

## KAMU HİZMETLERİNDE BİLGİ TEKNOLOJİLERİ UYGULAMALARI: FIRSAT VE TEHDİTLER\*

Mehmet Devrim AYDIN\*\*

### Öz

20. yüzyılın son çeyreğinde yaşanan bilimsel gelişmeler, iş dünyasında ve devlet yönetiminde mevcut yapı ve sistemleri önemli ölçüde etkileyerek “yeni ve farklı bir dünyanın” habercisi olmuştur. Bu değişim çerçevesinde devletler tarafından kullanılan Bilgi Teknolojileri (BT) uygulamalarının kamu hizmetlerine pek çok açıdan önemli katkılarda bulunduğu gözlenmektedir. Ancak son yıllarda devlet birimlerinin yararlandığı BT uygulamaları arasında yer alan “Kitle İzleme Teknolojilerinin”, bireysel hak ve özgürlükler üzerinde önemli bir tehdit oluşturduğu gözlenmektedir. İzleme teknolojilerinin kötüye kullanımına ait çok sayıdaki olumsuz örnek, çağdaş dünyada gelişip yaygınlaşan BT uygulamalarının bir “Gözetim Toplumu” yaratılmasına neden olabileceği yönündeki kaygıları güçlendirmektedir. Bu çalışmada, söz konusu kaygılardan yola çıkılarak, BT uygulamalarının bireysel özgürlüklere ve toplumsal hayata olumlu ve olumsuz yansımalarının, kapsamlı bir muhasebesi yapılmıştır. Çalışma bulguları, 21. yüzyılda “bireyin mahremiyetinin korunmasının” ve BT uygulamaları yoluyla “bireysel özgürlüklerin geliştirilmesinin” mümkün olduğunu, ancak bu idealin gerçekleştirilebilmesinin üç temel koşula bağlanabileceğini göstermiştir; değişen şartlara göre sürekli olarak güncellenen ve güçlü yaptırımları olan bir hukuksal çerçeve; demokratik, açık ve çoğulcu bir toplum yapısı ve bu ideale adanmış bir kamu yönetimi.

**Anahtar Sözcükler:** Bilgi teknolojileri, kamu hizmetleri, kitle izleme teknolojileri, mahremiyet, gözetim toplumu.

### Abstract

#### Information Technology in Public Services: Opportunities and Threats

Scientific advancements at the last quarter of 20th century brought “a new and different world” by affecting the existing structures and systems in both business and government. In this framework, Information Technologies (IT) used by states have contributed a lot to public services in many respects. While

\* Bu çalışma TÜBİTAK desteği ile gerçekleştirilmiştir.

\*\*Doç. Dr., Hacettepe Üniversitesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, Beytepe/Ankara, mdaydin@hacettepe.edu.tr

this encouraging IT transformation is gaining an impetus, “Mass Surveillance Technologies” (MST) used by state agencies pose an important threat on civil rights and liberties. Some examples of corruption in MST usage are strengthening the suspects and worries about the emergence of a Surveillance Society. This study tries to make a comprehensive analysis of pros and cons of IT usage in public services with regard to civil liberties and social structure. In conclusion, the study shows that “protection of privacy” and “advancement of civil liberties” in the 21<sup>st</sup> century are possible, but the realization of this ideal rests on three conditions; a continuously updated legal structure with strong sanctions; a democratic, open and pluralistic society and a public administration highly committed to this ideal.

**Keywords:** Information technology, public services, mass surveillance technologies, privacy, surveillance society.

## GİRİŞ

21. yüzyılda, dünya çapında rekabet üstünlüğünün en önemli anahtarlarından biri, bilgi teknolojilerine (BT) hâkimiyet, teknolojiyi üretebilme ve kullanabilme gücüdür. BT, en değerli kaynaklar olarak nitelenen petrol ve altının yerini almaya başlamakta, pek çok ülkenin kalkınma stratejilerini büyük ölçüde BT platformu üzerinde inşa etmeye başladığı görülmektedir. BT kullanımının yaygınlaşması, iş dünyasının yanı sıra devlet vatandaş ilişkilerine de yansımakta, kamu hizmetlerinde BT kullanımı giderek yaygınlaşmakta ve bu yeni hizmet anlayışında, “kağıt dolaştırılması” esasına dayalı geleneksel bürokrasi, yerini elektronik ortamda web siteleri üzerinden sunulan ve bilgisayar ve cep telefonları vasıtasıyla ulaşılabilen e-Devlet uygulamaları ile farklı bir hizmet biçimine ve modern bir bürokrasi anlayışına terk etmektedir (Leblebici vd., 2003a). BT uygulamaları ile dünyada ve Türkiye’de, bir yandan örgüt yapıları değişip kaynak kullanımında kalite, hız ve verimlilik sıçraması yaşanırken, diğer yandan da bütünüyle farklı, yeni bir toplumsal düzenin oluşumuna tanıklık edilmektedir (Bensghir, 1996; Öktem, 2004; Aydın, 2005; Öktem ve Aydın, 2005).

Bununla birlikte, yukarıda sıralanan olumlu gelişmelere karşın teknolojinin zihinlerde soru işaretleri yaratan boyutları da bulunmaktadır. Son yıllarda insan hakları savunucuları, bazı teknolojik uygulamaların hem insan hakları hem de bireyin mahremiyeti<sup>1</sup> açısından büyük bir tehdit oluşturduğunu iddia etmekte (Steinhardt, 2003); Orwell’in (1984) “Büyük Birader” veya Foucault’nun (1979) “Panoptikon Toplum” tanımlamalarına atıfta bulunarak günümüz toplumunun tehlikeli bir şekilde, insanların her anının izlendiği bir “Gözetim Toplumuna” (surveillance society) dönüşmekte olduğunu

belirtmektedirler (ACLU, 2006a; Blanchette ve Johnson 1998: 1; Whitaker 2000: 139). Örneğin emniyet ve istihbarat birimlerinin suçlularla, ulusal ve uluslararası terörizmle etkili bir mücadele yürütebilmesi amacıyla geliştirilen teknolojik sistemler bu açıdan önemli tartışmalar yaratmaktadır (tartışmaların Türkiye boyutunda polis bilgi sistemleri açısından bir değerlendirme için bkz. Leblebici vd., 2003b). Çalışmanın ikinci bölümünde, “BT ve Yeni Tehditler” başlığı altında ayrıntılarıyla incelenecek olan söz konusu sistemler aşağıda maddeler halinde sıralanmıştır:

1. Sabit Hatlı Telefonların, Cep Telefonlarının Dinlenmesi ve İnternet Trafiğinin İzlenmesi,
2. Güvenlik Kameralarıyla İzleme,
3. Parmak İzi ve DNA Veri Tabanları,
4. İnternet Üzerinde Sansür,
5. Devlet Birimlerinin, Arama Motorları, Sohbet Siteleri ve e-posta Servis Sağlayıcılarından Bireylere Ait Özel Bilgileri Talep Hakkı,
6. Terör Şüphelileri ve Yardımcılarını İçeren Elektronik Veri Tabanları.

Bu ve benzeri uygulamaların, amaç dışı kullanım halinde oluşturabilecekleri risklerin büyüklüğü göz önüne alındığında, bireysel özgürlüklerin ve özel yaşamın dokunulmazlığının zarar görebileceği yeni ve baskıcı bir dünya sistemi ile karşı karşıya olunduğunu savunan çevrelerin kaygılarının nedenlerini anlamak hiç de güç olmayacaktır. DNA veri tabanlarının oluşturduğu etik sorunlar üzerinde araştırmalar yapan Harvard Üniversitesi profesörlerinden David Lazer’in bir sorusu bu anlamda oldukça etkileyicidir (New Scientist, 2005): “Başkan Edgar Hoover’ın ellerinin herkesin DNA bilgilerinin üzerinde olmasını kim isterdi?” Lazer’in ortaya koyduğu bu soru, demokratik ülkelerde dahi devletlerin elindeki bu güçlü silahların, hırslı ve kanunlar konusunda pek de hassas olmayan politikacılar tarafından kötüye kullanılma riskinin mevcudiyeti konusunda bir uyarı olarak da görülebilir.

İnsan hakları savunucuları, 11 Eylül 2001’de gerçekleşen terör eylemi sonrasında güvenlik güçlerinin izleme teknolojileri konusundaki gücünü oldukça artıran Amerika Birleşik Devletleri’nde (ABD), politikacıların terörle mücadele ederken farkında olmadan bir “gözetim toplumu” (surveillance society) yaratma riskinin yüksekliği üzerine uyarıda bulunmaktadırlar. Örneğin, New York Sivil Özgürlükler Derneği Başkanı (New York Civil Liberties Union) Lieberman, kamuoyuna yaptığı bir açıklamada parmak izi ve DNA veritabanları ile ilgili olarak “yaşamayı istediğimiz özgür toplumun bu olduğunu düşünmüyorum” sözleriyle bu alandaki kaygılarını dile getirmektedir (Kluger, 2006). Yine Amerikan Sivil Özgürlükler Derneği (American Civil

Liberties Union/ACLU) Başkanı Steinhardt (2003) ise, ABD Temsilciler Meclisi'nde Yönetmelik Reform Komitesi karşısında sunduğu konuşmada Amerikan toplumunun bir gözetim toplumu olma yolunda hızla ilerlediğini belirtmektedir. Gerçekten de yaşanan pek çok örnek, Lieberman ve Steinhardt gibi insan hakları savunucularının BT'nin amaç dışı kullanımını konusundaki kaygılarını desteklemektedir. Üstelik ABD'nin yakın geçmişte Watergate gibi büyük bir skandal yaşamış olması da uyarıların ciddiye alınması gerektiğini göstermektedir. ABD'de 1972 yılında, Demokrat parti seçim merkezinin ve telefonlarının Cumhuriyetçiler tarafından yerleştirilen teknolojik araçlarla dinlendiğinin ortaya çıkarılması ile patlayan ve yakın tarihin en çarpıcı siyasi skandalları arasında yerini alan Watergate, BT'nin kötüye kullanımının çarpıcı örneklerinden biri olarak görülebilir (Fox, 2005). Türkiye'de de, izinsiz telefon dinleme olgusunu tanımlamak için kullanılan "Telekulak" kavramı sık sık gündeme gelmekte, hâkim kararı olmadan gerçekleştirilen keyfi uygulamalar, sık sık haber ve eleştiri konusu olmaktadır (Akşam, 2005; Zaman, 2005).

Bugün giderek gelişen "Kitle İzleme Teknolojileri"nin (Mass Surveillance Technology) sunduğu yeni imkânlar da göz önüne alındığında, BT'nin amaç dışı kullanımı konusundaki kaygıların hiç de haksız olmadığı yönündeki kanaatler güçlenmektedir. Buna ek olarak, insan hakları savunucuları, günümüz insanının şiddet ve terör faaliyetlerine karşı can güvenliğinin sağlanabilmesi için özgürlüklerinden vazgeçmek zorunda bırakıldığını savunmaktadırlar. Bir diğer deyişle halk kitleleri ister istemez bir "güvenlik-mahremiyet" paradoksuna sürüklenmektedir (Stanley ve Steinhardt, 2003). Özellikle terör olayları sonrasında ABD'de (11 Eylül 2001 saldırıları) ve İngiltere'de (Londra'daki 7 Temmuz 2005 metro ve otobüs saldırıları ve 9 Ağustos 2006'da uçaklara yönelik saldırı girişimi) alınan önlemlerin aşırılığı, bir tür "terör paranoyası" yaratılarak kişisel özgürlüklerin askıya alınabileceği düşüncelerinin doğmasına yol açmaktadır. Örneğin Knox (2006), Londra'da 9 Ağustos 2006 uçak saldırısının önlenmesinden sonra Bush yönetiminin bu olayı, Irak'taki başarısızlığı gizlemek ve seçimlerde oy kaybını engellemek için halkın dikkatini tekrar terörizmle olan geniş ölçekli global savaşa yönlendirmek amacıyla kullandığı yorumunu yapmaktadır.

Bu çalışma, yukarıda sunulan çarpıcı tartışmaların oluşturduğu oldukça karmaşık bir çerçevede, BT uygulamalarının bireysel özgürlükler ve toplumsal hayata olumlu ve olumsuz yansımalarının kapsamlı bir muhasebesini yapmayı amaçlamaktadır. Çalışmanın birinci bölümü, BT'nin kamu hizmetlerinde yarattığı olumlu dönüşüme ve yeni fırsatlara odaklanmaktadır. İkinci bölümde BT'nin bireysel özgürlükler üzerinde oluşturduğu tehditler incelenmekte, sonuç kısmında ise genel bir değerlendirme yapılmaktadır.

## 1. BT VE YENİ FIRSATLAR

BT alanında yaşanan göz kamaştırıcı teknolojik ve bilimsel ilerleme, değişimin hızının artık kestirilemediği, yeni bir toplumsal yapı ve yeni bir uygarlığın kapılarını açmıştır (Drucker, 1994; Drucker, 2000: 111; Toffler, 1989: 99, 171-172; Toffler ve Toffler, 1996: 14; Toffler ve Toffler, 1997: vi-ix). Yaşanılan değişim ve gelişmeler, kamu yönetimi ve kamu hizmetlerinde de kendini göstermektedir. Özellikle gelişmiş ülkelerde geleneksel devlet modelinden, hizmetlerin büyük ölçüde elektronik ortam üzerinden yürütüldüğü elektronik devlet modeline (e-Government) yönelen bir dönüşümün 1990'lı yıllarda giderek hızlanmaya başladığı görülmektedir. Örneğin ABD'de 1993 yılında başlatılan kamu yönetiminin yeniden yapılandırılması çalışmalarında (National Performance Review) BT, önemli bir araç olarak nitelenmiştir (Brown, 1998: 335). ABD'de ortaya konulan çok sayıda e-Devlet projesi, BT alanında yapılacak bir atılımın geleceğin yüksek rekabete dayanan, dinamik uluslararası ticaret ortamında ABD'nin liderliğini perçinleyeceği düşüncesine dayanmaktadır. Diğer taraftan BT dalgasının önünde yer almayı amaçlayan AB ülkeleri de önemli bir atılım yaparak 23 Mart 2000'de Lizbon'da eAvrupa (eEurope) Projesini başlatmışlardır (eEurope Project, 2000). eAvrupa Projesi, İnternet kullanımının yaygınlaştırılması ve bilgi toplumunun temel yapı taşlarının oluşturulması yoluyla, AB'nin dünyadaki en rekabetçi ve dinamik ekonomi haline getirilmesi gibi iddialı bir vizyona sahiptir (eEurope Project, 2000; eEurope 2002 Project, 2000; eEurope 2005 Project, 2002; Akdeniz, 2003; Aydın, 2005).

Kamu hizmetlerinde BT'nin kullanımıyla, hizmetlerin sunumunda sürat, kalite ve verimlilik alanlarında büyük bir dönüşüm yaşandığı görülmektedir (Lehr, 1998). İnternet teknolojisi, bu dönüşümün temel ateşleyicilerinden biri olarak görülebilir. İnternet, kitlesel yaygınlaşma hızı açısından da daha önceki buluşlardan ayrı bir yere sahiptir. ABD'de yürütülen bir çalışmada (Mann vd., 2000: 13) önemli teknolojik buluşların, 50 milyon kişiden oluşan bir kitleye yayılma hızları kıyaslanmış ve şaşırtıcı bir sonuç elde edilmiştir: Buna göre telefon 74 yıl, radyo 38 yıl, bilgisayar 16 yıl, televizyon 13 yılda bu ölçekte bir kitle içinde kullanıma girmişken, bu sürenin İnternet için 4 yıl olduğu görülmüştür. Bu durum teknolojik gelişmelerin toplumu etkileme hızının son yıllarda tarihin hiçbir döneminde olmadığı kadar süratli olduğunu ve teknolojinin toplumsal dönüşümlere, iş hayatına ve hatta devlet yönetimine etkisinin de bilim çevrelerinin beklediğinden hızlı olabileceğini göstermektedir. Gerçekten de bugün gelişmiş ülkelerde vatandaşlar, İnternet yoluyla kamu hizmetlerinden elektronik ortamda haftada 7 gün ve 24 saat, kesintisiz bir şekilde yararlanabilmektedir. Geleneksel devlet modelindeki, kamu kurumları

önünde bekleme, işlem kuyruklarında zaman yitirme ve bürokratik işlemlerde kırtasiyecilik vb. pek çok sorun, 1990'lı yılların ortalarından itibaren büyük bir hızla azalmakta, kamu kesiminde büro ortamında İnternet ve bilgisayar kullanımı vazgeçilmez hale gelmektedir (UNDPEPA-ASPA, 2001: 1).

Öte yandan İnternet, sağladığı özgürlükler ve bilgiye coğrafi sınırları aşan bir erişim imkânı sunmasıyla, bir “dijital bilgi ve özgürlük çağını” da başlatmış gözükmektedir. BT alanındaki ilerleme o denli hızlı ve o denli kapsamlıdır ki, gelişmeler, devlet yönetimi, eğitim, sağlık, ticaret vb. alanlarda BT'nin sağladığı yeni fırsatların fizikteki adıyla bir “kuantum sıçraması” olarak nitelenebilecek kadar büyük ölçekli olabileceğini göstermektedir (Erkan, 1998: 241). Gerçekten de BT'nin bireye ve topluma sunduğu imkânların büyüklüğü ve bu imkânların demokrasi ve özgürlükleri genişletmek amacıyla kullanıldığında sağlanacak faydanın boyutu düşünüldüğünde heyecanlanmamak mümkün değildir. ABD ve AB ülkelerinde 1990'lı yılların ikinci yarısından itibaren hızla yaygınlaşan BT programlarının toplumsal hayatta pek çok alanda önemli bir dönüşüm yarattığı görülmektedir.

BT'nin sunduğu bu yeni fırsatları değerlendirebilmek için öncelikle hangi alanlarda ne tür katkılar sağladığının görülmesinde yarar vardır. Söz konusu alanlar genel olarak e-Demokrasi, e-Devlet, e-Sağlık, e-İş ve e-Öğrenmeden oluşan beş başlık altında toplanarak incelenebilir.

**Tablo-1: Kamu Hizmetlerinde BT Uygulamalarının Bireysel ve Toplumsal Hayata Sunduğu Yeni Fırsatlar**

<b>e-Demokrasi</b>
- Çevrimiçi (online) oy kullanma
- İnternet üzerinden siyasi kampanyalar düzenleme
- Oy kullanacakların kaydedilmesi
- Kamuoyu yoklamaları
- Siyasiler ile vatandaşlar arasında iletişim
- Yasama sürecinin İnternet üzerinden izlenebilmesi ve yasa tasarıları hakkında bilgi sunulması
<b>e-Devlet</b>
- e-Devlet Kapısı Üzerinden Ödeme Yapılması: Bireylerin devletten almak zorunda olduğu bilgiler ve devletin tuttuğu diğer kayıtlarda (nüfus kağıdı, pasaport, tapu ve kadastro, nüfus, adli kayıt ve sicil, askerlik, ithalat/ihracat vb.) resmi bir ortak web sitesinin kullanılması.
- e-Devlet Kapısı Üzerinden Etkileşimli Kamu Hizmetleri: Kamu kurumları arasında sağlanan ortak standartlarla tüm kamu kurumlarının veri paylaşabilir hale gelmesi ve böylece devlet içi yazışmaların, belge ve veri aktarımlarının, BT altyapısı üzerinden gerçekleştirilmesi.
- Geniş Bant İnternet: Yüksek hızlı İnternet ile zamandan tasarruf.
- Kamu Veri Tabanlarının Karşılıklı İşlerliği ve Veri Paylaşımı
- Kamu Alımlarının İnternet üzerinden düzenlenmesiyle maliyet kazancı
- Video-konferans: Kamu görevlilerinin toplantılarını zaman ve mekandan bağımsız BT altyapısı üzerinden yapabilemesi.
<b>e-Sağlık</b>
- Elektronik Sağlık Kartları: Bireye ilişkin bilgilerin kağıt ortamından kurtarılıp, taşınabilir kartlara yüklenmesi.
- Sağlık Bilgi Ağları: Bireylerin sağlıkları ile ilgili tüm verilerin düzenli bir biçimde veri bankalarında saklanması ve hastane, laboratuvar ve ev arasında bilgi transferi yapılabilmesi.
- Uzaktan Tarama: Röntgen, ultrason, tomografi sonuçlarının İnternet üzerinden uzaktaki bir uzmana gönderilmesi.
- Video-konsültasyon: Herhangi bir yerdeki hastaya, uzmanların, bulunduğu yerden bağımsız olarak BT altyapısı aracılığıyla uzaktan konsültasyon yapması.
- Koruyucu Sağlık Hizmetlerinin Uzaktan Sunulması
<b>e-İş</b>
- Evde Çalışma
- Bilgisayar Destekli Tasarım ve Üretim
- Çevrimiçi Alışveriş ve Banka Hizmetleri
- Elektronik Ticaret
- Satış Sonrası Uzaktan Etkileşimli Eğitim
<b>e-Öğrenme</b>
- Etkileşimli Uzaktan Eğitim ve Sanal Kampüs
- Kütüphanelere İnternet Üzerinden Erişim
<b>Kaynak:</b> TÜBA-TÜBİTAK-TTGV, 1995; eEurope 2005 Project, 2002; Economist, 2000; CDD, 2006; Hacker ve Dijk, 2000; Wilhelm, 2000; Hague ve Loader, 1999.

Görüldüğü gibi kamu hizmetlerindeki dönüşüm neredeyse toplumsal hayatın tüm boyutlarına etkiye bulunacak denli büyük boyutludur. Ancak bu dönüşümün etkilerini somut olarak görmeden, onu bir kuantum sıçraması olarak nitelendirmek sağlıklı bir yaklaşım olmayacaktır. Bu nedenle çalışmanın bu aşamasında, kamu hizmetlerinde BT kullanımında önemli bir yol almış AB ülkelerindeki BT uygulamaları incelenerek bu uygulamalardan sağlanan somut kazançlar ele alınacaktır.

AB ülkelerinde kamu hizmetlerinde BT uygulamaları üzerine gerçekleştirilen en kapsamlı çalışma, 2004 yılı Aralık ayında Avrupa Komisyonu Bilgi Toplumu Genel Müdürlüğü e-Devlet Birimine sunulan ve 253 kurum, 28.332 şirket ve 19.896 vatandaşın katılımıyla gerçekleştirilen “Top of the Web” başlıklı rapordur (eGovernment, 2004). Çalışmada kamu hizmetlerini elektronik ortamda kullanan vatandaşların tatmin düzeyi ve bu hizmetlerin elektronik ortamda sunumunun ekonomilere sağladığı katkı araştırılmıştır. BT kullanımının bireylere ve ekonomiye katkısının açık bir şekilde görülebilmesi açısından 15 Avrupa ülkesinde yürütülen bu çalışmanın bazı önemli bulguları aşağıda sıralanmaktadır (eGovernment, 2004):

- e-işlemlerle kazanılan ortalama zaman: AB ülkelerindeki İnternet kullanıcılarının kamu hizmetini geleneksel yöntemle almak yerine elektronik ortamda çevrimiçi olarak almakla, işlem başına ortalama 1 saat zaman kazandığı saptanmıştır.

- Kişisel gelir vergisi bildirim: Kullanıcılar, elektronik ortamda gerçekleştirilen gelir vergisi bildirim işlemlerinde işlem başına ortalama 71 dakika tasarruf sağlamıştır. Bu da 2003 yılında 15 AB ülkesinde toplam 7,3 milyon saatlik bir tasarruf anlamına gelmektedir. (Çalışma, e-işlemlerin yaygınlaşması ile bu rakamın yıllık “100 milyon saate” çıkacağını belirtmektedir).

- İş dünyasında Katma Değer Vergisi bildirim: İşlem başına ortalama 38 dakika ve 10 Euro tasarruf sağlanmıştır. Böylece 2003 yılında iş dünyası yaklaşık 29,3 milyon Euro elde edilmiştir. (Bu rakamın e-işlemlerin yaygınlaşması ile 230 milyon Euro’ya çıkması beklenmektedir).

- Yeni şirket kaydı: İş dünyasında 2003 yılında 2,2 milyon Euro tasarruf sağlanmıştır.



- Halk kütüphaneleri (katalog tarama): Kullanıcılar ortalama olarak işlem başına 81 dakika tasarruf etmişlerdir ve bu miktar 15 AB ülkesinde toplam olarak 1.021 çalışma yılına denk gelen bir tasarrufu temsil etmektedir.

- Kullanıcı tatmini: Araştırma, kullanıcıların %62'sinin aldıkları e-hizmetten çok memnun olduğunu göstermektedir. Ayrıca kullanıcıların %77'si çevrimiçi hizmetleri diğerlerine tavsiye edeceklerini belirtmektedir ki, bu durum yakın gelecekte e-hizmet kullanımının çok daha yaygınlaşacağını da göstermektedir.

Yukarıdaki bulgulara ek olarak, eGovernment (2004) çalışması, e-işlemlerden sağlanan kazançların sadece zaman ve para ile sınırlı olmadığını göstermiştir. "Esneklik", "daha hızlı hizmet" ve "daha hızlı yanıt" gibi unsurlar, sıralamada zaman ve para kriterlerinin ardından kullanıcı memnuniyetini etkileyen başlıca kriterler olarak ön plana çıkmaktadır. Çevrimdışı (offline) hizmetten çevrimiçi (online) hizmete geçerken, kullanıcıların zaman kazanmanın yanı sıra zamanın kullanımında da büyük bir "esneklik" kazandığı görülmektedir, çünkü geçmişte sadece çalışma saatlerinde ve ilgili kamu kurumuna bizzat gidilerek işlem yapılabilirken, artık haftanın 7 günü ve günün 24 saati evden veya işyerinden çevrimiçi hizmete ulaşılabilmektedir.

Kamu kesiminde BT uygulamalarının AB ülkelerinin ekonomilerine ve AB vatandaşlarına zaman, hız, maliyet, esneklik gibi pek çok boyutta katkıda bulunduğu görülmektedir (eGovernment, 2004). Bu bulgular Türkiye gibi gelişmekte olan ülkeler için BT ve e-Devlet hareketinin ne denli büyük bir önem taşıdığını kanıtlamaktadır. İncelenen e-hizmetler sıradan bir AB vatandaşı için işlem başına ortalama 1 saatlik tasarruf anlamına gelirken, kamu bürokrasinin çarklarının kırtasiyecilik, iş yükü vb. nedenlerle çok daha yavaş çalıştığı Türkiye gibi bir ülkede bu rakamın 1 saatin çok daha üzerinde olacağı düşünülmektedir. Türkiye'de AB tarafından öngörülen diğer temel kamu hizmetlerinde sağlanabilecek gelişmelerle ekonomi için yüzlerce milyon doları bulan bir tasarrufun mümkün kılınması beklenmektedir (Aydın, 2005).

Bununla birlikte BT alanındaki gelişmelerin bir başka yönü daha bulunmaktadır: "İzleme" ve "denetim".

## **2. BT VE YENİ TEHDİTLER: KİTLE İZLEME TEKNOLOJİLERİ**

Görüldüğü gibi BT uygulamaları bireysel ve toplumsal hayata önemli katkılarda bulunmaktadır, ancak diğer yandan insan hakları savunucularınca

eleştirilen teknolojik izleme uygulamaları da yaygınlaşmaktadır. İzleme teknolojilerinin giderek ucuzlaması ve güçlerinin artmasıyla birlikte kitlesel izleme ve insanların hayatı hakkında bilgi toplama her zamankinden çok daha kolay bir hale gelmiştir (ACLU, 2006b). Çalışmanın aşağıdaki kısmında izleme teknolojilerine yönelik kaygıların kökenleri ve bu kaygılara neden olan BT uygulamaları ayrıntılı olarak incelenmektedir.

### 2.1. BT Uygulamalarına Yönelik Kaygıların Kökenleri

Çağdaş dünyada BT, kamu hizmet kalitesini yükseltmek, maliyetleri düşürmek, verimliliği artırmak ve vatandaşın beklentilerine daha duyarlı bir kamu yönetimi modeline geçiş yapmayı sağlayacak bir araç olarak görülmektedir. Ancak diğer pek çok bilimsel buluş gibi BT de, kötü amaçlarla kullanılabilme olasılığı olan bir araçtır. Vatandaş memnuniyetini artırmak için tasarlanmış ve kimilerine göre yeni bir tür özgürlüğün ve yönetim anlayışının ilk adımı olan İnternet ve BT'nin, otoriter/totaliter bir devlet yapısında, toplum içindeki herkesin numaralandırılıp izlendiği bir “açık hapisane” yaratma amacıyla kullanılma riski de mevcuttur. BT tabanlı yeni totalitarizm üzerindeki tartışmaların aslında 20. yüzyıl başlarında ortaya çıktığı görülmektedir. Yevgeny Zamyatin, 1920'lerde “Biz” adını taşıyan kitabında, sınai gelişim ve teknolojik kalkınmanın, bir bolluk ortamı yaratacağını düşünen ve bunu bir tür “ütopya” olarak gören pek çok bilim adamı ve yazardan radikal bir şekilde ayrılmıştır (Zamyatin, 1986). Zamyatin, daha sonra George Orwell (1984) ve Aldous Huxley (1989) gibi yazarlar tarafından da dile getirilen, teknolojik gelişmeyle birlikte doğabilecek “totaliter rejimler” tehlikesine değinerek bir antitez ortaya koymuştur (Zamyatin, Orwell ve Huxley'nin görüşlerinin yarattığı kaygılar çerçevesinde Türkiye’de polis bilgi sistemlerinin algılanma biçimi üzerine detaylı bir değerlendirme ve öneriler için bkz. Leblebici vd. 2003b). O kadar ki, bu antitez veya diğer deyişle anti-ütopya, yazar tarafından, radikal bir eleştiri silahına dönüştürülmüş ve sonuç olarak da “Biz”, SSCB’de hiçbir zaman basılmamış, yazarın ise sürgünde ölmesine neden olmuştur. Kitap, günümüz toplumunda ortaya çıkmaya başlayan ve artık giderek çok daha şiddetli olarak tartışılan bazı gelişmelerden bahsetmektedir: “Geleceğin toplumunda insan doğadan ve kendi benliğinden koparılmış, bizleşerek teknolojiye ve bürokratik devlete teslim olmuştur. Kişisellik yoktur. İnsanların adları değil numaraları vardır. Saydam, cam duvarların arkasında yaşayan insanların her dakikası devletçe belirlenmektedir.” (Zamyatin, 1986).

Teknolojik devrime yöneltilen eleştirilerde, Zamyatin’i izleyen Orwell (Bin Dokuz Yüz Seksen Dört) ve Huxley (Cesur Yeni Dünya), belki de çok daha fazla ses getirmişlerdir (Orwell, 1984; Huxley, 1989). Bu çalışmalara

Foucault'nun (1979), insanların sürekli göz altında tutulduğu Panoptikon Toplum uyarısına yer verdiği "Discipline and Punish: The Birth of the Prison" adlı eseri de eklenebilir. Panoptikon (Panopticon) terimi aslında filozof Jeremy Bentham'ın kardeşi Samuel Bentham'a aittir, fakat terim Jeremy Bentham'ın felsefi görüşleriyle bütünleşmiş olduğundan onun adıyla anılmaktadır (Pease-Watkin, 2003). Bentham'a göre Panoptikon, ortasında bir kulenin bulunduğu ve kuledeki gözetleyenin tüm mahkumları izleyebildiği, çember biçimli bir hapisane binası tasarımına verilen isimdir. Ayrıca tasarım, labirent tarzı duvarlarla ışık ve ses geçişini de engellediğinden, mahkumlar gözetlenip gözetlenmediklerini de fark edememekte, dolayısıyla da onları izleyen bir nöbetçi olmadığı durumlarda bile izlendiklerini düşünerek kaçmaya cesaret edememektedirler (Pease-Watkin, 2003). Yukarıda da belirtildiği gibi Panoptikon terimi asıl şöhretini Michel Foucault'ya borçludur. Foucault (1979), bütün hiyerarşik yapıların sürekli izleme/gözetleme olgusu nedeniyle Bentham'ın hapisanesine evrildiğini belirterek, çağdaş dünyanın bir anlamda büyük bir hapisaneye dönüştüğünü ima eder. Gerçekten de sokaklarda, marketlerde, metroda ve otoparklarda izleme kameralarının kullanımı, özel şirketlerde personelin kameralarla izlenmesi, e-postalarının denetlenmesi, İnternet trafiğinin denetimi gibi uygulamalar, toplumsal hayatın bütününde Panoptik yapıların doğmasına yol açmakta ve bu gelişme de Foucault'nun öngörüsüne güç kazandırmaktadır (ACLU, 2006a; Blanchette ve Johnson 1998:1; Whitaker 2000:139).

## 2.2. BT Uygulamaları Korkuları Destekliyor mu?

Gözetim toplumu kaygılarını alevlendiren BT uygulamaları genel olarak Kitle İzleme Teknolojileri başlığı altında toplanabilir. Bu uygulamalar ağırlıklı olarak kamera ve dinleme araçlarının kullanımına odaklanmaktadır, ancak teknolojik imkânların gelişmesiyle müdahale imkânları da çeşitlenmiştir. Çalışmanın bu kısmında söz konusu uygulamalar altı madde halinde toplanarak detaylı olarak incelenmektedir:

### **- Sabit Hatlı Telefonların, Cep Telefonlarının Dinlenmesi ve İnternet Trafiğinin İzlenmesi**

Mevcut telekomünikasyon teknolojisi, güvenlik birimlerine sabit hatlı telefon ve cep telefonu iletişim trafiğini izleme imkânını sunmaktadır. Telefon dinleme olarak bilinen bu uygulama, çıkarılan kanunlarla mahkeme iznine bağlanmış olsa da, uygulamada zaman zaman durumun aciliyeti gerekçe gösterilerek, gelişmiş ülkelerde dahi bu izinlerin alınmasının göz ardı edilebildiği görülmekte ve kamuoyunda sıklıkla özel hayatın dokunulmazlığına müdahale edildiği yönünde tartışmalar oluşmaktadır (ACLU, 2005).

ABD’de 16 Aralık 2005 tarihli New York Times gazetesinde yer alan bir araştırma, Başkan Bush’un, ABD Ulusal Güvenlik Birimi’ne (National Security Agency/NSA) hakim kararı olmadan binlerce Amerikan vatandaşının telefon ve e-posta trafiğini izleme talimatı verdiğini ve bunun Amerikan anayasasına açıkça aykırı olduğunu belirtmektedir (Risen ve Lichtblau, 2005). Yine ABD’de 2006 yılında USA Today’de yayınlanan bir başka araştırma da aynı konuya değinerek, ülkenin büyük telefon şirketlerinin NSA ile Amerikan vatandaşlarının telefon kayıtlarının izlenmesi konusunda işbirliği yaptığını ortaya koymaktadır (Cauley, 2006). Bu bilgiler ABD hükümetinin yargı makamlarından izin almaksızın telefon görüşmelerini dinlediği iddialarını doğrular gözükmektedir.

Yukarıda sıralanan kaygıları gündemde tutan belki de en tartışmalı iddia ise dünya çapında kitle izleme amacıyla kullanıldığı öne sürülen ve ABD-İngiltere inisiyatifinde bir proje olduğu savunulan, ancak ilgili hükümetlerce resmi olarak kabul edilmemiş ECHELON projesidir (Keefe, 2006; Richelson ve Ball, 1985; Hager, 1996; Coşkun, 2000; Bildirici, 1998). İddialara göre, proje sayesinde, telefon ve İnternet iletişim ağlarının gelişmiş yazılımlar ile sürekli olarak izlenmesi mümkün olabilmektedir. Keefe’ye (2006) göre, ECHELON sistemi, başlangıçta ABD ve İngiltere arasında oluşturulmuş ve ardından da Avustralya, Kanada ve Yeni Zelanda’nın katılımıyla kapsama alanını genişletmiş bir birliktir. Sistem, bilgisayar sistemleri yoluyla radyo, uydu iletişimi, telefon, faks ve e-posta trafiğini izleyerek istihbarat toplama amacına hizmet etmektedir. ECHELON sisteminin başlangıçta Sovyetler Birliği ve Doğu Bloku’nu izlemek amacıyla kullanılırken, günümüzde anti-terör, uyuşturucu trafiği, siyasi ve diplomatik istihbarat amaçlı kullanıldığı savunulmaktadır. Yine iddialara göre sistem bugün sanayi casusluğuna dahi hizmet edebilmektedir (Richelson ve Ball, 1985; Hager, 1996; Coşkun, 2000; Bildirici, 1998).

#### **- Güvenlik Kameralarıyla İzleme**

Yaygın kullanım biçimiyle “güvenlik kameraları” olarak adlandırılan “Kapalı Devre Televizyon” (Closed Circuit Television/CCTV) teknolojisi, belirli bir bölgeden kameralarla elde edilen görüntünün sinyaller yoluyla önceden belirlenmiş sınırlı sayıdaki monitöre aktarımına dayanmaktadır (Urbaneye, 2006). 1950’lerde ilk kameraların trafik düzenlemesi amacıyla kullanılmasının ardından hızla gelişen CCTV teknolojisi, bugün ağırlıklı olarak, suçun önlenmesi ve/veya ortaya çıkarılması amacıyla başvurulmuş bir araç haline gelmiştir (Hempel ve Töpfel, 2002). Güvenlik kamerası kullanımı başlangıçta trafik güzergahları, sokaklar, metro istasyonları, otoparklar, alışveriş merkezleri, işyerleri gibi alanlarda yoğunlaşırken zamanla maliyetinin

oldukça düşmesiyle birlikte; günümüzde binalara, evlere ve ticari taksilere kadar yaygınlaşmıştır. Kameralar pek çok suçun aydınlatılmasında, suçluların yakalanmasında etkili olmakta ve güvenlik güçlerinin çalışmalarını önemli ölçüde desteklemektedir.

Avrupa ülkelerindeki güvenlik kamerası kullanımını farklı boyutlarıyla inceleyen “Urbaneye Projesi” bu alanda AB ülkelerindeki en kapsamlı çalışmalardan biridir (Urbaneye, 2002). Proje kapsamında 2002 yılında yapılan bir araştırmaya göre AB ülkeleri arasında sokaklara yerleştirilen güvenlik kamerası sayısı en yüksek olan İngiltere’de bu rakam 4 milyon civarındaydı (sadece Londra’da yaklaşık 400.000 adet) (McCahill ve Norris, 2002a; McCahill ve Norris, 2002b). Bugün İngiltere’deki tüm şehir merkezleri, güvenlik kameraları ile izlenmektedir ve bu durum, aynı zamanda sıradan vatandaşların da, bilgi ve izinleri olmadan izlendikleri anlamına gelmektedir.

Günümüzde hemen her demokratik ülkede kamuoyu ve basın yayın organları, telefon görüşmelerinin dinlenmesi konusunda oldukça hassastır. Vatandaşların ülke içindeki her hareketinin izlenebildiği yeni kamera sistemlerinin sokaklarda kullanımı ve giderek yaygınlaşması yüzünden kısa vadede benzer bir tartışmanın güvenlik kameraları üzerinde de yürütüleceğine kesin gözüyle bakılabilir. Çünkü, mevcut teknoloji, güvenlik kameralarına eklenen gelişmiş mikrofonlarla sokaklarda yapılan konuşmaların da dinlenebilmesine imkân vermektedir. Bu sayede elde edilen özel hayata ait gizli bilgilerin amaç dışı kullanılmayacağı yasal düzenlemelerle garanti edilmesinin oldukça önemli bir konu olarak gündeme taşınması olasılığı hiç de uzak değildir.

Türkiye’de de “Mobil Elektronik Sistem Entegrasyonu” (MOBESE) projesi ile cadde ve sokakların sürekli olarak kameralarla izlenmesine dayanan gelişmiş sistemler, 2005 yılından itibaren kullanıma girmiştir (İEM, 2006). Resmi olarak 17.06.2005 tarihinde İstanbul’da hizmete giren MOBESE, İstanbul Valiliği’nin desteği ile İstanbul Emniyet Müdürlüğü bünyesinde faaliyete geçirilen bir “Kent Bilgi ve Güvenlik Sistemi” olarak tanımlanmaktadır (İEM, 2006). Projede, İstanbul halkına sunulmakta olan kamu hizmetlerinin iyileştirilmesi, yönetim işlevinin kolaylaştırılması, muhtarlık hizmetlerinin düzenlenmesi ve suç sayısının düşürülmesi hedeflenmektedir. Bu çerçevede 952 muhtarlık, 3.500 polis aracı, 150 mobil polis karakol ünitesi, İl ve İlçe Komuta Merkezleri ve İl Emniyet Müdürlüğü hizmetlerinin yürütülmesini sağlayan 12 ayrı sistem, yazılımlar ile entegre edilmiştir. MOBESE sisteminin yakın gelecekte Türkiye’deki tüm kentlere yayılması planlanmaktadır. (İEM, 2006).

### **- Parmak İzi ve DNA Veri Tabanları**

Parmak izi veri tabanları başlangıçta sadece polis merkezlerine getirilen tutukluların suçlu olup olmadıklarının anlaşılması için kullanılan bir uygulama iken, daha etkili bir analiz için nüfusun tamamının bu veri tabanlarına eklenmesi düşüncesi giderek güç kazanmaktadır (Smith, 2006). Bu nedenle son yıllarda sadece tutukluların değil suçla ilişkisi olmayan sıradan insanların da vize işlemleri, havaalanı kontrol noktaları vb. pek çok işlem esnasında parmak izlerinin alındığı görülmektedir.

Parmak izi veri tabanları bugün artık DNA örneklerine dayanan gelişmiş veri tabanlarıyla birlikte kullanılmaya başlanmıştır. DNA, insan dahil çoğu canlıda bulunan, yaşamın gelişimi ve devamı için gerekli genetik materyali içeren bir kimyasal parmak izi olarak tanımlanabilir (Forensic, 2006). ABD’de hemen her eyaletin suçlulara ait bir DNA veri tabanı bulunmaktadır. Ayrıca FBI tarafından oluşturulan ve CODIS (Combined DNA Index System) adını taşıyan merkezi veri tabanı üzerinden tüm eyaletlere ait verilere ulaşmak da mümkün kılınmıştır (CODIS, 2006). ABD’deki merkezi veri tabanında Haziran 2006 itibariyle 3.452.901 kişiye ait kayıt bulunmaktadır (NDIS, 2006). İngiltere’de ise, 2005 yılı itibariyle 5,5 milyon insanın verilerinden oluşan bir parmak izi veri tabanı mevcuttur ve 1995 yılında kurulan Ulusal DNA Veri tabanında da (National DNA Database/NDNAD) Şubat 2006 itibariyle 3 milyon civarında DNA örneği muhafaza edilmektedir (NDNAD, 2006a; NDNAD, 2006b).

ABD’de DNA veritabanları konusundaki yeni projelerden biri de tüm çalışanlara bir DNA kimlik kartı hazırlanması projesidir. DNA kartının iş başvurularında kullanılması ile yasadışı işçi kullanımına (özellikle sayıları 12 milyonu bulan kaçak göçmen işçiler) son verilmesi de planlanmaktadır (Kugler, 2006). Yakın gelecekte hem ABD hem de İngiltere’de parmak izi veritabanlarında olduğu gibi DNA veri tabanlarının da tüm ülke nüfusunu dahil edecek şekilde genişletilmesi olasılığı oldukça yüksektir, çünkü güvenlik güçleri, bu sistemlerden en etkili sonuçların alınmasının ancak veri tabanının tüm ülkeyi kapsaması ile mümkün olduğunu savunmaktadır (Smith, 2006). Diğer yandan insan hakları savunucuları söz konusu veri tabanlarının amaç dışı kullanımı olasılığının her zaman mevcut olduğunu ve bu takdirde de ciddi sorunların doğacağını belirtmektedirler (Kugler, 2006).

Öte yandan DNA veri tabanlarının suçluların saptanmasındaki gücü de artık rakamsal olarak ortaya çıkmaktadır. İngiltere’de NDNAD’ın kurulduğu tarih olan 1995’ten 2005 yılına kadar geçen sürede yaklaşık 600.000 olayda suçlu kimliğinin DNA karşılaştırması sayesinde belirlenmesi söz konusu

teknolojinin kriminal arařtırmalarda adeta bir devrim yaratmakta olduđunu göstermektedir (New Scientist, 2005).

### **- İnternet Üzerinde Sansür**

Aralarında Çin'in de bulunduđu bazı kapalı rejimlerde ise İnternet trafiđi; İnternet filtreleri ve çeřitli bilgisayar programları yardımıyla yoğun olarak denetlenmekte, ülke vatandaşlarının rejim için tehdit oluşturduğuna inanılan web sitelerine erişimi engellenmektedir (Hermida, 2002). İnsan hakları savunucuları Çin hükümetinin web sitelerini, sohbet odalarını ve özel e-posta mesajlarını denetlemek için görevlendirdiđi memur sayısının 2002 yılında 30.000 civarında olduđunu belirtmektedir (BBC, 2002).

Bugün Çin'de elektronik ortamda hizmet veren arama motorları ve řirketler, Çin'li yetkililerle imzaladıkları özel bir anlaşma (Public Pledge on Self-Discipline for China Internet Industry) çerçevesinde; devlet güvenliđini tehlikeye atacak, toplumsal istikrarı bozacak, yasa ve düzenlemeleri ihlal edecek, batıl inanç ve müstehcenlik içeren bilgilerin yayınlanması ve dağıtımından uzak duracaklarını taahhüt etmektedirler (HRW, 2006). Örneđin, Çin'ce hizmet sunan, "Yahoo China" ve "Google China" arama motorlarında, aralarında "Tiananmen Meydanı", "Tibet" ve "Falun Gong tarikatı" gibi kelimelerin; "New York Times" gazetesi, "Radio Free Asia", "Human Rights Watch" ve "Avustralya Yayın Birliđi" gibi kurumlara ait web sitelerinin bulunduđu binlerce yasaklı kelime, deyim ve web sitesinin arařtırılması imkânı bulunmamaktadır (HRW, 2006).

Yahoo ve Google'ın üst düzey yetkilileri bu durumun dođal olduđunu, çünkü kurumlarının faaliyette buldukları ülkenin hukuk kuralları ve düzenlemelerine uymak zorunda olduklarını belirtmektedirler (Wong, 2002). 2006 yılı Ocak ayında ABD kamuoyunda, Çin hükümetinin belirlediđi bazı kelimelere oto-sansür uyguladıkları yönünde eleřtirilere maruz kalan Microsoft Şirketi yetkilileri de aynı gerekçeleri ileri sürerek, Çin'deki web sitelerinde Çin hükümetinin mevcut yasalarına uymak zorunda olduklarını belirten bir yanıt yayınlamak zorunda kalmışlardır (HRW, 2006). Bunlara ek olarak yine Çin'de hizmet sunan MSN Messenger ve Skype gibi sohbet sitelerinde de yazılı sohbet esnasında Çin hükümetinin yasaklılar listesindeki kelimelerin kullanımı mümkün olamamaktadır (HRW, 2006).

**- Devlet Birimlerinin, Arama Motorları, Sohbet Siteleri ve e-posta Servis Sağlayıcılarından Bireylere Ait Özel Bilgileri Talep Hakkı**

Arama motorları, sohbet siteleri ve e-posta servis sağlayıcıları, bu araçları kullanan insanların özel hayatlarına ait çok değerli bir bilgi havuzuna sahiptirler. Bu alandaki temel kaygı da söz konusu bilgilerin amaç dışı kullanım riskidir. Örneğin bir arama motoru, onu kullanan kişinin tüm ilgi alanlarına ilişkin döküme sahiptir. Sohbet siteleri ise kişilerin özel ve ticari tüm bağlantılarını açığa çıkarabilir. Yine e-posta servisleri de kişilerin özel veya ticari bağlantılarına ait doğrudan bilgi sunabilirler. Yukarıda da değinildiği gibi, servis sağlayıcı şirketler buldukları ülkenin yasalarına uymaktadırlar, bir diğer deyişle eğer devlet birimleri herhangi bir bilgi talebinde bulunurlarsa bu bilgiler kendilerine verilmektedir. Örneğin Google arama motoruna ait “Gizlilik Politikası” incelendiğinde, devlet müdahaleleriyle ilgili dokuzuncu maddede, şirketin devlet organlarından gelecek “arama emirleri, mahkeme emirleri veya kişisel bilgileri edinmeye yönelik celpler gibi yasal süreçlere” uyduğu açıkça belirtilmektedir (Google Gizlilik Merkezi, 2006). Google’a bağlı bir e-posta ve sohbet hizmeti olan Gmail’e ait Gizlilik Politikası’nda ise kullanıcılar tarafından silinen e-postaların, şirketin yedekleme sisteminde çevrim dışı (offline) olarak saklanabileceği belirtilmektedir. Görüldüğü gibi Gmail’in, geçmişe yönelik bir arşivleme yapabileceği beyan edilmektedir. Bu durum, istendiğinde yıllar öncesine ait e-posta trafiği ve içerikleri ile sohbet kayıtlarına ait arşiv bilgilerinin de devlet birimlerine sağlanabileceği anlamına gelmektedir (Gmail Privacy Notice, 2005). Söz konusu teknolojik imkânların amaç dışı kullanım halinde özel hayatın dokunulmazlığına önemli ölçüde zarar vermesi kaçınılmazdır.

**- Terör Şüphelileri ve Yardımcılarını İçeren Elektronik Veri Tabanları**

11 Eylül 2001 saldırıları sonrasında ABD’de yaşanan süreç insan hakları savunucularının teknolojinin kullanımı konusundaki pek çok kaygısına dayanak olmaktadır. Washington Post gazetesinde yayınlanan bir araştırma, ABD’de 11 Eylül 2001 saldırılarının ardından oluşturulan geniş kapsamlı anti-terör yapılanmasının boyutlarının ne denli büyük olduğunu gözler önüne sermektedir (Pincus ve Eggen, 2006). ABD’de söz konusu yapılanmanın önemli bir parçası da Ağustos 2004’te Başkan Bush tarafından kurulan “Ulusal Anti-Terör Merkezi”dir (National Counterterrorism Center/NCTC) (NCTC, 2006).

NCTC, ABD’de terörizm konusunda tüm kurumlar tarafından elde edilen istihbaratı analiz etmek ve entegre etmekle sorumlu ana birim olarak faaliyetlerini yürütmektedir (NCTC, 2006; NCTC, 2005). NCTC tarafından



kullanılan ve ulusal ve uluslararası terör şüphelilerinin ve onlara yardım sağlayanların isimlerinin yer aldığı veri tabanı, 2006 yılı Mart ayı itibarıyla 325.000 kişilik bir hacme ulaşmıştır (Guardian, 2006; Pincus ve Eggen, 2006). Uzmanlara göre bu sayı 2003 yılındaki 75.000'ler düzeyinden yaklaşık 4 kat büyüerek bugünkü düzeyine çıkmıştır ve sürekli olarak da büyümeye devam etmektedir. NCTC listesi, temel olarak NSA (National Security Agency), CIA (Central Intelligence Agency) ve FBI (Federal Bureau of Investigation) tarafından hazırlanmıştır ve halen güncelleme işlemleri söz konusu kurumlar tarafından yürütülmektedir. Liste, ABD'de kamu güvenliğiyle ilgili tüm birimler tarafından kullanılmaktadır. Güvenlik amacıyla oluşturulan NCTC yapılanmasına karşı, sivil özgürlük savunucuları ve uzmanlar, bu ölçüde kapsamlı terörizm listelerinin çok sayıda masum insanın ismini de içermesi olasılığının arttığına dikkat çekmektedir (Pincus ve Eggen, 2006).

Görüldüğü gibi devlet birimleri BT'den, kitle izleme alanında; denetim, sansür, dinleme, görüntüleme, bilgi toplama, arşivleme vb. uygulamaların oluşturduğu geniş bir yelpazede yararlanmaktadır. Söz konusu uygulamaların tümü güçlü bir hukuksal çerçeve içerisinde düzenlenmesi gereken, aksi halde bireysel özgürlükler üzerinde olumsuz sonuçlar yaratma potansiyeli yüksek uygulamalardır. Çalışmanın izleyen kısmında bireysel özgürlüklere duyarlı bir hukuksal çerçevenin temel unsurlarının neler olması gerektiği ve terörle mücadele paralelinde şekillenen yeni dünya gündeminde mahremiyeti koruyucu hukukun yeri üzerinde durularak, bu yönde değerlendirme ve önerilere yer verilecektir.

## **GENEL DEĞERLENDİRME VE SONUÇ**

Günümüzde kamu hizmetlerinde süratle yaygınlaşan BT uygulamalarının avantaj ve dezavantajları üzerindeki tartışmalar halen sürmektedir. Ancak bu tartışmalar, yeni teknolojilerin oluşturduğu hayat tarzının daha kısıtlayıcı değil, daha özgürlükçü olabilmesinin ve vatandaşlara sunulan hizmetlerin kalitesinin geliştirilmesinin de yollarını açmaktadır.

BT uygulamalarının günümüz toplumuna sunduğu imkânlar bir araya getirildiğinde; özellikle gelişmekte olan ülkelerde iktisadi anlamda ekonomiye sağlayacağı katkıların başka iyileştirme çalışmalarıyla karşılaştırılmayacak ölçüde yüksek olduğu anlaşılmaktadır. Bununla birlikte söz konusu imkânlardan yararlanan vatandaşların haklarının sürekli güncellenen ve geliştirilen hukukî düzenlemelerle güvence altına alınmadığı ülkelerde, BT'nin bireysel özgürlükleri kısıtlamak amacıyla kullanılma tehlikesinin ağır bastığı da bir gerçektir.

### ***Bireysel Özgürlükleri Koruyucu Bir Hukukî Altyapı Zorunluluğu***

Gücün iktidardakilerce kötüye kullanımı, genellikle çağdaş demokrasinin gereği olan ve birbiriyle bağlantılı iki ilkenin, “topluma hesap verme” (accountability) ve “şeffaflık” (transparency) ilkelerinin ihlali sonucunda oluşmaktadır (Brin, 1998). Dolayısıyla hesap verme ve şeffaflık konusunda oluşturulacak etkili bir hukukî altyapı ile amaç dışı kullanım engellenerek, bireysel özgürlüklerin korunmasını garanti altına almak mümkündür. Ancak gelişmekte olan ülkelerde bu yöndeki düzenlemeler tamamlanmadan, izleme ve veri tabanı teknolojilerinin kullanımına geçildiği ve dolayısıyla da uygulamaların istismara açık olduğu görülmektedir. İstismarın önlenmesi ve şeffaflığın sağlanabilmesi amacıyla gelişmiş ülkelerde 1960 ve 70’li yıllarda önemli adımlar atıldığı görülmektedir. Bu alanda en önemli adımlardan biri, ABD’de 1966 yılında çıkarılan Bilgi Edinme Özgürlüğü Yasası’dır (Freedom of Information Act) (FOIA, 1966; USDOJ, 2006). 1972 yılında ABD’de önemli bir siyasi çalkantı yaratan Watergate skandalının ardından ise 1974’te Özel Hayatın Korunması/Mahremiyet Yasası (Privacy Act) parlamentodan geçmiştir. ABD’yi izleyen Fransa 1974 yılında “Bilişim ve Özgürlükler Komisyonu’nu” (Commission Nationale de l’Informatique et des Libertés); İngiltere ise 1979 yılında “Lindop Komitesi’ni” (Lindop Committee on Data Protection) kurarak “Veri Koruma” alanında hukuksal bir altyapı oluşturma çalışmalarını başlatmışlardır. AB ülkeleri ise 24 Ekim 1995’te çıkarılan “Veri Koruma Yasası” (Data Protection Law) ile bu alanda en kapsamlı düzenlemelerden birini oluşturmuşlardır (Directive 95/46/EC, 1995)<sup>2</sup>. Türkiye ise, biraz gecikmeli olmakla birlikte, Ekim 2003’te parlamentodan geçen ve Nisan 2004’te uygulamaya giren 4892 sayılı yasa ile “Bilgi Edinme Özgürlüğünü” tanımıştır. 24 Ocak 2004’te yürürlüğe giren 25356 sayılı “Dilekçe ve Bilgi Edinme Hakkının Kullanılması” başlıklı Başbakanlık Genelgesi ve 27 Nisan 2004 tarihinde yürürlüğe giren 25445 sayılı “Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas ve Usuller Hakkında Yönetmelik” ile de kamu yönetiminde “şeffaflık” ve “topluma hesap verme” konusundaki hukukî çerçeve sağlamlaştırılmaya çalışılmıştır<sup>3</sup>. Diğer taraftan mahremiyetin korunması alanında da adımlar atılmış ve hakim kararı olmadan telefonların dinlenmesi olgusunu sonlandırmak amacıyla “Telekomünikasyon İletişim Başkanlığı” kurulmuştur<sup>4</sup>. 23 Temmuz 2006 tarihinde faaliyete geçen Başkanlık, izinsiz dinlemeleri tespit etme ve dinlemelerin; 23.7.2005 tarihinde yürürlüğe giren 5397 sayılı kanuna ve 10.11.2005 tarihli Resmi Gazetede yayımlanarak yürürlüğe giren “Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik” hükümlerine uygunluğunu denetleme görevini üstlenmiştir (Telekomünikasyon Kurumu, 2006). Ancak henüz bir veri

koruma yasasının çıkarılmamış olması, Türkiye açısından ciddi bir eksiklik olarak göze çarpmaktadır. Bu çerçevede AB müktesebatına uyum çalışmaları kapsamında, “Adalet ve İçişleri” başlığı altında yer alan veri koruma alanında, henüz kat edilmesi gereken önemli bir mesafe bulunduğu görülmektedir<sup>5</sup>.

### ***Terör Tehdidinin Şekillendirdiği Yeni Bir Bakış Açısı***

21. Yüzyıl’da devlet yönetiminde ve kamu hizmetlerinin sunumunda hız, kalite, verimlilik ve maliyet alanlarında iyileştirmelerin, artık BT ve sağladığı imkânlar dikkate alınmadan tasarlanabilmesi mümkün değildir. Ancak kamu hizmetlerinde BT’nin amaç dışı kullanımı halinde bireysel özgürlükler alanında doğabilecek muhtemel riskler, artık sadece gelişmekte olan ülkelerde değil, gelişmiş ülkelerde de ciddiye alınıp tartışılmaktadır. Çünkü BT uygulamalarının amaç dışı kullanımı genellikle bireyin temel hak ve özgürlüklerinden birini oluşturan özel yaşamın gizliliğinin tahribi sonucunu yaratmakta, devlet ve vatandaş arasındaki güven ilişkisi zedelenmektedir. Söz konusu risklerin ortadan kaldırılması yoluyla vatandaş ve devlet arasındaki “karşılıklı güveni” tesis etmek ve sürekli kılmak gerekmektedir. Ancak bunun, dünyanın bugün içinde bulunduğu terör tehdidi nedeniyle kolayca gerçekleştirilebilmesi imkânı da giderek azalmaktadır. Bu nedenle BT alanında artık terör olgusunu da içeren daha “kapsamlı ve yeni bir bakış açısının” oluşturulması bir zorunluluktur. Çünkü BT ve bireysel özgürlükler alanındaki mevcut literatürün iki önemli unsurdan oluşan yeni BT gündeminin gerisinde kalmaya başladığı görülmektedir: 1. Batılı ülkelerdeki terör paranoyası ve bu yüzden daha yüksek bir hızla geliştirilen izleme teknolojileri, 2. Hukuksal çerçevenin, teröre karşı mücadelenin bireysel özgürlükleri tahrip etmeyecek bir platformda yürütülmesini sağlamak ve izleme teknolojilerindeki gelişmenin hızına ayak uydurabilmek amacıyla sürekli olarak güncellenmesi ihtiyacı. İlerideki çalışmalara ve bu yeni bakış açısına katkı sağlamak amacıyla aşağıda, söz konusu iki gündem maddesi analiz edilmektedir:

**1. Batılı Ülkelerde Terör Paranoyası ve Kitle İzleme Teknolojilerine Büyük Ölçekli Yatırımlar:** BT uygulamalarının yarattığı tehditleri içeren literatürde sıklıkla, gelişmekte olan ülkeler ve otoriter/kapalı rejimlerde, özgürlükleri koruyucu bir hukukî altyapı oluşturulmadığından dolayı bireyin mahremiyetine zarar verildiği vurgulanmaktadır. Ancak bu çalışmanın bulguları artık söz konusu düşüncenin gerçeği tam anlamıyla yansıtmadığını göstermektedir, çünkü Batılı ülkelerde son yıllarda oluşan “terör paranoyası” nedeniyle, bugün artık sanıldığı aksine “Gözetim Toplumu” yaratma tehlikesinin, ABD ve İngiltere gibi gelişmiş demokratik sistemlerde daha yoğun olarak yaşandığı görülmektedir (ACLU, 2005; ACLU, 2006b). Bunun en somut

örneği, ABD’de 11 Eylül 2001’de gerçekleşen saldırıdan 6 hafta sonra kongrenin adeta panik içinde çıkardığı “Vatansever Yasası” (Patriot Act) ile güvenlik güçlerinin yetkilerinin olağanüstü ölçüde artırılmasıdır (Stanley ve Steinhardt, 2003: 9). Ayrıca, ABD ve diğer pek çok Batılı ülke, söz konusu paranoya sonucunda, “Kitle İzleme Teknolojileri” alanına büyük bütçeler ayırmaktadır ve buna hukukî denetimin gevşetilmesi, yargı izni olmaksızın dinleme gibi uygulamaların da eklenmesiyle, insan hakları savunucularının oldukça kaygı verici buldukları bir süreç yaşanmaktadır. Bu durum, özgürlüklerin korunması ile ilgili çalışmalarda bugüne dek sıklıkla kullanılan “gelişmiş ülke-gelişmekte olan ülke” ve “açık toplum-kapalı toplum” ayrımlarının artık açıklayıcılığını yitirdiğini göstermektedir. Söz konusu yaklaşımlar gelişmiş Batı ülkelerinde yaşanan terör paranoyasını ve yarattığı olumsuz sonuçları göz ardı etmektedir. İzleyen çalışmalarda, günümüz koşullarında artık koruyucu bir hukuksal altyapının gerçekleştirilmesinin tek başına yeterli olmadığı; “hukukun üstünlüğüne inanan”, “demokratik haklar konusunda duyarlı” ve “sağduyulu” kamu yönetimlerinin de bu yapıya eşlik etmesi gerektiği vurgulanmalıdır.

**2. Hukukun, Terör Paranoyasının Oluşturduğu Yeni Dünya Gündemini ve BT’nin Gelişme Hızını Yakalaması:** BT alanındaki mevcut literatür, özellikle gelişmekte olan ülkelerde hukukî altyapı kurulmadan gerçekleştirilen BT uygulamalarının zararlı etkilerinden söz etmektedir. Ancak bu yaklaşım tek başına anlamlı değildir, çünkü gelişmekte olan bir ülkenin, gelişmiş ülkelere ait hukuksal mevzuatı benimsemesiyle, hukuka uygunluğun kolayca sağlanabileceği gibi oldukça hatalı bir kanaatin doğmasına yardımcı olmaktadır. Oysa hukukî altyapının ve mevzuatın sürekli olarak güncellenemediği ve geliştirilemediği durumlar da, en az bir hukuksal çerçeveye sahip olmamak kadar yıkıcı olabilmektedir. Bu ihtiyacı yaratan önemli faktörlerden biri, BT’nin genel teknoloji dalgasının içerisinde en hızlı gelişen alan olmasıdır. Bu da ister istemez çoğu durumda, hukuksal düzenlemelerin BT uygulamalarının önünde gitmesi değil, onları izlemesi anlamına gelmekte; değişimin hızı çok yüksek olduğu için, güncellemelerin de süratle gerçekleştirilmesi gerekmektedir. Güncellemeyi zorunlu kılan diğer faktör ise yukarıda da belirtildiği gibi terör tehdidi nedeniyle Batılı ülkelerde mahremiyet konusundaki hukukî mevzuatın yeniden düzenlenmesi ve bir anlamda da hukukî denetimin gevşetilmesi gibi bir eğilimin yaygınlaşmaya başlamasıdır. Oysa yapılması gereken, mevcut hukuksal yapının, teröre karşı mücadelenin insan haklarını ihlal etmeden sürdürülmesine imkân verecek ve “güvenlik ve mahremiyet” denkleminde yeni bir denge oluşturacak şekilde tekrar düzenlenmesi olmalıdır. Görüldüğü gibi BT alanındaki hukuksal çerçeve, değişen gündem ve yeni teknolojik uygulamaların yarattığı beklenmedik

sonuçlar paralelinde sürekli olarak güncellenmek durumundadır. Dolayısıyla, izleyen çalışmalarda sadece bir hukukî altyapının öneminden bahsetmekle yetinilmemeli, dünya gündeminin ve BT alanının değişim hızından kaynaklanan hukuksal güncelleme ve geliştirme ihtiyacının önemi ve söz konusu güncellemeleri yapabilecek ölçüde iyi yetişmiş bir BT hukukçuları grubunun oluşturulması zorunluluğu da önemle vurgulanmalıdır.

Sonuç olarak, bu çalışmanın bulguları, 21. Yüzyıl'da bireyin mahremiyetinin korunmasının ve BT uygulamaları yoluyla bireysel özgürlüklerin geliştirilmesinin mümkün olduğunu, ancak bu idealin gerçekleştirilebilmesinin üç temel koşula bağlanabileceğini göstermektedir; değişen şartlara göre sürekli olarak güncellenen ve güçlü yaptırımları olan bir hukuksal çerçeve; demokratik, açık ve çoğulcu bir toplum yapısı ve bu ideale adanmış bir kamu yönetimi.

## NOTLAR

<sup>1</sup> Mahremiyet, bireyin özel yaşamını diğerlerinin izleme alanının dışında tutabilme ve kendisi hakkındaki bilgi akışını denetleyebilme kabiliyetidir. Bir başka ifadeyle, kişisel hayata ait bilgilerin gizliliğini koruyabilme kabiliyeti olarak da tanımlanabilir.

<sup>2</sup> AB ülkelerinde veri koruma mevzuatı ile ilgili daha fazla bilgi için Avrupa Komisyonu Veri Koruma web sitesini ziyaret ediniz  
<[http://ec.europa.eu/justice\\_home/fsj/privacy/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm)>.

<sup>3</sup> Türkiye'de bilgi edinme hakkının kullanımına ilişkin uygulamada çeşitli sorunlar yaşandığı ve bazı devlet birimlerinin, vatandaşlardan gelen bilgi edinme taleplerine yeterince hassas davranmadığı görülmektedir (bu konuda kapsamlı bir çalışma için bkz. Akdeniz, 2004). Ayrıca konunun Türkiye boyutuyla ilgili daha fazla bilgi için bkz. <<http://www.bilgiedinmehakki.org>> ve dünyadaki gelişmeler için bkz. Uluslararası Bilgi Edinme Özgürlüğü Ağı web sitesi <<http://www.foiadvocates.net>>.

<sup>4</sup> Türkiye'de mahremiyetin korunması konusunda yürütülen çalışmaları kapsayan ve Uluslararası Mahremiyet Örgütü (Privacy International) tarafından hazırlanmış bir rapor için bkz. (Privacy International, 2004).

<sup>5</sup> “Kişisel Verilerin Korunması Kanunu Tasarısı” Adalet Bakanlığı tarafından bakanlıklar ile ilgili kamu kurum ve kuruluşlarının görüşüne gönderilmiştir. 2 Haziran 2004 tarihinde Başbakanlığa sevk edilen tasarı, Başbakanlığın 14.03.2005 tarih ve 1113 sayılı yazısı gereği “Üzerinde Çalışılanlar” bölümüne alınmıştır. Adı geçen tasarı, veri korumasında genel kabul gören temel uluslararası metinlerin izini taşımakta ve Türkiye'de kişisel verilerin işlenmesinde hukuka uygunluk denetimi yapacak olan “Kişisel Verileri Koruma Kurumu”nun kurulmasını öngörmektedir (Ersoy, 2006).

**KAYNAKÇA**

- ACLU (2005) **NSA Spying on Americans is Illegal**, American Civil Liberties Union/ACLU web sitesi, 29.12.2005, son erişim tarihi: 11.08.2006, <http://www.aclu.org/privacy/spying/23279res20051229.html>
- ACLU (2006a) **Surveillance & Wiretapping**, American Civil Liberties Union/ACLU web sitesi, son erişim tarihi: 11.08.2006, <http://www.aclu.org/privacy/spying/index.html>
- ACLU (2006b) **ACLU Ad Calls for Investigation Into President's Surveillance of U.S. Citizens**, American Civil Liberties Union/ACLU web sitesi, son erişim tarihi: 11.08.2006, < <http://www.aclu.org/safefree/spying/index.html>>
- Akdeniz, Y. (2003) **Beyaz Kitap: İnternet'in Çok Taraflı Yönetimi-Türkiye'deki Politika Yaratma Sürecinin Çağdaşlaşmasına Doğru**, Türkiye Bilişim Vakfı Dizisi: 1, İstanbul: Papatya Yayıncılık.
- Akdeniz (2004) **Türkiye'de Bilgi Edinme Hakkı Kanunu'nun Bakanlıklar Tarafından Uygulanması**, son erişim tarihi: 11.08.2006, [http://www.bilgiedinnehakki.org/doc/tr\\_uygulama\\_rapor.pdf](http://www.bilgiedinnehakki.org/doc/tr_uygulama_rapor.pdf)
- Akşam (2005) **Telekulak'ta Patlama**, Akşam Gazetesi web sitesi, 21 Şubat 2005 Pazartesi, son erişim tarihi: 11.08.2006, <http://www.aksam.com.tr/arsiv/aksam/2005/02/21/politika/politika5.html>
- Aydın, M. D. (2005) "eAvrupa+ ve Türkiye: Bilgi Teknolojileri Alanında Avrupa Birliği Kriterlerine Uyum", **Hacettepe Üniversitesi İİBF Dergisi**, 23(1), 287-311.
- BBC (2002) **China Blocking Google**, BBC News web sitesi, Pazartesi, 2 Eylül 2002, son erişim tarihi: 11.08.2006, <http://news.bbc.co.uk/2/hi/technology/2231101.stm>
- Bensghir, T. K. (1996) **Bilgi Teknolojileri ve Örgütsel Değişim**, Ankara: TODAİE, Yayın No: 274.
- Bildirici, F. (1998) **Gizli Kulaklar Ülkesi**, İstanbul: İletişim Yayınları.
- Blanchette, J. F. and D. Johnson (1998) "Cryptography, Data Retention, and The Panopticon Society", **Computers and Society**, June.
- Brin, D. (1998) **The Transparent Society**, New York: Addison-Wesley.

- Brown, M. M. and C. Brudney (1998) "A 'Smarter, Better, Faster, and Cheaper' Government", **Public Administration Review**, July/August.
- Cauley, L. (2006) **NSA has Massive Database of Americans' Phone Calls**, USA Today web sitesi, son erişim tarihi: 11.08.2006, [http://www.usatoday.com/news/washington/2006-05-10-nsa\\_x.htm](http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm)
- CDD (2006) **Center for Digital Democracy**, Dijital Demokrasi Merkezi web sitesi, Son Erişim Tarihi: 11.08.2006, <http://www.democraticmedia.org>
- CODIS (2006) **Combined DNA Index System**, FBI web sitesi, son erişim tarihi: 11.08.2006, <http://www.fbi.gov/hq/lab/codis/index1.htm>
- Coşkun, E. (2000) **Küresel Gözaltı: Elektronik Gizli Dinleme ve Görüntüleme**, Ankara: Ümit Yayınları.
- Directive 95/46/EC (1995) **The Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data**, 24 Ekim 1995, son erişim tarihi: 11.08.2006, <[http://www.cdt.org/privacy/eudirective/EU\\_Directive\\_.html](http://www.cdt.org/privacy/eudirective/EU_Directive_.html)>
- Drucker, P. F. (1994) **Yeni Gerçekler**, Çev. B. Karanakçı, Ankara: Türkiye İş Bankası Kültür Yayınları.
- Drucker, P. F. (2000) **21. Yüzyıl İçin Yönetim Tartışmaları**, Çev. İ. Bahçivangil ve G. Gorbon, İstanbul: Epsilon Yayıncılık.
- Economist (2000), "Survey: Government and the Internet-Digital democracy", **The Economist** dergisi, 22 Haziran 2000.
- eEurope Project (2000) **eEurope: An Information Society for All**, Avrupa Konseyi Raporu, 23-24 Mart 2000, Lizbon, son erişim tarihi: 11.08.2006, [http://europa.eu.int/information\\_society/eeurope/2002/news\\_library/pdf\\_files/initiative\\_en.pdf](http://europa.eu.int/information_society/eeurope/2002/news_library/pdf_files/initiative_en.pdf)
- eEurope 2002 Project (2000) **eEurope 2002: An Information Society for All-Action Plan**, Avrupa Konseyi ve Avrupa Komisyonu Raporu, 14.06.2000, Brüksel, son erişim tarihi: 11.08.2006, [http://europa.eu.int/information\\_society/eeurope/2002/action\\_plan/pdf/action\\_plan\\_en.pdf](http://europa.eu.int/information_society/eeurope/2002/action_plan/pdf/action_plan_en.pdf)
- eEurope 2005 Project (2002) **eEurope 2005: An Information Society for All**, Avrupa Konseyi Raporu, 21-22 Haziran 2002, son erişim tarihi: 11.08.2006, [http://europa.eu.int/information\\_society/eeurope/2002/action\\_plan/text\\_en.htm](http://europa.eu.int/information_society/eeurope/2002/action_plan/text_en.htm)

- eGovernment (2004) **Top of the Web: User Satisfaction and Usage Survey of eGovernment services**, Avrupa Komisyonu Bilgi Toplumu Genel Müdürlüğü (DG Information Society European Commission) e-Devlet Birimi (eGovernment Unit) için Aralık 2004'te Hazırlanan Rapor, son erişim tarihi: 11.08.2006.  
[http://europa.eu.int/information\\_society/activities/egovernment\\_research/doc/top\\_of\\_the\\_web\\_report\\_2004.pdf](http://europa.eu.int/information_society/activities/egovernment_research/doc/top_of_the_web_report_2004.pdf)
- Erkan, H. (1998) **Bilgi Toplumu ve Ekonomik Gelişme**, Ankara: Türkiye İş Bankası Kültür Yayınları No: 326.
- Ersoy, E. (2006) "Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması", **Akademik Bilişim 2006 Konferansı**, 9-11 Şubat 2006, Pamukkale Üniversitesi, Denizli, son erişim tarihi: 11.08.2006, <http://ab.org.tr/ab06/bildiri/6.doc>
- FOIA (1966) **Freedom of Information Act**, ABD Bilgi Edinme Özgürlüğü yasası tam metni, son erişim tarihi: 11.08.2006, [http://www.usdoj.gov/oip/foia\\_updates/Vol\\_XVII\\_4/page2.htm](http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm)
- Forensic (2006) **What is DNA?** İngiltere İç İşleri Bakanlığı'na bağlı The Forensic Science Service web sitesi, son erişim tarihi: 11.08.2006, [http://www.forensic.gov.uk/forensic\\_t/inside/about/general.htm#9](http://www.forensic.gov.uk/forensic_t/inside/about/general.htm#9)
- Foucault, M. (1979) **Discipline and Punish: The Birth of the Prison**, New York: Vintage Books.
- Fox, S. (2005) **Deep Throat Revealed**, Washington Post web sitesi, 31 Mayıs 2005, son erişim tarihi: 11.08.2006, <http://www.washingtonpost.com/wp-srv/national/longterm/watergate/front.htm>
- Gmail Privacy Notice (2005) **Gmail Privacy Policy**, 14 Ekim 2005, son erişim tarihi: 11.08.2006, <http://mail.google.com/mail/help/privacy.html>
- Google Gizlilik Merkezi (2006) **Gizlilik Politikası-Sık Sorulan Sorular**, Google web sitesi, son erişim tarihi: 11.08.2006, <[http://www.google.com/privacy\\_faq.html](http://www.google.com/privacy_faq.html)>
- Guardian (2006) **Civil liberties fear as US terror suspect list rises to 325,000**,
- The Guardian gazetesi web sitesi, Perşembe, 16 Şubat, 2006, son erişim tarihi: 11.08.2006, <http://www.guardian.co.uk/usa/story/0,,1710756,00.html>
- Hacker K. L. and J. V. Dijk (2000) **Digital Democracy: Issues of Theory and Practice**, London: Sage Publications.



- Hager, N. (1996) **Secret Power-New Zealand's Role in the International Spy Network**, New Zealand: Craig Potton Publishing.
- Hague, B. N. ve B. D. Loader (1999), **Digital Democracy: Discourse and Decision Making in the Information Age**, Londra: Routledge.
- Hempel, L. ve E. Töpfel (2002) **Inception Report**, Avrupa Birliği Urbaneye Projesi web sitesi, Working Paper 1, son erişim tarihi: 11.08.2006, [http://www.urbaneye.net/results/ue\\_wp1.pdf](http://www.urbaneye.net/results/ue_wp1.pdf)
- Hermida, A. (2002) **Behind China's internet Red Firewall**, BBC News web sitesi, Salı, 3 Eylül 2002, son erişim tarihi: 11.08.2006, <http://news.bbc.co.uk/1/hi/technology/2234154.stm>
- HRW (2006) **How Multinational Internet Companies assist Government Censorship in China**, Human Rights Watch (HRW) web sitesi, <http://www.hrw.org/reports/2006/china0806/5.htm>
- Huxley, A. (1989) **Cesur Yeni Dünya**, (çeviren: Ender Gürol), Güneş Yayınları, İstanbul.
- İEM (2006) **MOBESE**, İstanbul Emniyet Müdürlüğü MOBESE web sitesi, son erişim tarihi: 11.08.2006, <http://mobese.iem.gov.tr/>
- Keefe, P. R. (2006) **Chatter: Uncovering the Echelon Surveillance Network and the Secret World of Global Eavesdropping**, New York: Random House.
- Knox, O. (2006) **Bush seeks political gains from foiled plot**, Yahoo News web sitesi, son erişim tarihi: 11.08.2006, [http://news.yahoo.com/s/afp/20060810/pl\\_afp/britainattacksairline\\_060810185330](http://news.yahoo.com/s/afp/20060810/pl_afp/britainattacksairline_060810185330)
- Kugler, S. (2006) **NYC Mayor Advocates U.S. Worker Database**, Breitbart.com web sitesi, 24 Mayıs 2006, son erişim tarihi: 11.08.2006, <http://www.breitbart.com/news/2006/05/24/D8HQE6B80.html>
- Leblebici, D. N., M. K. Öktem ve M. D. Aydın (2003a) "Türkiye'de Kamu Kesiminde Bilgi Teknolojileri Uygulamaları ve E-Bürokrasi: Örgütsel Dönüşüm Üzerindeki Etkiler", **Kamu Yönetiminde Kalite 3. Ulusal Kongresi**, Ankara: TODAİE, Yayın no: 319, 501-512.
- Leblebici, D. N., M. K. Öktem, M. D. Aydın ve İ. Pekgözlü (2003b) "Bilgi Teknolojileri ve Polis Bilgi Sistemlerinin Etkililiği Üzerine Bir Değerlendirme", **1. Polis Bilişim Sempozyumu**, Ankara: Emniyet Genel Müdürlüğü: 309-313.

- Lehr, W. and F. R. Lichtenberg, Frank R. (1998) "Computer Use and Productivity Growth", **The Journal of Industrial Economics**, June..
- Mann, L., E. Eckert and C. S. Knight (2000) **Global Electronic Commerce: A Policy Primer**, Washington: Institute for International Economics.
- McCahill, M. and C. Norris (2002a) **CCTV in Britain**, Avrupa Birliđi Urbaneye Projesi web sitesi, Working Paper No: 3, son eriřim tarihi: 11.08.2006, [http://www.urbaneye.net/results/ue\\_wp3.pdf](http://www.urbaneye.net/results/ue_wp3.pdf)
- McCahill, M. and C. Norris (2002b) **CCTV in London**, Avrupa Birliđi Urbaneye Projesi web sitesi, Working Paper No: 6, son eriřim tarihi: 11.08.2006, [http://www.urbaneye.net/results/ue\\_wp6.pdf](http://www.urbaneye.net/results/ue_wp6.pdf)
- MOBESE (2006) **Mobil Elektronik Sistem Entegrasyonu projesi**, son eriřim tarihi: 11.08.2006, <http://mobese.istanbul.pol.tr>
- NCTC (2005) **Report on Reauthorization of the USA Patriot Act**, ABD Temsilciler Meclisine sunulan ve Ulusal Anti Terör Merkezi (National Counterterrorism Center) ile ilgili bilgileri içeren rapor, son eriřim tarihi: 11.08.2006, [www.fas.org/irp/congress/2005\\_rpt/hrpt109-174pt2.html](http://www.fas.org/irp/congress/2005_rpt/hrpt109-174pt2.html)
- NCTC (2006) **Values Statement**, ABD'ye ait National Counterterrorism Center web sitesi, son eriřim tarihi: 11.08.2006, [http://www.nctc.gov/about\\_us/about\\_nctc.html](http://www.nctc.gov/about_us/about_nctc.html)
- NDIS (2006) **National DNA Index System Statistics**, FBI web sitesi, son eriřim tarihi: 11.08.2006, <http://www.fbi.gov/hq/lab/codis/clickmap.htm>
- NDNAD (2006a) **The National DNA Database**, İngiliz Parlamentosu belgeleri, Şubat 2006, son eriřim tarihi: 11.08.2006, <http://www.parliament.uk/documents/upload/postpn258.pdf>
- NDNAD (2006b) **The National DNA Database**, İngiltere'ye ait The Forensic Science Service web sitesi, Şubat 2006, son eriřim tarihi: 11.08.2006, [http://www.forensic.gov.uk/forensic\\_t/inside/news/docs/NDNAD.doc](http://www.forensic.gov.uk/forensic_t/inside/news/docs/NDNAD.doc)
- New Scientist (2005) **Will DNA Profiling Fuel Prejudice?**, New Scientist web sitesi, son eriřim tarihi: 11.08.2006, <http://www.newscientist.com/article.ns?id=mg18624944.900>
- Orwell, G. (1984) **Bin Dokuz Yüz Seksen Dört**, (çeviren: Nuran Akgören), İstanbul: Can Yayınları.

- Öktem, M. K. (2004) “Bilgi Teknolojileri ve Kamu Yönetimi”, U. Ömürganülşen ve M. K. Öktem (der.), **Kamu Yönetimi: Gelişimi ve Güncel Sorunları** içinde, Ankara: İmaj Yayınevi, 139-186.
- Öktem, M. K. ve M. D. Aydın (2005) “Bilgi Teknolojileri ve Türk Kamu Yönetiminde Dönüşüm”, **Hacettepe Üniversitesi İİBF Dergisi**, 23(2), 257-282.
- Privacy International (2004), **Republic of Turkey**, Uluslararası Mahremiyet Örgütü web sitesi, Türkiye Ülke Raporu, son erişim tarihi: 11.08.2006, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-83783](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-83783)
- Pease-Watkin, C. (2003) **Bentham’s Panopticon and Dumont’s Panoptique Bentham Project**, University College London, son erişim tarihi: 11.08.2006, <http://www.ucl.ac.uk/Bentham-Project/journal/cpwpnan.htm>
- Pincus, W. and D. Eggen (2006) “325,000 Names on Terrorism List: Rights Groups Say Database May Include Innocent People” **Washington Post**, Wednesday, February 15, son erişim tarihi: 11.08.2006, <[http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021402125\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021402125_pf.html)>
- Privacy Act (1974) **The Privacy Act of 1974**, ABD Mahremiyet Yasası (düzeltilmiş haliyle), son erişim tarihi: 11.08.2006, <http://www.cftc.gov/foia/foiprivacyact.htm>
- Richelson, J. T. and D. Ball (1985) **The Ties That Bind: Intelligence Cooperation between the UKUSA Countries**, London: Allen & Unwin.
- Risen, J. ve E. Lichtblau (2005) **Bush Lets U.S. Spy on Callers Without Courts**, New York Times web sitesi, 16.12.2005, son erişim tarihi: 11.08.2006, <http://www.nytimes.com/2005/12/16/politics/16program.html?ei=5090&en=e32072d786623ac1&ex=1292389200>
- Smith, M. E. (2006) “Let’s Make the DNA Identification Database as Inclusive as Possible”, **The Journal of Law, Medicine & Ethics**, 34 (2), 385-89.
- Stanley J. and B. Steinhardt (2003) **Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society**, American Civil Liberties Union’s (ACLU) Technology and Liberty Program, ACLU web sitesi, son erişim tarihi: 11.08.2006, [http://www.aclu.org/FilesPDFs/aclu\\_report\\_bigger\\_monster\\_weaker\\_chains.pdf](http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf)
- Steinhardt, B. (2003) **Technology and Liberty Program on Government Data Mining**, ABD Temsilciler Meclisi Yönetmelik Reform Komitesi Konuşması, son erişim tarihi: 11.08.2006, <http://www.aclu.org/safefree/general/17262leg20030520.html>

- Telekomünikasyon Kurumu (2006) **10 Ağustos 2006 tarihli Telekomünikasyon İletişim Başkanlığı toplantısı**, Telekomünikasyon Kurumu web sitesi, son erişim tarihi: 11.08.2006, [http://www.tk.gov.tr/Etkinlikler/Ulusal\\_Etkinlikler/basin-toplantilari/2006/basin\\_toplantisi\\_10.08.2006.htm](http://www.tk.gov.tr/Etkinlikler/Ulusal_Etkinlikler/basin-toplantilari/2006/basin_toplantisi_10.08.2006.htm)
- Toffler, A. (1989) **The Third Wave**, New York: Bantam Books.
- Toffler, A. ve H. Toffler (1996) **Yeni Bir Uygarlık Yaratmak: Üçüncü Dalganın Politikası**, (çeviren Zülfü Dicleli), İstanbul: İnkılap Kitabevi.
- Toffler, A. ve H. Toffler (1997) **Geleceği Yeniden Düşünmek: İş Yönetimi, Rekabet, Kontrol, Liderlik, Pazarlar ve Dünya**, Derleyen: R. Gibson, (çeviren: Sinem Gül), İstanbul: Sabah Kitapçılık.
- TÜBA-TÜBİTAK-TTGV (1995) **Enformatik Alanına Yönelik Bilim, Teknoloji ve Sanayi Politikaları Çalışma Grubu Raporu**, Ankara: TÜBİTAK, Mayıs.
- UNDPEPA-ASPA (2001) **Benchmarking e-Government: A Global Perspective**, Birleşmiş Milletler Kamu Ekonomisi ve Kamu Yönetimi Birimi (UNDPEPA) ve Amerikan Kamu Yönetimi Derneği (ASPA) ortak raporu.
- Urbaneye (2006) **On the Threshold to Urban Panopticon?** Urbaneye Projesi web sitesi, son erişim tarihi: 11.08.2006, <http://www.urbaneye.net/>
- USDOJ (2006) **Freedom of Information Act**, ABD Adalet Bakanlığı (United States Department of Justice/USDOJ) Bilgi Edinme Özgürlüğü yasası web sitesi, son erişim tarihi: 11.08.2006, <http://www.usdoj.gov/04foia/>
- Vocino, T. and J. Rabin (1981) **Contemporary Public Administration**, New York: Harcourt Brace Jovanovich.
- Whitaker, R. (2000) **The End of Privacy**, New York: The New Press, 2000.
- Wilhelm, A. G. (2000) **Democracy in the Digital Age: Challenges to Political Life in Cyberspace**, London: Routledge.
- Wong, B. (2002) **China's Internet ban extends to parts of Yahoo search engine**, Asian Observer web sitesi, son erişim tarihi: 11.08.2006, <<http://www.asiaobserver.com/China/China-story5.htm>>
- Zaman (2005) **Meclis Kulislerinde 'Telekulak' Paniği**, Zaman Gazetesi web sitesi, 21.12.2005 Çarşamba, son erişim tarihi: 11.08.2006, <http://www.zaman.com.tr/?hn=239718&bl=politika&trh=20051221>
- Zamyatin, Y. (1986) **Biz**, (çev. Füsün Tülek), İstanbul: Ayrıntı Yayınları.