Seferberlik Hizmetleri
- Kara Nakil Araçları için Lojistik Sefer Görev Emri Sorgulama
- Deniz Nakil Araçları için Lojistik Sefer Görev Emri Sorgulama
- Hava Nakil Araçları için Lojistik Sefer Görev Emri Sorgulama
- İş Makineleri için Sefer Görev Emri Sorgulama
- Kara Yolu Özel Nakliyat Firmaları Lojistik Seferberlik Sorgulama
- Deniz Yolu Özel Nakliyat Firmalari Lojistik Seferberlik Bilgisi Sorgulama
- Hava Yolu Özel Nakliyat Firmalari Lojistik Seferberlik Bilgisi Sorgulama

- Mal ve Hizmet (Ürünler) ile ilgili Firmalar için Lojistik Seferberlik Bilgisi Sorgulama
- Sağlık Tesisleri için Lojistik Seferberlik Bilgisi Sorgulama
- Turistik Tesisler için Lojistik Seferberlik Bilgisi Sorgulama
- Tersaneler için Lojistik Seferberlik Bilgisi Sorgulama
- Özel Insaat Firmalari Lojistik Seferberlik Bilgisi Sorgulama
- Harp Sanayi Firmalari Lojistik Seferberlik Bilgisi Sorgulama
- MSB Bilgi Edinme Hakkı Hizmetleri
- MSB Gerçek Kişi Bilgi Edinme Başvurusu
- MSB Gerçek Kişi Bilgi Edinme Başvurularını Sorgulama
- MSB Bilgi Edinme Hakkı Hizmetleri
- MSB Tüzel Kişi Bilgi Edinme Başvurusu
- MSB Tüzel Kişi Bilgi Edinme Başvurularını Sorgulama
- Diğer Kurumsal Hizmetler
- Diğer Kurumsal e-Devlet Hizmetleri

Milli Eğitim Bakanlığı

- Milli Eğitim Bakanlığı Öğrenci Bilgi Sistemi
- MEB Sınav Sonuç Sorgulama
- MEB Sınav Yeri Sorgulama

Nüfus Vatandaşlık İşleri Genel Müdürlüğü

- Adres Değişikliği Bildirimi

PTT

- En Yakın PTT
- PTT Kayıtlı Gönderi Takibi

Sağlık Bakanlığı

- Aile Hekim Bilgisi Sorgulama
- Organ Nakli Bilgisi Sorgulama
- Yeşil Kart Durum Bilgisi Sorgulama

Sivil Havacılık Genel Müdürlüğü

- Uçuş Mürettebatı Lisans/Rating Müracaatı

Sosyal Güvenlik Kurumu

- 4A Hizmetleri
- 4A Almanya/Bulgaristan Emekli Ödemeleri
- 4A Banka ve Adres Degisikligi
- 4A Emekli Aylık Bilgisi
- 4A Emekli Aylığı Kesintileri
- 4A Emekli Ödeme Bilgileri
- 4A Emeklilik Kaydı
- 4A Hizmet Dökümü
- 4A Müstahaklık Bilgisi
- 4A Sigortalı Tescil Kaydı Tespiti
- 4B Hizmetleri
- 4B Banka ve Adres Degisikligi
- 4B Basamak Bilgisi
- 4B Borç Durumu
- 4B Emekli Aylık Bilgisi
- 4B Emekli Aylığı Kesintileri
- 4B Hak Sahipliği
- 4B Hizmet Bilgisi
- 4B Müstahaklık Bilgisi
- 4B Tescil Kaydı
- 4B Ödeme Dökümü
- 4C Hizmetleri
- 4C Emeklilik İşlemleri Evrak Takibi
- 4C 2022 Sayılı Kanun Kapsamında Evrak Takibi
- 4C Banka Degisikligi

- 4C Bir Aylik Maas Tercihi
- 4C Emekli Aylık Bilgisi
- 4C Emekli Aylığı Kesintileri
- 4C Hak Sahipligi (Çalışan)
- 4C Hak Sahipliği (Emekli)
- 4C Müstahaklik Bilgisi
- 4C Tescil Kaydı
- 4C İsteğe Bağlı Ödeme Dökümü
- Ortak (4A/4B/4C) Hizmetler
- 4A/4B/4C Muayene Katılım Payı Sorgulama
- 4A/4B/4C İlaç Kullanım Süresi Sorgulama
- SPAS Müstahaklik Sorgulama(Saglik Provizyon Aktivasyon Sistemi)
- 4A/4B Isgöremezlik Ödemesi Görme
- Diger Hizmetler
- 4A Hizmet Dökümü Barkod Doğrulama
- Hekim Bilgilendirme
- Sahis Ödeme Durumlari Görüntüleme
- Tedavi Bilgileri Sorgulama

Tapu ve Kadastro Genel Müdürlüğü

- Tapu Bilgileri Sorgulama
- Tapu Harç Sorgulama

TBMM Başkanlığı

- TBMM İnternet Üzerinden Randevu
- TBMM e-Dilekçe Hizmeti

T.C. Merkez Bankası

- Günlük Döviz Kurları

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

- Araç Muayene İşlemleri

- Araç Muayene Sorgulama
- Denetim İşlemleri
- Ceza Sorgulama
- Uyarı Sorgulama
- Firma İşlemleri
- Firma Sorgulama
- Taşıma Kapasitesine Göre Firma Sorgulama
- Uluslararası Firma Sorgulama
- Mesleki Yeterlilik İşlemleri(SRC/ODY/ÜDY)
- Mesleki Yeterlilik Belgesi Sorgulama
- Sınav Bilgileri Sorgulama
- Meslek Kursları Sorgulama
- Eğitim Tamamlama Belgesi(Sertifika) Sorgulama
- Mesleki Yeterlilik Sınav Başvuru/Güncelle
- Sınav Başvuru Sorgulama
- Sınav Giriş Belgesi Sorgulama
- Sınav Sonuç Sorgulama
- TÜVTURK
- TÜVTURK Mobil Muayene İstasyon Bilgisi Sorgulama
- TÜVTURK Muayene Durum Sorgulama
- TÜVTURK Muayene Randevu Kayıt
- TÜVTURK Muayene Randevu Listeleme
- TÜVTURK Muayene Randevu İptal
- TÜVTURK Muayene İstasyon Bilgisi Sorgulama
- Yetki Belgesi İşlemleri
- Araç Yetki Belgesi Sorgulama
- Başvurularımı Sorgulama
- Firma Acente Sorgulama

- Firma Şube Sorgulama
- Güzergah Sorgulama
- Taşıt Yetki Belgesi Sorgulama
- Yetki Belgesi Basvuru Durum Sorgula
- Yetki Belgesi Detay Sorgulama
- Yetki Belgesi Sorgulama
- Yetki Belgesi Yeterlilik Sorgula

Denizcilik Müsteşarlığı

- Booklet Plan ve Dökümantasyon Tetkik ve Onayları
- Freeboard Hesapları ile Plan Tetkik ve Onay Ücreti(ısim, sicil limanı, numarası vb. değişimi durumlarında)
- Freeboard Hesapları ile Plan Tetkik ve Onayı
- Gemi Denge Yükleme Bilgileri Booklet Onay Ücreti(ısim, sicil limanı, numarası vb. değişimi durumlarında
- Gemi Denge Yükleme Bilgileri Booklet Onayı
- Gemi Yaralı Denge ve Yükleme Booklet Onay Ücreti(İsim, sicil limanı, numarası vb. değişimi durumlarında)
- Gemi Yaralı Denge ve Yükleme Booklet Onayı
- Yolcu Gemileri Yangın Emniyet Planı - Can Kurtarma Emniyet Planı - Gemi Plan Onay Ücreti (İsim, sicil limanı, numarası vb. değişimi durumlarında)
- Yolcu Gemileri Yangın Emniyet Planı - Can Kurtarma Emniyet Planı - Gemi Plan Onayı
- Yük Bağlama El Kitabı, SOPEP, SMPEP Onay Ücreti (ısim, sicil limanı, numarası vb. değişimi durumlarında)
- Yük Bağlama El Kitabı, SOPEP, SMPEP Onayı
- Deniz Ticareti Genel Müdürlüğü Harç Kalemleri - Acente İşlemleri
- Gemi Acenteliği Yetki Belgesi Ücreti
- Gemi Acenteliği şube Yetki Belgesi Ücreti
- Gemi Acentesi Yetki Belgesi Değişikliği Ücreti
- Deniz Ticareti Genel Müdürlüğü Harç Kalemleri - Düzenli Hat Belgelendirme Ücreti

- Denize Elverişlilik Belgesi
- Diğer Denetim Ücretleri
- CLC 92 Sertifikası
- Gemilerde Kullanılan Donanım için Tip Onayı
- Limbo Gözetim İşlemleri
- Özet Kayıt (CSR) Belgesi
- GMDSS Cihazlarına Kıyıda Bakım Yetki Belgesi - Belgelendirme
- Gemi Adamı Donatımında Asgari Emniyet Belgesi
- Gemi Jurnallerinin Liman İdarelerinde Tasdiki
- Gemi Sicilinde Yapılan Kayıt Düzeltmeleri
- Gemi Siciline Atıf Yapan Belge Suretleri ile Sicil Kayıt Suretleri
- Gemi Söküm Bölgesi Dışı, Gemi Söküm Yetki Belgesi
- Gemi Sörvey Belgeleri
- Muafiyet Belgesi
- Telsiz - Telgraf Emniyet Belgesi
- Uluslararası Yükleme Sınır Belgesi
- Yolcu Gemisi Emniyet Belgesi
- YüK Gemisi Telsiz - Telefon Emniyet Belgesi
- Yük Gemisi Teçhizat Emniyet Belgesi
- Yük Gemisi İnşa Emniyet Belgesi
- Gemi Tasdiknamesi
- Gemi İnşa ve Tersaneler Genel Müdürlüğü Harç Kalemleri - Tekne İmal Alanı İşlemleri
- Mevcut Tekne İmal Alanı Organizasyonu ve Yerleşim Planı Onayı Bedeli
- Tekne İmal Alanı Kısmi İşletme İzni Belge Bedeli
- Tekne İmal Alanı Organizasyonu ve Yerleşim Planı İçin İTDK'ca Mahallinde İnceleme
- Tekne İmal Alanı İçin Yeni Yüzer Havuz Başvuru Bedeli
- Tekne İmal Alanı İşletme İzni Belge Bedeli

- Gemi İnşa ve Tersaneler Genel Müdürlüğü Harç Kalemleri - Tekne İmal ve Çekek Alanı İşlemleri
- Gemi İnşa ve Tersaneler Genel Müdürlüğü Harç Kalemleri - Tersane İşlemleri
- Mevcut tersane alanı organizasyonu ve yerleşim planı onayı bedeli
- Tersane kısmi işletme izni belge bedeli
- Tersane Alanı Organizasyonu ve Yerleşim Planı (İdarece Mahilinde İncelenmesi Gerekli Görülen)
- Tersane Mevcut Yüzer Havuzlarla İlgili Başvuru
- Tersane için İTDKca mahallinde inceleme
- Tersane işletme izni belge bedeli
- Gemilerde Bulunan Yangın ve Can Kurtarma Teçhizatı Test Muayene Firmalarının Kontrol ve Onayı
- Harç Mevzuuna Giren İşlemlerin Terkini
- Kayıtlı Gemi Ölünceye Kadar Bakma Akdi Temliki
- Kayıtlı Gemi Üzerinde Tesis Olunacak İpotek
- Kayıtlı Gemi İvaz Karşılığı Temliki veya Tescil Düzenlemesi
- Kayıtlı Gemi İvaz Karşılığında Mukavele İle İntifa Hakkı Tesisi
- Kira Mukavelelerinin Gemi Siciline Şerhi
- Kondüsyon Değerlendirme Sörveyi
- Liman Devleti Kontrolü
- Liman ve Kıyı Yapıları - Liman ve Kıyı Tesisleri Geçici İşletmeye / İşletmeye Açılma Sörvey Hizmetleri
- STCW Belgeleri
- Su Motorsikleti İşlemleri / Muafiyet Belgesi
- Su Altı Motosikleti Kayıt Belgesi Verilmesi
- Su Motosikleti İmalat Yetki Belgesi Verilmesi
- Su Motosikleti İmalat Yetki Belgesi Vizesi
- Su Üstü Motosikleti (Jet-Ski)Kayıt Belgesi Verilmesi
- Uluslararası Sözleşmeler Kapsamındaki Muafiyet Belgeleri

- Transitlog Belgesi
- Türk Bayraklı Gemilere Yapılan Sörveyler
- Türk Boğazlarındaki Zorunlu Denetim (Survey) Hizmetleri
- Türk Uluslararası Gemi Sicil Kayıt Harcı
- Ulaştırma Bakanlığı Bayrak Şehadetnameleri
- Uluslararası Sözleşmeler Gereği Yapılması Zorunlu Sörveyler
- CAS Uygunluk Belgesi
- Can Kurtarma Donanımları Muayene ve Test Sertifikası
- Can Kurtarma Filikaları Muayene ve Test Sertifikası
- Can Kurtarma Salları Muayene ve Test Sertifikası
- DOC (ISM) Şirket Uygunluk Belgesi
- IAPP (Uluslararası Hava Kirliliğinin Önlemesi Belgesi)
- IOPP (Uluslararası Petrolle Kirlenmenin Önlemesi Belgesi)
- ISPP (Uluslararası Pis Sular ıle Deniz Kirlenmesini Önleme Belgesi)
- Katı Yük Taşıma Uygunluk Belgesi
- Muafiyet Belgesi
- Organik Tutulma Önleyici Sistem Kaydı
- Organik Tutulma Önleyici Sistem Uygunluk Belgesi
- Petrol Tankeri Operasyonlarının Emniyetli Yürütüldüğüne Dair Belge
- RadyoEmniyet-Telsiz Telefon Emniyet Belgesi
- SMC (ISM) Emniyetli Yönetim Belgesi
- Tahıl Taşıma Uygunluk Belgesi
- Tehlikeli Yük Taşıma Uygunluk Belgesi
- Uluslararası Yükleme Sınır Belgesi
- Yangın Söndürme Sistemleri Muayene ve Test Sertifikası
- Yolcu Gemisi Emniyet Belgesi
- Yük Gemisi Teçhizat Emniyet Belgesi
- Yük Gemisi İnşa Emniyet Belgesi

- Yerinde Söküm Sörveyi
- Yeterlilik Belgesi
- Yola Elverişlilik Belgesi - Liman Çıkış Belgesi
- Yıllık Tonaj Harcı
- Ölçme Belgesi
- Ötv'siz Yakıt Alım Defteri / Gemi Hareket Kayıt Jurnali
- Gemi Hareket Kayıt Jurnali
- Ötv'siz Yakıt Alım Defteri
- Özel Tekne Belgesi Ücreti
- Özel Yat Kayıt Belgesi
- Üç Gün ve Daha Fazla Demirde Kalma Ücreti

Çevre ve Şehircilik Bakanlığı

- Yapı Kooperatifleri Giriş Uygulaması

Yüksek Öğrenim Kredi ve Yurtlar Kurumu Genel Müdürlüğü

- Kredi Yurtlar Kurumu Burs Basvurusu Sorgulama
- Kredi Yurtlar Kurumu Katki Kredisi Sorgulama
- Kredi Yurtlar Kurumu Kredi Geri Ödeme Sorgulama
- Kredi Yurtlar Kurumu Kredi Numarasi Sorgulama
- Kredi Yurtlar Kurumu Yeniden Yapilandirma Kredi Geri Ödeme Sorgulama
- Kredi Yurtlar Kurumu Yurt Basvurusu Sorgulama
- Kredi Yurtlar Kurumu Ögrenim Kredisi Sorgulama

Mahalli İdareler Genel Müdürlüğü

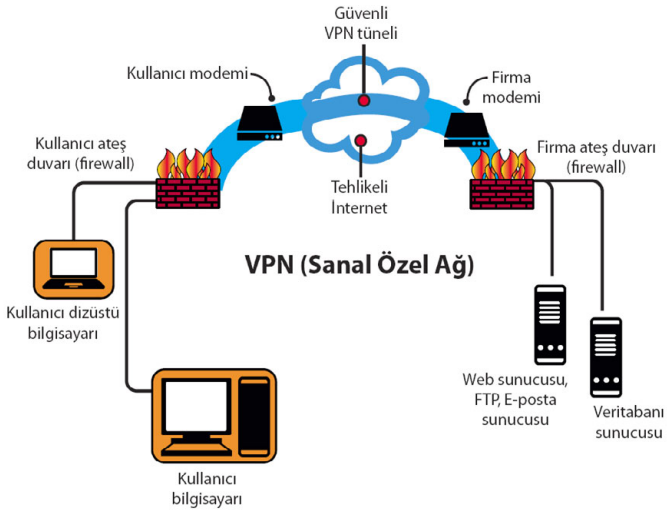
- Yerel Bilgi Giriş Uygulaması

Son erişim: 2 Mayıs 2012

Ek-2: VPN ve BitTorrent

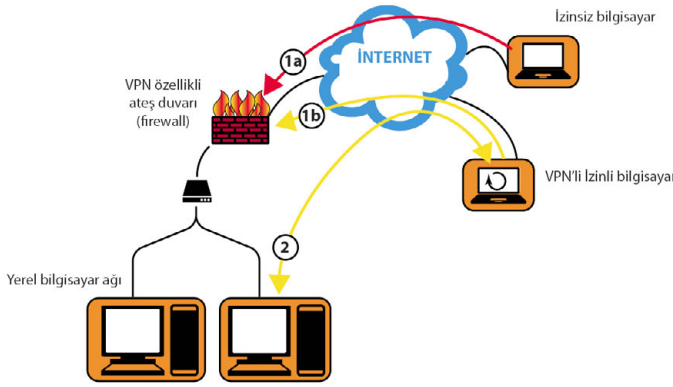
VPN Nedir?

VPN (Virtual Private Network - Sanal Özel Ağ) ağlara güvenli bir şekilde uzaktan erişimde kullanılan bir teknolojidir. Sanal bir ağ uzantısı yarattığından uzaktan bağlanan makine konuk gibi değil, ağa fiziksel olarak bağlıymış gibi görünür. Günümüzde firma ve kurumlar tarafından yaygın olarak kullanılan VPN, çalışanların nerede olursa olsun güvenli bir şekilde kurumlarının bilgisayar ağlarına bağlanmalarını sağlar. VPN üzerinden bir bilgisayar ağına bağlandığınızda bilgisayarınıza İnternet'e girdiği IP adresinin dışında başka bir IP adresi verilir.



VPN bağlantısı

VPN kullanılmasının nedenleri arasında: - Güvenli veri transferi ve bunun şifreli gerçekleşmesi - Gerçek IP adresinizi gizlemek - Başka bir IP adresi almak (ör. başka bir ülkeden) - Proksi ve filtreleri aşma - Engellenmiş sitelere erişim - Engellenmiş içeriklere erişim (ör. BBC iPlayer gibi)



VPN Çalışma Şekli

VPN Nasıl Çalışır?

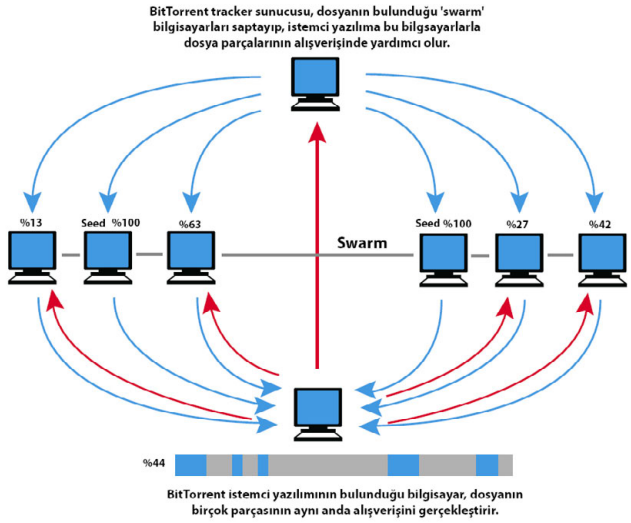
Kullanıcı VPN bağlantısını açıp kullanıcı adı ve şifresini girdikten hemen sonra VPN bağlantısı gerçekleştirilir. Örneğin kullanıcı ofise VPN üzerinden bağlandığında dosya ve diğer kaynaklara erişebilir. VPN üzerinden transferi yapılan veriler şifreli olarak gönderilirler.

BitTorrent Nedir?

BitTorrent İnternet üzerinden dosya paylaşım yazılımına ve aynı tekniği kullanan dosya takas sistemine verilen isimdir. Diğer eşten eşe paylaşım programlarından farkı; sabit olmayan bağımsız sunucu tanımlama dosyaları sayesinde sabit bir sunucuya ihtiyaç olmaksızın paylaşıma devam etmesidir. BitTorrent'in bir başka özelliğiyse dosya indirebilmeniz için, indirilmesine izin vermeniz gerekir. Yani başkalarıyla ne kadar çok dosya paylaşırsanız o kadar hızlı indirme yapabilirsiniz. Öte yandan İnternet bant genişliğini daha verimli kullanabilmek için BitTorrent indireceğiniz dosyaların değişik parçalarını aynı anda farklı bilgisayarlardan indirir. Örneğin kimi Linux işletim sistemi dağıtımları yeni çıkardıkları işletim sistemi sürümlerinin dağıtımını BitTorrent üzerinden gerçekleştirmektedir.

Adım adım BitTorrent şu şekilde çalışır:

- Bir web sayfasında bir dosya bağlantısına tıklıyorsunuz.
- BitTorrent istemci yazılımı bir 'tracker'la bağlantıya geçip BitTorrent çalıştıran ve istenilen dosyanın tamamını ('seed' bilgisayarlar) ya da dosyanın bir parçasını bulunduran (bunlar da bu dosyayı indirme aşamasındaki bilgisayalar olabilir) bilgisayarları bulur.
- 'Tracker' 'swarm'u belirler. Bu dosyanın tamamına ya da bir kısmına sahip alma ya da gönderme aşamasındaki bağlı bilgisayarlardır.



BitTorrent çalışma şekli

- 'Tracker' istemci yazılımın swarm'da bulunan diğer bilgisayarlarla istenilen dosyanın parçalarının değiş tokuşunun yapılmasını sağlar. Bilgisayarının dosyanın değişik parçalarını aynı anda alır.
- Eğer dosyanın tamamını indirdikten sonra BitTorrent yazılımını çalıştırmaya devam ederseniz, diğerleri .torrent dosyalarını bilgisayarınızdan alabilirler. Bu da sizin gelecekteki dosya indirmeleriniz daha hızlı olacaktır.

Ek-3: İnternet'te Anonimliğinizi ve Güvenliğinizi Korumanın Yolları

E-posta okuduğunuzda ya da Facebook sayfanızı güncellediğinizde, ya da banka hesabınızı kontrol ettiğinizde birçok noktada sizin İnternet trafiğiniz kaydedilir. Tor kullanarak trafiğinizi anonim hale getirebilir ve HTTPS kullanarak da veri alışverişinizi şifreleyebilirsiniz. Bu yolla iyi bir düzeyde korunma sağlarsınız. Ancak bu araçları kullanarak sınırlı bir korunma sağlarsınız. Çünkü İnternet Servis Sağlayıcınız ve ziyaret ettiğiniz siteler hala sizin hakkınızda bir takım bilgilere sahip olabilir.

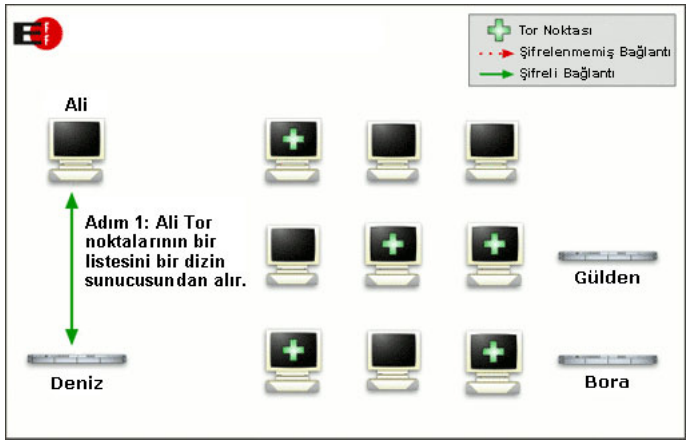
Güvenliğiniz ve anonimliğinizi kimi devletlerin dinlemesine karşı korumak göreceli olarak daha zordur. İnternet servis sağlayıcılarının kontrol edildiği ülkelerdeki İnternet kullanıcıları hangi tür dinlemelere maruz kalabileceklerinin farkında olmalılar. Aşağıda Tor'un çalışma prensibi ve TOR ve HTTPS kullanarak ne tür bir korunmaya sahip olabileceğiniz şemalarla anlatılmaktadır.

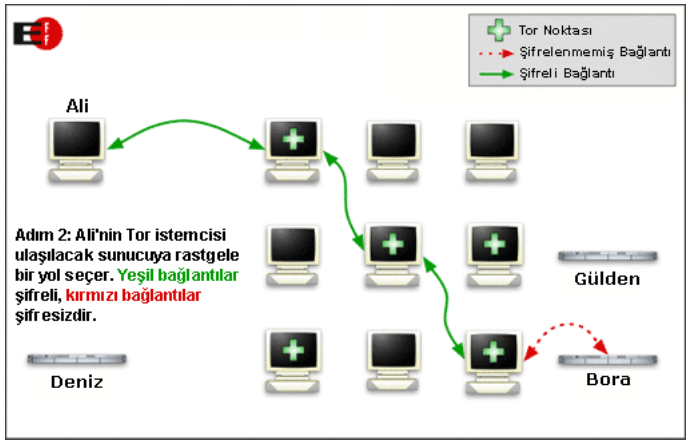
Tor Nedir ve Nasıl Çalışmaktadır?

Tor (The onion router ya da soğan yönlendirici) çevrimiçi anonimliğinizi korumayı amaçlayan özgür bir yazılımdır. Bunun için dağıtık anonim bir ağ mantığıyla çalışır. İnternet üzerinde size tam olmasa da büyük ölçüde bir anonimlik sağlar.

İlk aşamada bilgisayarınıza kurmuş olduğunuz Tor yazılımı bir dizin sunucusundan Tor noktalarının listesini indirir.

Bir web sayfası ya da e-posta sunucusu gibi bir sunucuya erişmek istediğinizde Tor ağ üzerinde bağlanılmak istenilen sunucuya giden özel bir yol oluşturur. Bunun için üzerinden geçilen her bir tor noktası verinin yalnızca hangi noktadan geldiğini ve hangi noktaya gideceğini bilir. Bu bağlantıların her biri şifrelidir.



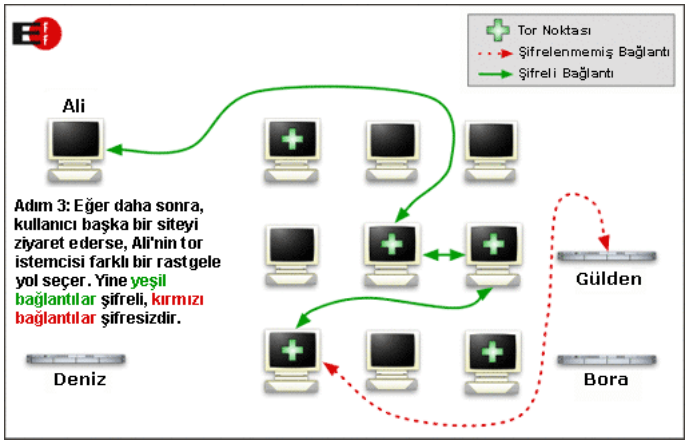


Yani üzerinden geçilen herhangi bir nokta verinin geçeceği bütün yolu bilemez. Bu yolla hattı dinleyen biri bağlantının hangi noktalar arasında kurulduğunu belirleyemez. Verimlilik için Tor yazılımı belli bir süre aynı yoldan giderken daha sonraki bağlantılar yeni bir yoldan kurulur.

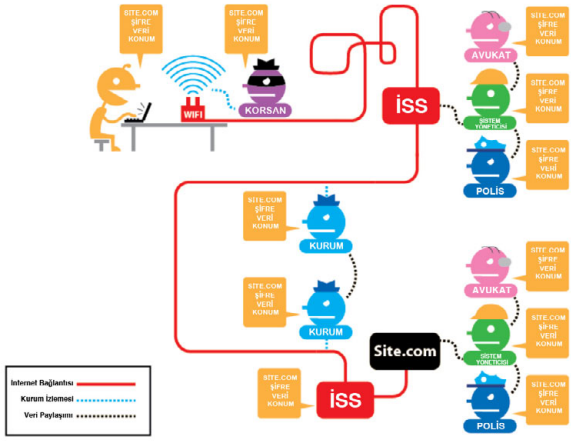
Kaynak: https://www.torproject.org/about/overview.html.en

HTTPS Everywhere

HTTPS Everywhere eklentisi Tor Projesi ve Electronic Frontier Foundation'ın ortak bir çalışmasıdır. İnternet'te birçok web sitesi https üzerinden şifreli haberleşmeye kısıtlı destek vermektedir ve öntanımlı olarak şifrelenmemiş olarak http üzerinden haberleşmeyi kurar ya da şifreli olsalar bile şifrelenmemiş sitelere bağlantı vermektedir. HTTPS Everywhere eklentisi bu sorunları yamayarak bütün



yapılan bağlantılara https üzerinden istekte bulunur. HTTPS ve Tor'un sağladığı İnternet'teki anonimlik ve güvenliği aşağıdaki şemalarda görebilirsiniz.

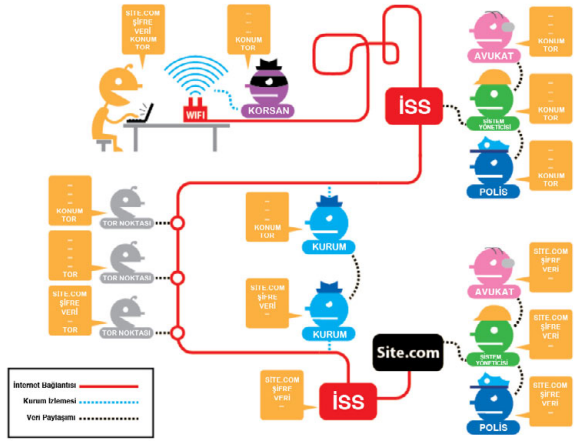


Kullanılmadıkları zaman

Başka ne yapılabilir?

Bunların yanında daha fazla korunma için web'de gezinirken web tarayacınıza ekleyebileceğiniz eklentileri ve destekledikleri web tarayıcıları aşağıda verilmiştir.

- Abine (korunma paketi) (Firefox | Chrome)
- Adblock Plus (reklamları engeller) (Firefox | Chrome)

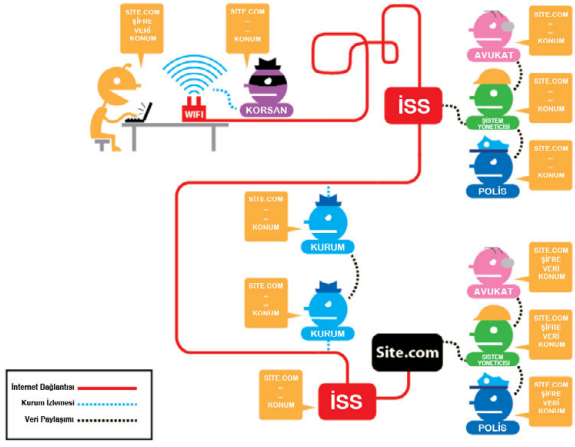


Yalnızca Tor kullanıldığında

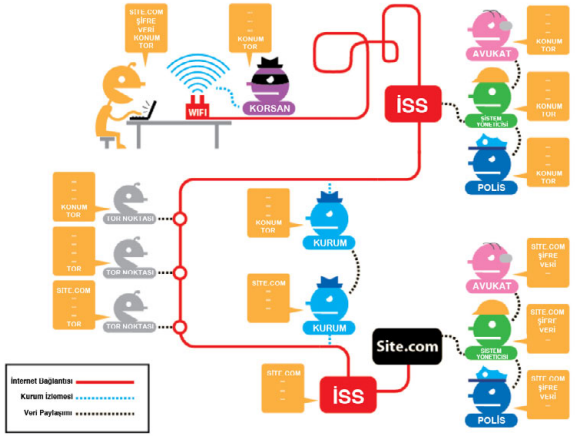
- AdBlock (reklamları engeller) (Safari | Chrome)
- AdSweep (reklamları engeller) (Opera | Chrome)
- Beef Taco (reklam amaçlı sizi izleyen çerezleri engeller) (Firefox)
- Disconnect (belli başlı sitelerin sizi izlemesini engeller) (Chrome | Firefox | Safari)
- Ghostery (üçüncü tarafların izlemesini engeller) (IE | Safari | Chrome | Firefox)
- RequestPolicy (üçüncü tarafların izlemesini düzenler) (Firefox)
- RefControl (siteye ne gönderildiğini düzenler) (Firefox)
- BetterPrivacy (Flash çerezlerini engeller) (Firefox | Others)
- NoScript (JavaScript'leri engeller) (Firefox)
- ScriptNo (JavaScript'leri engeller) (Chrome)
- NotScripts (JavaScript'leri engeller) (Opera)

Web'de arama yaparken kullanıcı bilgilerinizi kaydetmeyecek bir arama motoru kullanmanız önerilir. Buna bir örnek DuckDuckGo sitesi (http://www.duckduckgo.com).

Kaynak: http://donttrack.us/



Yalnızca HTTPS kullanıldığında



Hem HTTPS, hem de TOR kullanıldığında

Ek-4: Veri Koruma Örgütleri

- **State Watch** (http://www.statewatch.org)
- **Int. Campaign Aganst Mass Surveillance** (http://www.i-cams.org)
- **Electronic Privacy Information Center** (http://www.epic.org)
- **Sanal Veri Koruma Ofisi** (http://www.datenshutz.de)
- **European Digital Rights** (http://www.edri.org)

Kaynakça

Kitap ve Makaleler

Abe, K. (2004). "Everyday Policing in Japan: Surveillance, media, Government and Public Opinion", *International Sociology*, 19, s.215-231.

Abe, K. (2006). "Technologies of Surveillance", Theory Culture Society, 23, s.265-267.

Abe, K. (2009). "The Myth of Media Interactivity. Technology, Communications and Surveillance in Japan", *Theory Culture Society*, 26, s.73-88.

Arifoğlu, A. (2004). *E-Dönüşüm: Yol Haritası, Türkiye, Dünya*, Ankara: Sas Bilişim Yayınları.

Ayman-Güler, B. (2003). "Yönetişim, Tüm İktidar Sermayeye", *Praksis Dergisi*, 9, s. 93-116.

Ball, K. ve Webster, F. (2003). "Intensification of Surveillance", K. Ball ve F. Webster (der.), *Intenstification Surveillance* içinde, London: Pluto, s.1-15.

Baker, U. (2001). "F-tipi, Mernis ve İnternet: Hapishanenin İçi ve Dışı", *Birikim*, 142-143, s.17-22.

Baruh, L. (2007). "Read at Your Own Risk: Shrinkage of Privacy and Interactive Media", New Media & Society, 9(2), s.187-211.

Baruh, L. ve Soysal, L. (2009). "Public Intimacy and the New Face(book) of Surveillance: Role of Social Media in Reshaping of Contemporary Surveillance", T.Dumova ve R. Fiordo (der.), *Handbook of Research and Colloboration Software: Concepts and Trends* içinde, Heshey: PA. IGI Global, s.392-463.

Bauman, Z. (2005). *Bireyselleşmiş Toplum*, çev. Yavuz Alogan, İstanbul: Ayrıntı Yayınları.

Bauman, Z. (2006). *Küreselleşme*, çev. Abdullah Yılmaz, İstanbul: Ayrıntı Yayınları.

Baumann, Z. (2000). *Postmodernlik ve Hoşnutsuzlukları*, çev. İsmail Türkmen, İstanbul: Ayrıntı.

Bayne, S, (2004) "Smoothness and Striation in Digital Learning Spaces" *E-Learning*, C.1, S.2, s. 302-316.

Bayramoğlu, S. (2005). *Yönetişim Zihniyeti, Türkiye'de Üst Kurullar ve Siyasal İktidarın Dönüşümü*, İstanbul: İletişim Yayınları.

Bayramoğlu, S. (2002), "Küreselleşmenin Yeni Siyasal İktidar Modeli: Yönetişim", *Praksis Dergisi*, Ankara, S.7, s.85-116

Beck, U. (2011). *Risk Toplumu: Başka Bir Modernliğe Doğru*, çev. Kazım Özdoğan ve Bülent Doğan, İstanbul: İthaki Yayınları.

Bennett, C. J.(1992), *Regulating Privacy, Data Protection and Public Policyin Europe and the United States*, Cornell University Press.

Bentham, J. (2008). "Panoptikon ya da Gözetim-Evi", çev. Zeynep Özarslan, B. Çoban ve Z. Özarslan (der.). *Panoptikon: Gözün İktidarı* içinde, İstanbul: Su Yayınları.

Bereano, P. (2000). "Washington", Public Health, Vol. 17 Fall, s. 19-21, http://www.doh.wa.gov/sboh/Goals/Past/Genetics/2002_02-25/docs/Tab05-BereanoArticle.pdf, (Erişim tarihi: 15 Temmuz 2011).

Best, K. (2010). "Living in the Control Society: Surveillance, Users and Digital Screen Technologies", *International Journal of Cultural Studies*, 13(1), s.5-24.

Bildirici, F. (1998) *Gizli Kulaklar Ülkesi*. İstanbul: İletisim.

Binark, M., (2005). "İnternet'i veya Bilgisayar Dolayımlı İletişim Ortamını İncelemek İsteyen Bir Araştırmacının Soruları ve Sorunları", M. Binark ve B. Kılıçbay (der.) *İnternet, Toplum, Kültür* içinde, Ankara:Epos yayınları içinde, 177-190.

Bozok, N. (2011). "Biyoiktidara Özgü Bir Özne(l)leşme Pratiği Olarak Popüler Sağlıklı Yaşam Söylemi", *Toplum ve Bilim*, S.122, s.37-52.

Bygrave, L. (2002). *Data Protection Law*, Kluwer Law International, Hollanda 2002.

Castells, M. (2005). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür. Birinci Cilt: Ağ Toplumunun Yükselişi*. Çev. Ebru Kılıç. İstanbul: Bilgi Üniversitesi Yayınları.

Clarke, R. (1988). "Information Technology and Dataveillance", *Communications of the ACM*, 31 (5), s.498-512.

Conti, J.P. (2011). "Is Seeing Deceiving?", *Engineering and Technology Magazine*, Volume 6, Issue 3., s.70-71.

Creifelds, C. vd. (1997). *Rechtswörterbuch*, Münih: Beck.

Çavlin-Bozbeyoğlu, A. (2011). "Türkiye'nin Biyometrik Elektronik Kimlik Kartı Sistemi", *Toplum ve Bilim*, S.122. syf. 53-74.

Çelebi, A. (2002). "Risk ve Olumsallık: Sosyal Teori ve Sosyal Felsefe İlişkisini Anlamaya Yönelik İki Anahtar Kavram", *SBF Dergisi*, 56 (1), s.23-52.

Çoban, B. (2008). "Gözün İktidarı Üzerine", B. Çoban ve Z. Özarslan (der.), *Panoptikon: Gözün İktidarı* içinde, İstanbul: Su Yayınları.

Çomu, T. (2011). *Yeni Medyada Nefret Söylemi*. İstanbul: Kalkedon Yayınları.

Dandeker, C. (1990). *Surveillance, Power, and Modernity*, Cambridge: Polity Press.

De Mul, J. (2008). *Siberuzayda Macera Dolu Bir Yolculuk*, çev. Ali Özdamar, İstanbul: Kitap Yayınevi.

Deleuze, G., (2006), "Denetim Toplumları Üzerine Ek", *Müzakereler*, çev. İnci Uysal, İstanbul: Norgunk Yayıncılık.

Diken, B. (2011). *Nihilizm*, Çev. Aylin Onacak, İstanbul: Ayrıntı Yayınları.

Dolgun, U. (2008). *Şeffaf Hapishane Yahut Gözetim Toplumu*, Ankara: Ötüken Yayıncıklık.

Dyson, E. (2008). "Reflection on Privacy 2.0", *Scientific American*, s.50-55.

Early, L. (1993) "Science, Technology and Human Rights: The Role of Data Protection", *Human Rights in the Twenty-first Century, A Global Challenge*, C.2, (Haz.). Katleen E. Mahoney, Paul Mahoney, Maritus Nijhoff Publishers, syf. 801-815.

Ekici, G. (2007). *Kamu Kurumlarının E-Devlet Uygulamalarında Vatandaş Bilgilerinin Güvenliği ve Korunması*. Hacettepe Üniversitesi SBE. Yayınlanmamış Y.Lisans Tezi.

EMO. (2009). *E-Gözaltı Raporu*, Ankara: EMO.

EPIC, (2006). *Privacy and Human Rights Report*.

Esen, S., Gönenç, L. (2008). "Religious Information on Identity Cards: a Turkish Debate", *Journal of Law and Religion*, C. 23, s.2.

Foucault, M. (2000). *Hapishanenin Doğuşu*, çev. Mehmet Ali Kılıçbay, Ankara: İmge.

Foucault, M. (2001). *Ders Özetleri* 1970-1982, çev. Selahattin Hilav, İstanbul: Yapı Kredi Yayınları.

Foucault, M. (2007). İktidarın Gözü, Seçme Yazılar, çev. Işık Ergüden, İstanbul: Ayrıntı Yayınları.

Gambetti, Z. (2007). "Linç Girişimleri, Neo-liberalizm ve Güvenlik Devleti", *Toplum ve Bilim*, No. 109, s. 7-34

Gambetti, Z. (2008). "Foucault'da Disiplin Toplumu-Güvenlik Toplumu Ayrımı",

Mesele, No. 20, s. 43-46.

Gandy, O.H. (2003). "Data Mining and Surveillance in the Post 9-11 Environment", K. Ball ve F. Webster (der.), *Intenstification Surveillance* içinde. London: Pluto, s.26-41.

Gandy, O. (1965). *The Panoptic Sort: A Political Economy of Personal Information*, Colo.: Westview Press.

Ganser, D. (2005). *NATO's Secret Armies: Operation GLADIO and Terrorism in Western Europe*. New York: Routledge.

Garland, D. (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*, Chicago: Chicago University Press.

Giddens, A. (2008). *Ulus Devlet ve Şiddet*, İstanbul: Kalkedon.

Gola, P., Schomerus, R. (2007). *Bundesdatenschutzgesetz Kommentar*, Münih: Beck

Güney, A. (2006). "Bob Jessop'da Yönetişim Kavramı: Stratejik İlişkisel Devlet Biçiminden Yönetişim Biçimine", *Memleket Siyaset Yönetim* 1, s. 153-171.

Günindi, E. (2012). "Elektronik Gözetleme – Büyük Biraderin Şirketleşmesi", *Sendika.org*, http://www.sendika.org/yazi.php?yazi_no=43118, (Erişim tarihi: 1 Mart 2012).

Güzelsarı, S. (2003). "Neoliberal politikalar ve Yönetişim Modeli", *Amme İdaresi Dergisi*, C.36, S.2, s. 17-34.

Hammarberg, T. (2012) *Avrupa'da İnsan Hakları*. (Çev.) Aysen Ekmekçi. İstanbul: İletişim Yayınları.

Hardt, M., Negri, A. (2008). *İmparatorluk*, çev. Abdullah Yılmaz, İstanbul: Ayrıntı Yayınları.

Holland, E.W. (2005). "Şizofreniden Toplumsal Denetime", içinde *Deleuze'de Toplum ve Denetim*, Ali Akay (der.), çev. Barış Başaran, İstanbul: Bağlam Yayınları, s.73-84.

Holland, P. (TARİH EKLENECEK). "Case-Study. Drug Testing in the Australian Mining Industry", *Surveillance and Society*, s.204–209.

İnceoğlu, Y. (2012). *Nefret Söylemi ve/veya Nefret Suçu*. İstanbul: Ayrıntı.

İnsel, A. (2005). *Neoliberalizm: Hegemonyanın Yeni Dili*, İstanbul: Birikim Yayınları.

Kaboğlu, İ.Ö., (2002). *Özgürlükler Hukuku, İnsan Haklarının Hukuksal Yapısı*, İmge, Ankara: İmge Yayınevi.

Karakaya-Polat, R. (2011). "İnternet ve Yurttaşlık Kavramını Dönüşümü", *16. İnternet Konferansı* sunum metni, http://inet-tr.org.tr/inetconf16/bildiri/96.doc, (Erişim tarihi: 10 Ocak 2012).

Karakehya, H. (2009). "Gözetim ve Suçla Mücadele: Gözetimin Tarihsel Gelişimi ile Yakın Dönemde Gerçekleştirilen Hukuki Düzenleme ve Uygulamalar Bağlamında Bir Değerlendirme", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, C.58 S.2, s.319-357.

Kesim-Güven, S. (2011). "Gözetimin Toplumsal Meşruiyeti", Hüseyin Köse (der.), *Medya Mahrem* içinde, s.173-198.

Kesim-Güven, S. (2007). *Gözetim Toplumu ve Toplumsal Meşruiyet*, Mimar Sinan Güzel Sanatlar Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Doktora Tezi.

Kırlıdoğ, M., Uçkan, Ö., Fidaner, I.B. (2011). "Derin Paket İzleme: Mahremiyet ve İletişim Hakları İhlalleri", *XVI. Türkiye'de İnternet Konferansı*, İzmir'de sunulan bildiri.

Kubilay, M.A., Adalıer, O. ve Karademir, A. (2010). "Türkiye'nin E-Kimlik Yolculuğu", *UEKAE Dergisi*, 2(4): s.6-25.

Kumaş, E., Birgören, B. (2010). "E-Devlet Kapısı Projesi Bilgi Güvenligi ve Risk Yönetimi: Türkiye Uygulaması", *Bilişim Teknolojileri Dergisi*, C.3, S.2, s.29-36., http://www.aid.sakarya.edu.tr/uploads/Pdf_2008_1_56.pdf, (Erişim tarihi: 5 Ocak 2012).

Küzeci, E. (2011). "Anayasal Bir Hak: Kişisel Verilerin Korunması", *Bilişim*, Y. 38, S. 128, s.142-149.

Küzeci, E. (2011a). "Devlet Gözetimine Karşı Avrupa İnsan Hakları Mahkemesi Kalkanı", *Bahçeşehir Üniversitesi-Kazancı Hakemli Hukuk Dergisi*, C.7, S. 81-82, s.7-61.

Küzeci, E. (2010). *Kişisel Verilerin Korunması*, Ankara: Turhan Kitabevi.

Lyon, D. (1997). *Elektronik Göz*, çev. Dilek Hattatoğlu, İstanbul:Sarmal Yayınları.

Lyon, D. (2003). "Surveillance after September 11, 2001", K. Ball ve F. Webster (der.), *Intenstification Surveillance* içinde, London: Pluto, 16-25.

Lyon, D. (2003). "Surveillance as Social Sorting:Computer Codes and Mobile Bodies", David Lyon (der.), *Surveillance and Social Sorting: Privacy, Risk and Digital Discrimination* içinde. New York: Routledge. s.13-30.

Lyon, D. (2006a). "9/11 Synopticon and Scopophilia: Watching and Being Watched", K. Haggerty and R. Ericson (der.), *The New Politics of Surveillance and Visibility* içinde, Toronto: University of Toronto Press.

Lyon, D. (2006b). *Gözetlenen Toplum*, çev. Gözde Soykan. İstanbul: Kalkedon Yayıncılık.

Lyon, D. (2007a). "Surveillance, Security and Social Sorting: Emerging Research Priorities", *International Criminal Justice Review* 17, s. 161-170, http://icj.sagepub.com/content/17/3/161, (Erişim tarihi: 28 Şubat 2011).

Lyon, D. (2007b). *Surveillance Studies An Overview*, Cambridge: Polity Press.

Lyon, D. (2010). *ID Surveillance*, Cambridge: Polity Press.

Lyon, L. ve Zureik, E. (2009). "Surveillance, Privacy, and the New Technology", L.A. Lievrouw ve S. Livingstone (der.), *New Media Volume IV: Social Institutions, Structures, Arrangements* içinde. London: Sage, s.256-269.

Mansifeld, N. (2006). *Öznellik: Freud'dan Haraway'e Kendilik Kuramları*, çev. Hüsamettin Çetinkaya ve Rahmi Durmaz. İzmir: Ara-lık.

Marquis, G. (2003). "Private Security and Surveillance: From the "Dossier Society" to Database Networks", David Lyon (der.), *Surveillance and Social Sorting: Privacy, Risk and Digital Discrimination* içinde. New York: Routledge, s.226-246.

Marshall, T.H. (2006). "Yurttaslık ve Toplumsal Sınıflar" içinde T.Humphrey Marshall ve Tom Bottomore (der.)., *Yurttaslık ve Toplumsal Sınıflar*, çev. Ayhan Kaya, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Marx, G.T. (1985). "The Surveillance Society: The Threat of 1984-Style Techniques", *The Futurist*, s.21-26.

Mattelart, A. (2010). *The Globalization of Surveillance*, Cambridge: Polity Press.

Mattelart, A. (2012) *Gözetimin Küreselleşmesi: Güvenlileştirme* Düzeninin Kökeni. (Çev.) Onur Gayretli ve Su Elif Karacan. İstanbul:Kalkedon.

McCahill, M. and Norris, C. (2002). *Urbaneye: CCTV in London*, YAYINEVİ.

Münchener Kommentar zum Bürgerlichen Gesetzbuch (2001) C.1 (m.1-240), (Haz.) K. Rebmann, F.J. Säcker, R. Rixecker, 4. baskı, Beck.

Nunes, M., (2006). *Cyberspaces of Everyday Life*, Minneapolis: University of Minesota Press.

Olgun, C. K. (2007). "Michel Foucault'nun İktidar Kavramına Giriş", *Sosyoloji Notları*, S.1, s.9-14.

Orwell, G. (1989). *Bin Dokuz Yüz Seksen Dört*, çev. Nuran Akgören, İstanbul: Can Yayınları.

Özkazanç, A. (2007). "Biyo-politik Çağda Suç ve Cezalandırma: Denetim Toplumunda Neo-liberal Yönetimsellik", *Toplum ve Bilim*, 108, s.15-51.

Özmen, L.A. (2010). *Türk Nüfus Hizmetleri Sistemi ve Mernis Projesi*, Gazi Üniversitesi SBE. Yayınlanmamış Y.Lisans Tezi.

Poggi, G. (2002). *Modern Devletin Gelişimi*, çev. Şule Kurat, Binnaz Toprak, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Rebmann, K, Säcker, F.J., Rixecker, R. (2001). *ünchener Kommentar zum Bürgerlichen Gesetzbuch*, C.1 (m.1-240), Münih: Beck.

Scott, J. (2008). *Devlet Gibi Görmek*, çev. Nil Erdoğan, İstanbul: Versus Kitap

Yayınları.

Schaar, P. (2009). *Das Ende der Privatspäre, Der Weg in die Überwachungsgesellschaft*, Münih: Goldmann.

Shapiro, M. (2005). "Every Move You Make: Bodies, Surveillance and Media", *Social Text* 83, 23(2), s.21-34.

Shields, P. (2006). "Electronic Networks, Enhanced State Surveillance and the Ironies of Control", *Journal of Creative Communications*, 1 (1), s.19-38.

Simitis, S. (1984). "Die informationelle Selbsbestimmung-Grundbedingung einer verfassungkonformen Informationsordnung", *NJW*, Heft 8, s.398-405.

Singel, R. (2009). "You Deleted Your Cookies? Think Again", *Wired Magazine*, http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/ (Erişim Tarihi: 25 Temmuz 2011).

Stalder, F. ve Lyon, D. (2002). "ID Cards and Social Classification", D. Lyon (der.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* içinde, London ve New York: Routledge, s.77-93.

Şimşek, O. (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması*, İstanbul: Beta.

Tekergül, M. (2010). *İşyerinde Elektronik Gözetim Uygulamaları*, Kadir Has Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi,

Topal, Ç. (2005). "Global Citizens and Local Powers: Surveillance in Turkey", *Social Text* 83, 23(2), s.85-93.

Toprak, A. vd. (2009). *Toplumsal Paylaşım Ağı Facebook: Görülüyorum Öyleyse Varım!*, İstanbul: Kalkedon Yayınları.

Törenli, N. (2004). "Enformasyon Toplumu ve Küreselleşme Sürecinde Türkiye". Ankara: Bilim ve Sanat Yayınları.

Uçkan, Ö. (2003a). *E-devlet, E-demokrasi ve Türkiye*, İstanbul: Literatür Yayıncılık.

Uçkan, Ö. (2003b). "E-Devlet, E-Demokrasi ve E-Yönetişim Modeli: Bir İlkesel Öncelik Olarak Bilgiye Erişim Özgürlüğü", *Stradigma Dergisi*, s.5, http://www.stradigma.com/turkce/haziran2003/makale_09.html. (Erişim tarihi: 15 Aralık 2011).

Uçkan, Ö. (2009). "Türkiye'de Bilgi ve İletişim Teknolojiler Politika Yapım Sürecinin Zaafları: Yönetişim Fobisi", *ICEGOV-Uluslar arası E Devlet ve E Yönetişim Konferansı, 12-13 Mart 2009*, Ankara'da sunulan bildiri.

Uçkan, Ö. (2011). "22 Ağustos: Türkiye İnternetinin Kara Deliği", http://www.gennaration.com.tr/yazarlar/22-agustos-turkiye-internetinin-kara-deligi/, (Erişim Tarihi: 1 Mart 2012).

Webster, F. (2004). *The Information Society Reader*, London: Routledge.

Webster, F. (2003). "Information Warfare, Surveillance and Human Rights", K. Ball ve F. Webster (der.), *Intenstification Surveillance* içinde, London: Pluto, s.90-111.

Werret, S. (2008). "Potemkin ve Panoptikon: Samuel Bentham ve On Sekizinci Yüzyıl Rusyasında Mutlakiyetçi Mimari", B. Çoban ve Z. Özarslan (der.), *Panoptikon: Gözün İktidarı* içinde, İstanbul: Su Yayınları.

Whitaker, R. (1999). *The End of Privacy*, New York: The New Press.

Wohlgemuth, H.H., Gerloff, J. (2005). *Datenschutzrecht, Eine Einführung mit praktischen Fällen*, Münih: Luchterhand.

Yosuntaş, Ç. (2008). *Sahte Kimlik*, Beykent Üniversitesi SBE. Yayınlanmamış Y.Lisans Tezi.

Zamyatin, Y. (2011). *Biz*, çev. Algan Sezgintüredi, İstanbul: Versus Kitap Yayınları.

Zureik, E. ve Hindle, K. (2004). "Governance, Security, and Technology: The Case of Biometrics." *Studies in Political Economy*, Vol. 73, Spring/Summer, s. 113-137.

Haber, Köşe Yazısı, Rapor, vs.

Akıllıoğlu, T. (2004). "İdari Usul ve Kişisel Verilerin Korunması", 11 Ağustos, http://www.idare.gen.tr/akillioglu-idariusul.htm. (Erisim tarihi: 6 Nisan 2012).

American Management Association (2008). "The Latest on Workplace Monitoring and Surveillance", (13 Mart), http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx, (Erişim tarihi: 27 Temmuz 2011).

Andaç, Ş. (2012). "Derin Google kişisel bilgi avında!", *Milliyet Gazetesi*, (30 Ocak), http://teknoloji.milliyet.com.tr/derin-google-kisisel-bilgi-avinda-/internet/haberdetay/30.01.2012/1495550/default.htm, (Erişim tarihi: 26 Şubat 2012).

AVAAZ.org (2012). İnternet gizliliğinin sonu, https://secure.avaaz.org/tr/stop_cispa_corporate_global/?cl=1744899201&v=13751, (Erişim tarihi: 20 Nisan 2012).

Avrupa Güvenlik ve İşbirliği Teşkilatı, "Freedom of Expression on the Internet", http://www.osce.org/fom/80723, (Erişim tarihi: 1 Mart 2012).

Baker, J., European Parliament agrees to send airline passenger data to US, *Computer World UK*, 19 Nisan 2012, http://www.computerworlduk.com/news/public-sector/3352378/european-parliament-agrees-to-send-airline-passenger-data-to-us/, (Erişim tarihi: 21 Nisan 2012).

Bamford, J. (2012). The NSA Is Building the Country's Biggest Spy Center

(Watch What You Say), *Wired Magazine*, 15 March 2012, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1, (Erişim tarihi: 22 Nisan 2012).

BiaNet – Bağımsız İletişim Ağı (2009). "Başbakan'a DTP ve DSP'den İki Ayrı "Dinleme" Önergesi", (19 Kasım 2009), http://bianet.org/bianet/ifade-ozgurlugu/118386-basbakana-dtp-, (Erişim tarihi: 1 Şubat 2012).

BiaNet - Bağımsız İletişim Ağı, "ABD Yolcusu Kalmasın, Bilgileri Gitti Bile", (20 Nisan 2012), http://www.bianet.org/bianet/dunya/137738-abd-yolcusu-kalmasin-bilgileri-gitti-bile, (Erişim tarihi: 21 Nisan 2012).

Boone, J. (2012). CISPA: The internet finds a new enemy, *GlobalPost*, 9 Nisan 2012, http://www.globalpost.com/dispatches/globalpost-blogs/the-grid/cispa-the-internet-finds-new-enemy-sopa, (Erişim tarihi: 20 Nisan 2012).

Chan, A. (2010). "GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated)", (14 Eylül) http://gawker.com/5637234/, (Erişim tarihi: 27 Şubat 2012).

Cyber Intelligence Sharing and Protection Act, *Wikipedia*, https://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act, (Erişim tarihi: 20 Nisan 2012).

Cumhuriyet Gazetesi (2010). "MOBESE'li Kent Sayısı Artıyor", (11 Ağustos), http://www.cumhuriyet.com.tr/?im=yhs&hn=164932. (Erişim tarihi: 1 Şubat 2012).

Eaton, K. (2011). "Google's Eric Schmidt Reveals NFC Smartphone Plans: It's All About Advertising", (16 Şubat), http://www.fastcompany.com/1728241/eric-schmidt-gives-away-googles-nfc-smartphone-plans-its-all-about-advertising, (Erişim tarihi: 23 Temmuz 2011).

Electronic Frontier Foundation (2012). Cybersecurity Bill FAQ: The Disturbing Privacy Dangers in CISPA and How To Stop It, https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it, (Erişim tarihi: 20 Nisan 2012).

Electronic Frontier Foundation (2012). Stop Cyber Spying, https://cyberspying.eff.org/, (Erişim tarihi: 20 Nisan 2012).

Federal Bureau of Investigation (2010). "Statement for the Record of Donald M. Kerr", Assistant Director Laboratory, Division on Internet and Data Interception Capabilities Developed, (24 Temmuz), http://web.archive.org/web/20010308191403/, (Erişim tarihi: 15 Temmuz 2011).

Federal Trade Commission (2010). "Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers", (Aralık), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf, (Erişim tarihi: 20 Temmuz 2011).

Fox News (2005). "FBI Ditches Carnivore Surveillance System", (18 Ocak), http://www.foxnews.com/story/0,2933,144809,00.html, (Erişim tarihi: 15 Temmuz 2011).

Geiger, H. (2011). "NFC Phones Raise Opportunities, Privacy and Security Issues", Center for Democracy & Technology, (11 Nisan), http://www.cdt.org/blogs/harley-geiger/nfc-phones-raise-opportunities-privacy-and-security-issues (Erişim tarihi: 20 Temmuz 2011).

"Google Policies & Principles", http://www.google.com/policies/, (Erişim tarihi: 26 Şubat 2012).

"Google Transparency Report", www.google.com/transparencyreport, (Erişim tarihi: 26 Şubat 2012).

Habertürk (2011). "ODA TV iddianamesi", http://im.haberturk.com/images/others/2011/09/10/odatv_iddianame.doc, (Erişim tarihi: 1 Şubat 2012).

ILO (1993). "Workers' privacy Part II: Monitoring and surveillance in the workplace", Conditions of work digest, Volume 12 Number, Geneva, http://www.ilo.org/public/libdoc/ilo/P/09921/09921(12).pdf, (Erişim tarihi: 27 Temmuz 2011).

ILO (1997). "Protection of workers' personal data", http://www.ilo.org/safework/normative/codes/lang–en/docName–WCMS_107797/index.htm (Erişim tarihi: 27 Temmuz 2011).

ILO Haber Bülteni (2007). "Equality at work - Just a family medical history: genetic testing before getting a job?", (9 Mayıs), http://www.ilo.org/global/about-the-ilo/press-and-media-centre/news/lang–en/WCMS_082589 (Erişim Tarihi: 26 Temmuz 2011.

Kincaid, J. (2010). "This Is The Second Time A Google Engineer Has Been Fired For Accessing User Data", *TechCrunch*, (14 Eylül), http://techcrunch.com/2010/09/14/google-engineer-fired-security/, (Erişim tarihi: 27 Şubat 2012).

Koçbaş, U. (2012). Takip Altındasınız, *OdaTV*, 20 Nisan 2012, http://www.odatv.com/n.php?n=takip-altindasiniz-2004121200, (Erişim tarihi: 22 Nisan 2012).

Milli İstihbarat Teşkilatı, "Merak edilenler", http://www.mit.gov.tr/me_diger.html, (Erişim tarihi: 31 Ocak 2012).

"New Rules on Use of Cookies to Store and Access Your Data", 26 Mayıs 2011, http://www.direct.gov.uk/en/NI1/Newsroom/DG_197239, (Erişim Tarihi: 23 Temmuz 2011).

Milliyet Gazetesi (2011). "CHP'li Acar Başbakan Erdoğan'a dinlemeleri sordu", (15 Eylül) http://siyaset.milliyet.com.tr/chp-li-acar-basbakan-erdogan-a-dinlemeleri-sordu/siyaset/siyasetdetay/15.09.2011/1438856/default

.htm (Erişim tarihi: 31 Ocak 2012).

National Human Genome Research Institute and the Department of Health and Human Services (HHS) (2009). "GINA" The Genetic Information Nondiscrimination Act of 2008, 6 Nisan 2009, http://www.genome.gov/Pages/PolicyEthics/GeneticDiscrimination/GINAInfoDoc.pdf, (Erişim Tarihi: 20 Temmuz 2011).

NTVMSNBC (2009)."Erdoğan: Ben de dinlendim, telekulak çirkin", 16 Kasım 2009, http://www.ntvmsnbc.com/id/25021648/, (Erişim tarihi: 1 Şubat 2012).

Office of the Privacy Commisioner of Canada (2010). "Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing", Mayıs 2011, http://www.priv.gc.ca/resource/consultations/report_201105_e.cfm, (Erişim tarihi: 20 Temmuz 2011).

Pileici, V. (2011). "Privacy watchdog sets sights on Google - Report raises concerns about how Internet giants track, profile and target us", *The Montreal Gazette*, (19 Temmuz), http://www.montrealgazette.com/technology/Privacy+watchdog+sets+sights+Google/5125124/story.html, (Erişim tarihi: 19 Temmuz 2011).

Privacy International (2007). "PHR2006-Privacy Topics-Workplace Privacy", 18 Aralık, https://www.privacyinternational.org/article/phr2006-privacy-topics-workplace-privacy Erişim tarihi: 26 Temmuz 2011).

Privacy International (2012). "Who's Who", https://www.privacyinternational.org/big-brother-incorporated/countries, (Erişim tarihi: 1 Mart 2012).

Radikal Gazetesi (2012). Tartışma yaratan konuşma için açıklama geldi, 21 Nisan 2012, http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetayV3&ArticleID=1085636&CategoryID=78, (Erişim tarihi: 21 Nisan 2012)

Rawnsley, A. (2011). "Pentagon Wants a Social Media Propaganda Machine", *Wired Magazine*, http://www.wired.com/dangerroom/2011/07/darpa-wants-social-media-sensor-for-propaganda-ops/#more-51990, (Erişim Tarihi: 25 Temmuz 2011).

Sağlık Bakanlığı Sağlık-NET Portalı (2012). "Sağlık NET Nedir?", http://www.sagliknet.saglik.gov.tr/portal_pages/notlogin/sagliknetnedir/sagliknetnedir.htm, (Erişim tarihi: 31 Ocak 2012).

Sol Portal (2012). "Telefonlar MİT kriterlerine göre dinleniyorsa, ülke ihanetten geçilmiyor!", 27 Ocak 2012, http://haber.sol.org.tr/devlet-ve-siyaset/telefo
nlar-mit-kriterlerine-gore-dinleniyorsa-ulke-ihanetten-gecilmiyor-haberi, (Erişim tarihi: 1 Şubat 2012).

The Guardian (2010). "CCTV aimed at Muslim areas in Birmingham to be dismantled", 25 Ekim 2010, http://www.guardian.co.uk/uk/2010/oct/25/

birmingham-cctv-muslim-areas-surveillance, (Erişim tarihi: 15 Temmuz 2011).

The Guardian (2010)"China demands ID from all buyers of mobile phone numbers", Pekin, 1 Eylül 2010, http://www.guardian.co.uk/world/2010/sep/01/china-mobile-phone-number-identity, (Erişim tarihi: 15 Temmuz 2011).

The Guardian (2010). "Unmanned drones may be used in police surveillance", 24 Eylül 2010, http://www.guardian.co.uk/uk/2010/sep/24/police-unmanned-surveillance-drones, (Erişim tarihi: 15 Temmuz 2011)

Türkiye Büyük Millet Meclisi, "Yazılı Soru Önergesi Bilgileri", http://www.tbmm.gov.tr/develop/owa/yazili_sozlu_soru_sd.onerge_bilgileri?kanunlar_sira_no=94764, (Erişim tarihi: 31 Ocak 2012).

Waugh, R. (2012). "EU says Google should 'halt' its upcoming privacy changes that share user details across search, Gmail and YouTube", *Daily Mail*, (3 Şubat), http://www.dailymail.co.uk/sciencetech/article-2095962/EU-says-Google-halt-upcoming-privacy-changes.html, (Erişim tarihi: 26 Şubat 2012).

Wong, P. (2010). "Conversations About the Internet #5: Anonymous Facebook Employee", *The Rumpus*, 11 Ocak 2010, http://therumpus.net/2010/01/conversations-about-the-internet-5-anonymous-facebook-employee/?full=yes, (Erişim tarihi: 27 Şubat 2012).

Zeyrek, D., Milletvekilini dinleme yasadışı, *Radikal Gazetesi*, 19 Nisan 2012, http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetayV3&ArticleID=1085386&CategoryID=78, (Erişim tarihi: 20 Nisan 2012)

Zetter, K. (2010). "Google Hack Attack Was Ultra Sophisticated, New Details Show", *Wired Magazine*, 14 Ocak 2010, http://www.wired.com/threatlevel/2010/01/operation-aurora/, (Erişim tarihi: 27 Şubat 2012).

Zetter, K., (2010). "Google Hackers Targeted Source Code of More Than 30 Companies", 13 Ocak 2010, http://www.wired.com/threatlevel/2010/01/google-hack-attack/, (Erişim tarihi: 27 Şubat 2012).

İnternet Adresleri

AKP, Adalet ve Kalkınma Partisi (2012), http://www.akparti.org.tr/site/haberler/basbakanerdoganin-hukumet-programini-sunus-konusmasinin-tam-metni/10899, (Erişim tarihi: 2 Mart 2012)

BTK, Bilgi Teknolojileri ve İletişim Kurumu, (2012). *Elektronik imza*, http://www.btk.gov.tr, (Erişim tarihi: 04.03.2012).

CNIL, Commission Nationale Informatique et Libertés, (2012). *La CNIL*, http://www.cnil.fr, (Erişim tarihi:04:03:2012).

Edevlet kapısı, (2012). *Türkiye Cumhuriyeti Vatandaş Kimlik Doğrulama Sistemi*, http://www.turkiye.gov.tr, (Erişim tarihi 04.03.2012).

Elektronik kimlik doğrulama sitemi, http://www.ekds.gov.tr, (Erişim tarihi: 8 Temmuz 2011).

Electronic Privacy Information Center, http://epic.org/privacy/airtravel/profiling.html, (Erişim tarihi: 10 Temmuz 2011).

Google tracks you. We don't. An illustrated guide, http://donttrack.us/, (Erişim tarihi: 10 Nisan 2012)

Nüfus ve vatandaşlık işleri genel müdürlüğü, http://www.nvi.gov.tr, (Erişim tarihi: 8 Temmuz 2011 ve 28 Şubat 2012).

Office of the Privacy Commisioner of Canada, http://www.priv.gc.ca, (Erişim tarihi: 8 Temmuz 2011).

Tor Project, https://www.torproject.org/about/overview.html.en, (Erişim tarihi: 10 Nisan 2012)

Turkcell İletişim Hizmetleri A.Ş., http://www.turkcell.com.tr, (Erişim tarihi: 8 Temmuz 2011).

Türkiye Cumhuriyeti Resmi Gazete, 5070 sayılı elektronik imza kanununu, 23/01/2004, s. 25355.

Ulusal Bilgi Güvenliği kapısı, http://www.bilgiguvenligi.gov.tr, (Erişim tarihi: 8 Temmuz 2011).

Özet

Bu kitabın amacı modern devletin yeni iletişim teknolojileri yoluyla toplumsal yaşamı ve yurttaşları artan oranda nasıl denetlediğini ve kontrol ettiğini ortaya koymaktır. Çalışma, dijital gözetim olgusunu ve yurttaşın sayısal bedenlenişin nasıl gerçekleştiğini göstermek için, Türkiye'deki T.C. kimlik numarasının sanal uzamda kullanımının topografyasını çıkarmıştır. Bu çerçevede, E-devlet kapısı uygulaması ve T. C. Kimlik numarası üzerinden işlem yapan diğer potansiyel kayıtlayıcılar (İnternet siteleri, siyasi partiler, vb.) incelenmiştir. Böylelikle, T.C. kimlik numarasının sanal uzamdaki kullanım alanları, potansiyel kayıtlayıcıları, kurum ve kuruluşlar arasındaki paylaşımı gösterilmiştir. Aynı zamanda, Türkiye'de yurttaşın sayısal bedenlenişinin sanal topografyası ortaya konulmuştur.

Neoliberalizmin yönetim anlayışı olan yönetişim uzantısı olan e-devlet modeli bilgi toplanması ve işlenmesi üzerine kuruludur. Bu nedenle devlet sürekli olarak, bilgiye ulaşmak amacıyla gözetim yapmaktadır. Modern devlet, e-devlet sistemi gibi yeni uygulamalarla yurttaşları artan oranda gözetler ve denetlerken, yurttaşlar da yeni iletişim teknolojilerini yoluyla iktidar talep etmeden birbirilerini gözetlemeye başlamıştır. Böylece gözetim tüm topluma yayılmıştır. Artık yurttaşlar kişisel bilgilerini (kimlik bilgileri, ekonomik bilgileri, sağlık ve sigorta bilgileri, tüketim alışkanlıkları bilgileri, istihdam bilgileri, vb.) farklı işlemler için verip gönüllü olarak kayıtlanmaya katkıda bulunmaktadırlar. Bu bilgiler doğrultusunda yurttaşlar hem ticari hem de kamuya ait veri tabanlarında numaralar ya da kodlar olarak saklanıp işlenmekte; böylece sayısal bedenlere dönüşmektedirler. Dijital gözetim teknolojilerinin ön plana çıktığı alanlar, askeri istihbarat alanları, devlet yönetimi, nufüs sayımı ve suç kontrolü, iş gözetimi ve denetimi alanları ve tüketim ve tüketici yapılandırılması alanlarıdır. E- devlet uygulamasına geçen toplumlarda belirtilen alanlardan elde edilen kişilere ait verilerin eşleştirildiği ve artan oranda kurumlar arasında paylaşıldığı gözlemlenmektedir. 1980lerde neoliberal politikalarla birlikte ortaya çıkan ve niceliksel olarak giderek artan ticari kayıtlayıcılar ve veri tabanları da bu paylaşım ağına dahildir. Farklı alandaki bilgiler, tek bir çatı altında toplanmasa da, devlet veri eşleştirmesi yoluyla gerektiğinde bu bilgileri topluca değerlendirecek teknik imkanlara sahiptir. Türkiye Cumhuriyetinde yurttaşlarının kayıtlanması için en kapsamlı çalışma, MERNİS projesi fikri ile 1972'de başlamış ve 2002 yılında uygulamaya geçmiştir. Bu

kapsamda, 2000 yılına gelindiğinde 120 milyonun üstünde kişiye T. C. Kimlik numarası verilmiştir ve bu bilgi nüfus cüzdanlarında yer almaya başlamıştır. Bu aşamadan sonra, Nüfus ve Vatandaşlık İşleri (NVİ) tarafından, kamu kurum ve kuruluşlarının ve diğer tüzel kişilerin gereksinim duyduğu kişi bilgilerine elektronik ortamda hızlı bir biçimde erişim sağlanması amacıyla Kimlik Paylaşım Sistemi (KPS) projesi yaşama geçirilmiştir. MERNİS dolayımı ile KPS de toplanan veriler, e-devlet kapısı ile e-kimlik kartı uygulamaları, Türkiye'de yurttaşın doğumdan ölüme, gündelik yaşamın her alanında dijital olarak kayıtlandığı, sınıflandırılabileceğini ortaya koymaktadır. Bu kayıtlamaların yarattığı en büyük sorun, T.C. kimlik numarası merkezi bir anahtar haline gelirken ve pek çok işlem bu numara üzerinden entegre halde yapılırken, bu numaranın kişisel veri olarak korunmamasıdır. Kişilerin çeşitli işlemler yaparken T.C. Kimlik numaralarını kullanması, onların kimliklerini doğrudan belirlenebilir hale getirmektedir. Bu nedenle, kimlik numarasıyla yapılan tüm işlemlerde "kişisel veri" oluşmaktadır. Kişisel verilerin korunmasına yönelik hem ulusal hem de uluslar arası belirli standartlar vardır. Ancak, her ne kadar bu konudaki çalışmalar devam etse de, Türkiye'de bu standartlara uygun bir yasal çerçevenin bulunmadığı gözlemlenmektedir. Yasal çerçevenin olmaması, Türkiye Cumhuriyeti yurttaşlarının kamusal otoriteler karşısında, yalnızca sayılarla belirlenmiş nesnelere dönüşmelerine yol açmaktadır. Bu kişilerin insanlık onurlarını zedelemektedir. Aynı zamanda, sürekli gözetlendiğini ve kontrol edildiğini düşünen yurttaşların kamusal yaşama özgür şekilde katılması ve kamusal haklarını kullanmasını kısıtlayabilmektedir.

Sonuç olarak, E-devlet uygulamaları, güvenlik, verimlilik, hızlılık, şeffaflık gibi söylemlere dayanan neoliberal politikalardan beslenmektedir. Yönetişim olgusu üzerinden meşruiyeti sağlanmaya çalışılan bu uygulamalarla, yurttaşlar artan oranda kayıt altına alınmaktadır. Türkiye'de yurttaşlar gerek MERNİS projesi sonucunda gerekse e-devlet kapısı uygulamasıyla artık sayısal olarak bedenleşmiştir. KPS ve e-devlet kapısı ile merkezsizleşmiş, ancak sürekli işleyen veri gözetimi ve denetimi söz konusudur. Böylece, yurttaş görünmez bir gözün her yerdeki iktidarını meşru ve doğal görmeye başmaktadır. Bu veri gözetiminin de kanıksanması ve içselleştirmesine neden olmaktadır. Bunlardan yola çıkarak bu çalışmanın temel önerileri şunlardır: Türkiye'de kişisel verilerin korunmasını sağlayacak insan haklarına dayalı bir politikanın ve yasal çerçevenin oluşturulması; kişisel verilerin gözetimi ve kullanımının farklı boyutlarını ele alan akademik çalışmaların yapılması ve sivil toplumun konuyla ilgili farkında lığı arttırması. Çalışmanın, en temel önerisi de Türkiye'de e-devlet kapısı ve e-kimlik kartı uygulamasının yurttaş odaklı olarak karşılılık ilkesi esasına dayalı olarak yürütülmesidir.

Abstract

Digital Surveillance in Turkey: Digital Personification of Citizens in Turkey from ID Numbers to E- IDs

The aim of this book is to demonstrate how modern state increasingly monitor and control citizens by means of new information and communication technologies (ICTs). This work infers topography of uses of Turkish ID Number in virtual environment in order to show how digital surveillance and digital personification of citizens are carried out. In this context, e-Government Gateway application and the other potential registering bodies (i.e. websites and political parties) were examined. In doing so, area of uses of Turkish ID Number in virtual environment, potential registering bodies and its sharing between different institutions and/or organisations are displayed. At the same time, they virtual topography of digital personification of citizens in Turkey is illustrated.

E government- the extension of governance which is the administrative mentality of neoliberalism- depends on gathering, storing and processing information. State, therefore, continuously monitors in order to obtain information. While modern state is increasingly monitoring and controlling citizens, citizens have started to watch each other by using ICTs without any demand by political power. In this way, surveillance permeates the society as a whole. Nowadays, citizens voluntarily contribute to the registering of information through submitting their personal information (identity information, financial information, health and insurance information, consumer behaviour, employment information) for different transactions. Based on this sort of information, citizens are stored in the form of codes and processed in both public and commercial databases. Thus, citizens are transformed to digital persons. The areas where digital surveillance technologies come to the fore are (1) military and intelligence; (2) state administration, census and crime control; (3) workplace; and (4) consumption and structuring of consumers. In societies where e-government applications are implemented, it is observed the personal information obtained from these four areas is linked with each other and increasingly shared between institutions. Commercial registering bodies and databases, which has been founded following the neoliberal polices in 1980s and increased in number, also take part in this

network to share information. Although information stored in different fields has not been brought under a single framework, the state has technical capacity to link all the information in all these fields through matching data (assemblage). The most exclusive effort for the registration of citizens in Turkey has started with the MERNİS (Central Civil Registration System) project in 1972. MERNİS was brought into service in 2000. In this framework, over 120 million citizens were given Turkish ID numbers and the inclusion of these ID numbers in the ID Cards has become obligatory. After the introduction of MERNİS, the project for the Identity Information System (KPS) was initiated. This aimed at enabling both public and private institutions and organisations to access the information they needed swiftly in the electronic environment. The data gathered in KPS through MERNİS and the e-government gateway and e-identity applications indicate that citizens in Turkey are digitally registered from birth till death, including many aspects of their daily lives. These also reveal the fact that they could be easily categorised. While Turkish ID number is becoming the central key that enables many transactions in an integrated way, it raises an important issue: this number is not protected as a "personal data". When individuals use of Turkish ID numbers in transactions, their identity can be straightforwardly determined. Therefore, in all transactions where Turkish ID Number is employed, personal data is created. There some national and international standards for the protection of personal data. Although some work has been undertaken in this field in Turkey, there is a lack of legal framework which complies with international standards. As a result of the absence of legal framework, citizens are being transformed into objects, labelled by numbers, before public authorities. The objectification impairs the dignity of citizens. Furthermore, this could create an impediment to citizens' free participation in public life and their enjoyment of civil and political rights since they would think that they are continuously watched and controlled. In conclusion, e-government applications are nourished by the main elements of neoliberal discourse such as "security, efficiency, rapidity and transparency". These applications, which try to provide their legitimacy through "governance", are increasingly registering citizens. Citizens in Turkey have been digitally personified by both MERNİS and e-Government gateway applications. KPS and e-government gateway provides a decentred but continuously operating data surveillance and control. In this way, citizens have started to naturalise and legitimise the omnipotent power of an invisible eye. Citizens, thus, take data surveillance as granted and internalize it. In the light of these, main recommendations of this work are as follows: (1) A legal framework and policies for Protection of Personal Data should be developed and implemented immediately. (2) Academic works should be conducted on different dimensions on data surveillance and use of personal data. (3) Non-governmental organisations should raise awareness of data surveillance and its consequences. One of the most important suggestions of this work is the implementation of e-government and e-identity applications in a citizen oriented way, based on the principle of reciprocity.

Özgeçmişler

Selma Arslantaş-Toktaş

2005 yılında Ankara Üniversitesi İletişim Fakültesi Gazetecilik Bölümü'nden mezun oldu. Lisansüstü derecesini, 2009 yılında Orta Doğu Teknik Üniversitesi Medya ve Kültürel Çalışmalar Yüksek Lisans Programı'nda yazmış olduğu "The Unionization (Problems) Concieved By Journalists in The Post-1980 Mediascape in Turkey" (1980 Sonrası Türkiye Medya Ortamında Gazetecilerin Sendika Algısı) başlıklı tez çalışması ile aldı. Aynı yıl Ankara Üniversitesi İletişim Fakültesi'nde Radyo Televizyon Sinema Ana Bilim Dalı'nda doktora programına başladı. "Türkiye'de Bilim Haberlerinin Görünürlüğü ve Temsili (1993-2007)" başlıklı TÜBİTAK projesinde bursiyer olarak çalıştı. İletişim eğitimi ve gazetecilik mesleğinin değişimine ilişkin makalelerinin yanı sıra ulusal ve uluslararası konferanslarda birçok bildirisi bulunmaktadır. Medyanın ekonomi politiği, medya politikaları, yeni medya, medya endüstrisinde emek süreçleri, ve sosyal politika temel ilgi alanları arasında yer almaktadır. Lisans mezuniyetinin ardından televizyon programı, belgesel ve kitap çalışmalarında üstlenmiş olduğu çeşitli görevlerin yanı sıra halen Ankara Üniversitesi İletişim Fakültesi Radyo Televizyon Sinema Bölümü'nde araştırma görevlisi olarak çalışmaktadır.

Mutlu Binark

1989 yılında Ankara Üniversitesi B.Y.Y.O. RTS. Bölümünden mezun oldu. Lisansüstü çalışmalarını Ankara Üniversitesi S.B.E'de gerçekleştirdi. 1999 yılında "İletişim Bilimleri" alanında doktora derecesi, 2003 yılında "İletişim Bilimleri" doçenti ünvanını aldı. Tokyo Üniversitesi'nde doktora, Aarhus Üniversitesi ve Syd-dansk Üniversitesinde doktora sonrası çalışmalarını sürdürmek için burslu konuk araştırmacı olarak bulundu. Halen Başkent Üniversitesi İletişim Fakültesinde öğretim üyesi olarak çalışmalarına devam etmektedir. Çalışma alanlarını iletişim sosyolojisi, kültürlerarası iletişim, eleştirel medya okuryazarlığı, toplumsal cinsiyet ve popüler kültür metinleri, ile yeni iletişim teknolojileri oluşturmaktadır. Yayınlanmış bazı çalışmaları arasında Kadın ve Popüler Kültür (S.İrvan ile der. ve çev.) (1995); Tüketim Toplumu Bağlamında Örtünme Pratiği ve Moda (B.Kılıçbay ile) (2000); "Consumer Culture, Islam and the Politics of Lifestyle: Fashion for Veiling in Contemporary Turkey" European Journal of Communication (2002); "Media Monkeys: Intertextuality, Fandom and Big Brot-

her in Turkey" Big Brother International: Formats, Critics and Publics içinde (B. Kılıçbay ile) (2004); İnternet, Toplum, Kültür (B.Kılıçbay ile birlikte der.) (2005); "Kültürlerarası İletişim Çalışmalarının Türkiye Haritası" Kültür ve İletişim (2006); Zaman ve Uzam İçinde Haydarpaşa Garı: Görsel ve Sözlü Tanıklık (2007) (İ.Kocabıyık ve G.Çulha ile birlikte); Yeni Medya Çalışmaları (der.) (2007); Eleştirel Medya Okuryazarlığı (Mine Gencel-Bek ile birlikte) (2007); Kültür Endüstrisi Olarak Dijital Oyun (Günseli Bayraktutan-Sütcü ile birlikte) (2008); Dijital Oyun Rehberi:Oyun Tasarımı, Oyuncu ve Türler (Günseli Bayraktutan-Sütcü ve Işık Barış Fidaner ile birlikte derleme) (2009); Toplumsal Paylaşım Ağı Facebook: Görülüyorum Öyleyse Varım! (2009, A.Toprak, A.Yıldırım, E.Aygül, S.Börekçi ve T.Çomu ile birlikte) Yeni Medyada Nefret Söylemi (2010), STÖ'ler için Bilişim Rehberi (K.Löker ile) (2011) sayılabilir. Kültür ve İletişim dergisinin Yayın Kurulu üyesidir. TÜBİTAK-SOBAG adına Haziran 2007-Aralık 2008 tarihleri arasında "Türkiye'de Dijital Oyun Kültürü" adlı projeyi yürüttü. Bu proje TÜBİTAK tarafından Nisan 2011 de sosyal bilimler alanında başarı öyküsü olarak seçilen projeler arasında yer aldı. Halen yeni medyada nefret söylemi ve yeni medya okuryazarlığı ile yeni medya etik ilkeler üzerine çalışmalarına devam etmektedir. Alternatif Bilişim Derneği kurucu üyesidir. www.yenimedya.wordpress.com ve www.dijitaloyunkulturu.wordpress.com bloglarının yazarıdır.

Ergin Şafak Dikmen

Bilkent Üniversitesi Güzel Sanatlar Tasarım ve Mimarlık Fakültesi İletişim ve Tasarım Bölümü'nden 2006 yılında mezun oldu. Lisansüstü derecesini, Anhalt Üniversitesi (Almanya) Tasarım Bölümü, Bütünleşik Tasarım Yüksek Lisans Programında Görsel Yanılgı ve Tasarım Alanında Kullanımı başlıklı tez çalışmasıyla 2008 yılında aldı. Aynı yıl Anhalt Üniversitesi yerleştirme sergisinde, Double Layer Video Project canlandırma filmi; 3. Uluslararası Cinema & Design (İstanbul) sergisinde Görmek İçin Yaklaş canlandırma filmi sergilendi. 2008 yılında Bilkent Üniversitesi Elektromanyetik Araştırma Merkezinde grafik tasarım ve animasyon uzmanı olarak çalıştı. 2009 yılında Ankara Üniversitesi, Sosyal Bilimler Enstitüsünde doktora programına başladı. Halen Ankara Üniversitesi, İletişim Fakültesinde uzman olarak çalışıyor. İlgi alanları; yeni medya, medya estetiği, canlandırma, dijital oyunlar.

Işık Barış Fidaner

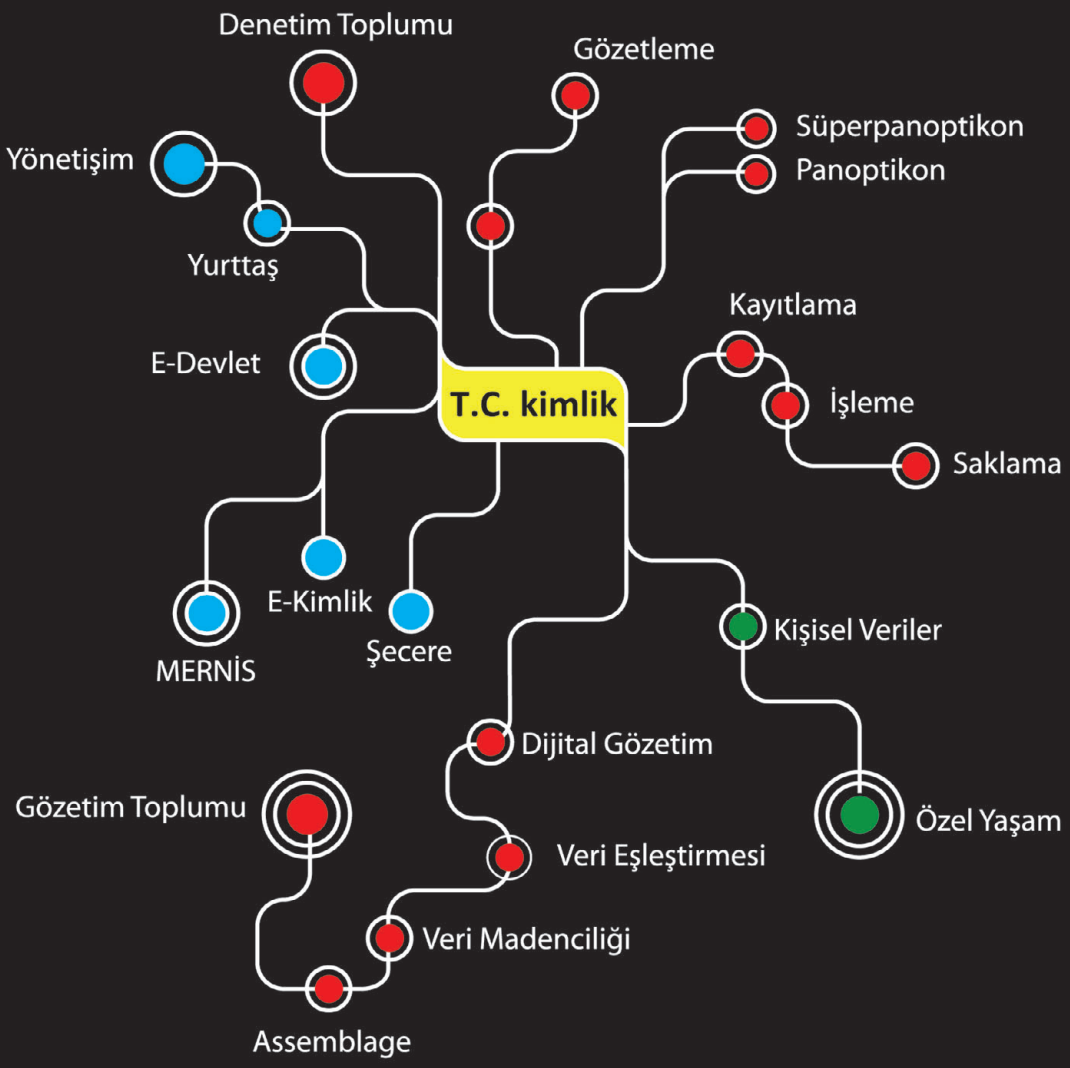
1983'te Ankara'da doğdu. Amiga ile başlayan oyun geliştirme isteği onu bilgisayar programcılığına yöneltti. Lisans ve yüksek lisans eğitimini, "Yüz modelleme, canlandırma" ve "Hareketli görüntüde nesne izleme" konulu tez çalışmaları ile Boğaziçi Üniversitesi Bilgisayar Mühendisliği bölümünde tamamladı. Halen aynı bölümde Bayesci istatistiksel yöntemler ve biyoinformatik uygulamaları konusundaki doktora tezi üzerine çalışmaktadır. Alternatif Bilişim Derneği üyesidir. Dijital Oyun Rehberi derlemesi (Mutlu Binark ve Günseli-Bayraktutan Sütcü ile) 2009'da, Cesur Yeni Medya özgür e-derlemesi (Alternatif Bilişim ile) 2011'de yayınlanmıştır.

Elif Küzeci

2001 yılında Başkent Üniversitesi Hukuk Fakültesi'nden mezun oldu. Lisansüstü derecesini 2004 yılında "İnternet'te Basın Özgürlüğü" başlıklı tezi ile Ankara Üniversitesi Sosyal Bilimler Enstitüsünden aldı. Aynı üniversitede gerçekleştirdiği doktora çalışmaları 2010 yılında neticelendi ve "Kişisel Verilerin Korunması" başlıklı tezi ile doktor ünvanını aldı. 2011 yılında Bahçeşehir Üniversitesi Hukuk Fakültesi'nde yardımcı doçent doktor olarak atandı. Halen aynı fakültede çalışmalarını sürdürmektedir. Başlıca ilgi alanlarını; devlet kuramı, insan hakları ve bilişim hukuku oluşturmaktadır. "İnsan Hakları ve Kamu Özgürlükleri" (Turhan Yayınları, 4.Baskı Ankara 2001; Ahmet Mumcu ile birlikte) ve "Kişisel Verilerin Korunması" (Turhan Yayınları, Ankara 2010) başlıklı yayınlanmış iki kitabı bulunmaktadır. "Devlet Gözetimine Karşı Avrupa İnsan Hakları Mahkemesi Kalkanı", (Bahçeşehir Üniversitesi Hukuk Fakültesi-Kazancı Hakemli Hukuk Dergisi, Y.2011, C.7, S.81-82; s. 7-61); "Anayasal Bir Hak: Kişisel Verilerin Korunması" (Bilişim, 2011 Şubat ayı, Y. 38, S. 128, s. 142-149); "Beyaz Perdede Kara Bir Dönemin Gölgesi: Modernite ve Holokostu Sinema Aracılığıyla Anlamak" (Türkiye Barolar Birliği Dergisi, 2010 yılı Temmuz-Ağustos Sayısı); "Gender Equality in the Constitution of the Republic of Turkey", (Ankara Bar Review, V. 1, I. 2 June 2008, s. 18-27); "AİHS'nin 10. Maddesi Işığında Nefret İçerikli ve Irkçı Nitelikli Düşünce Açıklamaları", (Türkiye Barolar Birliği Dergisi, Y. 20, S. 71, s. 174-200) başlıklı yayınlanmış makaleleri ve çeşitli ulusal ve uluslararası sempozyumlarda sunulmuş bildirileri bulunmaktadır. "AİHS'nin 10. maddesi Işığında Nefret İçerikli ve Irkçı Nitelikli Düşünce Açıklamaları" başlıklı makalesi ile Aybay Hukuk Araştırmaları Vakfı'nın düzenlediği KAPANİ-SAVCI İnsan Hakları İnceleme Yarışması'nda 2005 yılında birincilik ödülü kazanmıştır. Bahçeşehir Üniversitesi Hukuk Fakültesi-Kazancı Hakemli Hukuk Dergisi yayın kurulu üyesidir.

Alkım Özaygen

Orta Doğu Teknik Üniversitesi Fizik Bölümü'nden 2001 yılında mezun oldu. Lisansüstü derecesini, 2006 yılında Çankaya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği bölümünde "Phylogenetic Supertree Construction Using Constraint Programming" (Kısıt Programlama Kullanarak Süperağaç Oluşturulması) başlıklı tez çalışmasıyla aldı. 1997-2000 yılları arasında TÜBİTAK Bilim ve Teknik Dergisi'nde araştırmacı-gazeteci ve sistem yöneticisi olarak çalıştı. Daha sonra Bilimsel ve Teknik Araştırma Vakfı (BİTAV) ve TRT'nin ortaklaşa hazırladığı 124 bölümlük 'Bilim ve Yaşam' programı ve 13 bölümlük Türk bilim adamlarının hayatını anlatan 'Işıkla Yazılmış Öyküler' programında araştırmacı ve yazar olarak çalıştı. 2009 yılında bir yıllığına Singapur'da bir yazılım firmasında mühendis olarak çalıştı. Halen Ankara Üniversitesi Siyasal Bilgiler Fakültesi İşletme Bölümü Sayısal Yöntemler Anabilim dalında öğretim görevlisi ve Ankara Üniversitesi Uzaktan Eğitim Merkezi'nde sistem yöneticisi olarak çalışmakta ve Ankara Üniversitesi İletişim Fakültesinde doktora çalışmalarına devam etmektedir.



alternatif bilişim

www.alternatifbilisim.org

FRIEDRICH EBERT STIFTUN

ISBN 978-605-62169-2-3