Abant İzzet Baysal Üniversitesi
Sosyal Bilimler Enstitüsü Dergisi – Journal of Social Sciences
Cilt / Volume: 2009-1 Sayı / Issue: 18

E-DEVLET'TE KULLANILAN GÖZETİM VE KAYIT TEKNOLOJİLERİNİN MAHREMİYET ÜZERİNDE ETKİLERİ

Muhittin TATAROĞLU*

ÖZET

E-devlet süreci hemen tüm dünyada yaygınlık kazanmıştır ve kamu yönetimlerinin tüm boyutlarıyla değişmesine yol açmaktadır. E-devlet kavramının etkinlik ve verimlilik, zaman tasarrufu gibi ekonomik boyutlu faydalarının yanında, kamuoyunun düşüncelerini öğrenme, tüm vatandaşların kolayca ulaşabilmeleri, hizmet sunumunda eşitlik, şeffaflık ve hatta elektronik olarak oy kullanma gibi demokratik boyutları da vardır.

E-devlet süreci bir toplumu, tüm boyutlarıyla, (sosyal siyasi, ekonomik teknolojik, idari) dönüştürmektedir. Bu dönüşümün sonuçlarını ise özenli tahminler dışında kestirmek mümkün değildir. Demokrasinin gelişmesi açısından oldukça büyük fırsatlar sunan e-devlet süreci, kişi mahremiyeti bakımından çok önemli sakıncalar da doğurmaktadır. Mahremiyet ise devlet ve birey ilişkilerinde önemli bir sorun alanı karşımıza çıkmaktadır. Bilgi ve iletişim teknolojileri gibi muazzam güç kaynaklarının cazibesi karşısında devlet ve hükümetlerin kişi mahremiyetini korunması demokrasi açısından yaşamsal önem kazanmaktadır. Mahremiyet sorunları özel sektörde yaşanacağı gibi, devletin kişi mahremiyetine yönelik ihlalleri de önemli artış sergilemektedir. Çalışmada e-devlet sürecinin kişi mahremiyeti açısından yarattığı tehlikeler ve yarattığı olumsuz sonuçlar incelenmiştir.
Anahtar Sözcükler: Mahremiyet; e-devlet; bilgi iletişim teknolojileri; demokrasi.

ABSTRACT

E-government process widespreaded world-wide ranche, and usage of ict affect all dimension of public administrations. Along with the economical benefit of e-government concept, “efficiency and productivity; there are democratic aspects, like acquisition to public opinion, equity in service providing, transparency and even e-voting.

E-government transforms all aspects of a society. Predicting the results of this transformation is, impossible but only attentive estimating. In terms of development of democracy, e-government offers rather large opportunities. Bu on the other hand bring with important threats to privacy right. Privacy is actually an important issue, in the relationship between person and government. Against the temptation of huge power resources like information and communication technologies, it is critical that the government or state stay in the route which protect personel privacy, according

* Yrd. Doç. Dr.. Muğla Üniversitesi Kamu Yönetimi Bölümü

democracy. Privacy matters can be also seen in private sector, likewise in public sector. İn this paper examined privacy matters which caused by e-government process.
Keywords: Privacy right; e-government; information and communication technology; democracy**.**

1. GİRİŞ

E-devlet olgusu, kamu yönetiminin içine girilmekte olan bilgi çağının temel karakteristiklerinden biridir. Bilgi iletişim teknolojilerinin hızla gelişmesi ve kamu yönetiminde yaygınlaşması, kamusal hizmet sunumunda etkinlik, verimlilik, eşitlik gibi olumlu gelişmeler sağlamış; vatandaş katılımı, kamuoyundan haberdar olma ve şeffaflık gibi olumlu gelişmeler sağlamıştır. Tüm e-devlet kurumları sanal örgütlerdir ve sanal bir dünyada dijital olarak varlıklarını sürdürmektedirler. Bu sanal dünya internetten oluşmaktadır. İnternet teknolojisinin ilk gözlenen sakıncalarından biri de kişi mahremiyetinin tehlikeye girmesidir.

Sanal ortamın güvenlik boyutları, gerçek dünyadakinden tamamen farklıdır. Gerçek dünyada insanlık tarihi boyunca suç türleri ve bunlara karşı geliştirilen güvenlik tedbirlerini bilmek mümkündür. Ancak sanal dünyada ne gibi suç türlerinin potansiyel tehdit olarak var olduğu, bu suçların toplumsal ve kişisel tahribatlarının neler olacağını tam olarak şimdiden kestirmek mümkün değildir. Gözlemler sanal ortamda işlenen ilk suçların; hack, kredi kartı dolandırıcılığı, gizli çekim ve bilgisayarlara sızma gibi kişi mahremiyeti ve kişinin gizli bilgilerine zarar verme gibi suçlar olduğunu ortaya koymaktadır.

Kişi mahremiyeti, temel haklardan sayılması ve toplumsal yaşam ve demokrasi ilkeleri bakımından kritik bir önem taşıması bakımından, önemli bir ilgi alanıdır. Bu bakımdan bilgi iletişim teknolojilerinin yaygınlaşması ve e-devlet süreçlerinde mahremiyetin zarar görme derecesi daha yüksek ve etkili olmaktadır. Örneğin bir kişinin saklı olması gereken özel bilgilerinin bir başka kişi tarafından elde edilip, kulaktan kulağa yayılması ile ulaşabileceği kitle, mahalle veya semt ile sınırlı olacak ve zaman içinde unutulabilecek iken; bu mahrem bilgilerin internette yayınlanmasıyla tüm dünyada yaşayan insanlara açık olacak; bir resim, video veya ses görüntüsü veya yazı defalarca kopyalanacak ve teorik olarak sonsuza değin sanal dünyada varlığını sürdürecektir.

Kişi mahremiyetinin üçüncü kişiler tarafından ihlali ya da korunmasından daha önemli bir sorun, vatandaş devlet ilişkilerinde ortaya çıkmaktadır. Kamu hizmeti sunumunda vatandaş ile devlet arasındaki ilişki, eşitsizlik esasına dayalıdır. Sunulan hizmet ve ilişki biçimini devlet belirler ve şartlara vatandaş uymak durumundadır. E-devlet kurumlarında vatandaşların hizmet alması pek çok kişisel bilgiyi, sunmasıyla mümkündür. Vatandaşlık numarası, yaş eğitim banka hesabı vs gibi istenen bilgilerin herhangi birinin

eksik olması durumunda çoğu zaman erişim aşaması bile kesilir. Öte yandan kişisel bilgilerin çoğu MERNİS, ADNKS, TAKBİS gibi sistemlerde toplanır ve kullanılır. Klasik devlette fiziki arşivlerde ve kağıt üzerinde bulunan kişisel bilgiler; e-devlet sürecinde ağlarla birbirine bağlı devasa sistemlerde dijital ortamda saklanmaktadır. Bu kişisel bilgilerin güvenliği için önlemler alınsa da, teknolojinin doğası gereği, eskisiyle kıyaslanamayacak ölçüde kitlesel bilgi üçüncü kişilerin saldırılarına maruz kalabilmektedir.

Bireylerden devletin egemenlik gücüne dayanarak bireylerin rızası olmadan toplanan bilgilerin hem diğer bireyler hem de devlet tarafından istismar örnekleri çalışmada incelenmiştir. Yine e-devlet kurumlarında toplanan kişisel bilgilerin korunamaması, birey aleyhinde sonuçlar doğuracak şekilde istismar edilmesi ve ilgili kurumlar tarafından "bilgi saçılması" şeklinde yayınlanması tehlikesi, bireylerde yerleşik bir korku hissine neden olmakta; davranış ve duygu değişimlerine yol açabilmektedir.

Siyasi iktidarlar kendilerine güç sağlayacak veya güçlerini artıracak araçların cazibesi karşısında zaafiyet gösterebilirler. İktidarların kendilerine büyük güçler sağlayan araçlara karşı bu güç hırsı ya da zaafiyeti (temptation of power), demokratik rejimlerin aşınmasına yol açabilmektedir. Bilgi iletişim teknolojileri de izleme, gözetleme gibi bazı alanlarda iktidarları baştan çıkaran yetenekler sunmaktadır. Bu araçlar vasıtasıyla baskıcı, totaliter ve antidemokratik eğilimlere yönelmek olasıdır. Bu bakımdan e-devlet, sunduğu pek çok olumlu gelişmelerin yanında kişi mahremiyeti ve demokrasi açısından olumsuz pek çok kritik tehlikeyi bünyesinde barındırmaktadır.

Modern devlette egemenliğin meşruluğu vatandaşlarını korumak ve hukuku uygulaya dayanmaktadır. Devlet hukuku uygulamaz ve konumuz açısından önemli olan vatandaşını koruma görevini yerine getirmez ise egemenliğinin meşruiyeti aşınır. Ampirik bulgular henüz emekleme aşamasında olan e-devlet sürecinde kamu kurumlarında saklanan kişisel bilgilerin korunamadığı, istismara uğradığı veya dışarıya saçıldığı pek çok vaka olduğunu göstermektedir. Bu durum ise vatandaşların e-devlete olan güven duygularını aşındırmakta; davranışlarını ve ruh hallerini olumsuz yönde etkilemektedir.

2. YÖNTEM

Çalışmada ilgili temel kavramlara değinildikten sonra konu ile ilgili hukuki mevzuat ve mahremiyeti etkileyen bilgi teknolojilerinin kullanıldığı kurumlar incelenmiş; bunların işlevleri, eksiklikleri ve sakıncaları araştırılmıştır. E-devlet sürecinde teknoloji kullanımını detaylı olarak, hümanist değerler, demokrasi, yönetim bilimi ve siyaset psikolojisi ve olası olumsuzlukları açısından inceleyen ilgili literatürün ağırlıklı olarak bilim kurgu yazınlarından oluşması ilginç bir durum sunmaktadır Bilgi iletişim sistemlerinin ve sanal yazılımların en önemli karakteristiklerinden olan karmaşıklık, hiçbir zaman tam

bir güvenlik sunamaması ve sorumluluk sorunu, kişi mahremiyeti bakımından kritik sorun oluşturduğundan, örnek olay ve ampirik bulgularla etraflı bir şekilde ele alınmıştır. Kamu yönetiminde uygulanan gözetim ve arşivleme odaklı bilgi iletişim teknolojilerinin yarattığı mahremiyet sorunları incelenmiş ve son olarak çözüm önerileri geliştirilmeye çalışılmıştır.

I- Mahremiyet

İnternet ortamında ve elektronik uygulamalarla bireylerin yaptıkları her türlü eylem, bireylerin kişisel bilgileri haline kolayca dönüştürülebilir. Öte yandan bilgi iletişim teknolojilerine dayalı tüm uygulamalar kişisel verilerin elde edilmesinde sonsuz imkânlar sunmaktadır. Bireylerin kişisel bilgilerinin gizli kalması nerede ise imkânsızdır denebilir. İnternette gezinmek veya herhangi bir işlem yapmak, kredi kartı ile alışveriş yapmak, otoyollarda OGS veya KGS ile ödeme yapmak, cep telefonunu sadece taşıyor olmak bile bireyin mahremiyet alanına giren bilgilerin açığa çıkması ve izlenmesi anlamına gelmektedir. Öte yandan bilgi iletişim teknolojileri vasıtasıyla bireyle hizmet sunumu veya diğer amaçlarla iletişim kuran kamu veya özel sektör kuruluşları, çoğu zaman emredici şekilde bireylerin kimlik bilgileri başta olmak üzere kişisel bilgilerini beyan etmelerini şart olarak dayatan yazılımlar geliştirmektedirler

Bu gelişme, bireyin mahremiyet hakkını dramatik bir şekilde ihlal etmektedir. Kişi mahremiyeti olarak da anılan mahremiyet hakkı, temel insan hakları kapsamında anılır ve demokrasi açısından en önemli ilkelerden biridir. Bu bakımdan mahremiyet kavramının öneminin vurgulanması gereklidir.

Mahremiyet genel olarak kişilerin tek başlarına kalabildikleri, istedikleri gibi düşünüp davranabildikleri, başkalarıyla ne zaman, nerede, nasıl ve hangi ölçüde ilişki ve iletişim kuracaklarına kendilerinin karar verebildikleri bir alanı ve bu alan üzerinde sahip olunan hakkı ifade eder. (Yüksel, 2003: 182). Bireyin davranışlarının, kişilik bilgilerinin, özelliklerinin ve kişi ile ilgili olan her şeyden başkalarının ne kadar haberdar olacağı da kişisel mahremiyet ile ilgilidir.

Mahremiyetin farklı boyutlarından bahsetmek mümkündür. Gizlilik şeklinde mahremiyet; bireylerin kendileri hakkındaki bilgileri, belirli eylemlerini, herkese veya seçtiği bazı kişilere karşı gizli saklamayı istemesi şeklinde ortaya çıkar. Anonim mahremiyet; bireylerin bazı davranışları (toplum içerisinde yapılmış olsa dahi) bireyle ilişkilendirilemeyecek şekilde yapma isteğidir. Otonomi mahremiyeti ise, bireyin bazı davranışlarının aleni veya gizli kalması tercihinin kendine bağlı olması, devlet veya diğer kişilerin ilgisine kapalı kalmasını tercih etmesidir.

Devlete karşı mahremiyet hakkı, diğer kişilere karşı mahremiyet

hakkından iki önemli bakımdan ayrılır. İlki özel kişiler hırsızlık gibi diğerinin rızası olmadan başkasının mahremiyetine girse de, birbirleriyle olan ilişkileri genelde gönüllü ve iradi olur. Birey diğerine açıklayacağı kişisel bilgileri üzerinde kontrol sahibidir. Bunun yanında birey diğer kişilere karşı mahremiyetini koruyacak güce ve önlemlere sahip olacaktır. Ancak devlet oldukça çok geniş bir alanda zoraki eylemleri gerçekleştirebilir. İkinci fark ise devletin vatandaşlar üzerinde fiziksel güç uygulamaya dayanan bir egemenliğinin olmasıdır. Bireylerin üçüncü şahıslara karşı kendi mahremiyetini koruyacak bazı tedbirler alması mümkündür (kendisini diğer vatandaşlara karşı kendi koruyabilir kilit ve hırsız alarmları gibi tedbirler alabilir). Ancak birey kendini ve kişisel bilgilerini koruyabilmesi açısından çok güçsüzdür. Kişisel bilgilerini devletten koruyabilmek için tek başvurabileceği yol, gizlemeye çalışmaktır (Friedman, 2000:186). Bu farklılığın mahremiyet üzerindeki etkileri bakış açısına göre değişiklik sergiler. Eğer devletin iyi niyetli olduğu, vatandaşlarının iyiliğini istediği ve kamu yararını gözettiği düşünülüyorsa, o zaman kişisel mahremiyet kamu görevlilerinin iyi olanı yapmalarını zorlaştıracak demektir. Ancak öte yandan devlet vatandaşlar aleyhine davranışta bulunabilecek bir kurum olarak görülüyorsa, o durumda devlete karşı kişisel mahremiyet ve korunması kesinlikle iyi bir şeydir. Mahremiyetin, kişisel suçların saklanmasında kullanılabileceği kabul edilse de, mahremiyetin devlete karşı korunması gerektiği temelinde görüş oldukça geniş kabul görmektedir.

A- Mahremiyet ve Demokrasi

Ortaçağ toplumlarında insanlar toplumsal düzendeki rollerine zincirlenmiş durumdaydı. Toplumsal olarak bir sınıftan diğerine geçmek hatta bir köyden diğerine veya başka bir ülkeye gitme şansları pek yoktu. Bireyler diledikleri gibi giyinme ve istediklerini yeme özgürlüğüne dahi sahip değillerdi. Zanaatçının satacağı malın fiyatı, köylünün malını satacağı yer, belliydi ve bunların tümü kurallar ve yükümlülüklerle belirlenmişti (Fromm, 1995:48)

Özel hayat ile kamu hayatı arasındaki denge, 1800'lü yıllarda değişmiştir. Bu dönemde özel hayat, kamu hayatından daha üstün olmaya başlamış; kamu hayatı ise görevler alanı olarak ayrışmaya başlamıştır (Gürbilek, 2001:118) Modernleşme süreciyle birlikte, "birey", "bireycilik", bireysel kimlik" ve "bireysel alan" gibi değerler ortaya çıkmıştır. Ardından "özel yaşam hakkı", veya "mahremiyet hakkı" hukuk düzenince tanınan bir hak kategorisi haline gelmiştir (Yüksel, 2003 :197). Devletle ilişkisinde vatandaşlık statüsüne kavuşan bireyin, hukuk düzeni tarafından kendisine tanınan haklarla ve yüklenen ödevlerle kişi haline gelerek hukuki bir kimlik kazanması, Amerikan bağımsızlığı (Mills, 2008:6) ve Fransız ihtilaliyle başlayan süreçte gerçekleşmiştir.

Liberal düşüncede mahremiyet, bireyin içinde rahat bırakıldığı veya bırakılması gerektiği, istediği gibi düşünüp davranabildiği, kendi bildiği şekilde

bizzat kendi iyiliğinin peşinde koşabildiği bir alan olarak tanımlanır. (Lukes, 1995:66; nakleden, Yücel:2003:201). Liberal görüşte mahremiyet, kamusal yaşam içinde yer alan, ancak kamusal müdahalelerden muaf tutulması gereken bir düşünce, davranış ve varoluş alanını ifade eder. Bu açıdan bakıldığında mahremiyet, birey ve toplumsal gruplar ile devletin de dahil olduğu geniş kamu arasındaki negatif ilişkiyi ima eder. Liberalizm özerk ve özgür birey kavramına özel önem vermektedir.

Liberalizmde özerk ve özgür birey merkez noktadadır. Özel hayat alanı ve kişisel özerkliği hukuken korunan birey, kendi değerlerini gerçekleştirmek ve geliştirmek için diğer insanlarla ilişkiye girer. (Craven, 1982:353) Bireysel özgürlük devlet ve toplumsal çoğunluk tarafından da ihlal edilebilir. Devlet ve toplum bazı değer ve davranışları zorla bireye benimsetme yoluna gidebilir. Bu durumda demokrasinin kilit unsuru olan özgür irade ve bir özgür iradenin oluşabileceği mahrem alana devlet müdahalesinin bir sınırı olmalıdır. Toplumun bireye karşı zorlama ve denetim gücüne, hukuki veya kamuoyunun manevi baskılarının sınırlandırılması, özgür toplum için yaşamsal önemdedir. Başkalarına zarar vermek haricinde bir birey üzerinde onun arzusuna rağmen zorlama ve denetim uygulanmamalıdır.

Westin, mahremiyet hakkının bağımsız ve serbest iradeye sahip özgür bireylerden oluşan grupların işbirliklerine imkan sağladığını söylemektedir (Westin, 1967:24). Oy kullanmanın gizli olması ve seçim süreçlerinde iktidar gözetiminin engellenmesi, mahremiyet hakkıyla mümkün olur. Bu bakımdan mahremiyet hakkı, kişilerin gereksiz ve uygunsuz soruşturma ve incelemeye uğramasını da engeller. Teknoloji kullanımının kamu ve özel sektörde yaygınlaşmasının kişi mahremiyeti açısından önemli bir tehdit oluşturduğu açık bir gerçektir. Ancak mahremiyet hakkının demokratik bir toplum için yaşamsal önemde olduğu gereği kadar vurgulanmamıştır. Bireylerin mahremiyet alanı, kişisel iradelerin oluştuğu bölgelerdir ve sağlıklı ve özgür bir iradenin oluşabilmesi için birey bu alanda kendisine müdahale edilmeden iradesini geliştirme imkanı bulmalıdır. Birey, mahremiyet alanına sahip olamazsa veya değişik müdahalelere maruz kalırsa veya izlendiği korkusuna kapılırsa, serbest bir iradeden bahsetmek mümkün değildir. Demokratik toplumların temelleri, iktidarların denetlenmesinde kamusal ilginin var olmasına ve birey ve grup yaşamlarını koruyan mahremiyet hakkına dayalıdır.

B- Kamu Yönetiminde Kişisel Verilerin İzlenmesi, Toplanması ve İşlenmesine Yönelik Kurumsal ve Yasal Görünüm

Kamu yönetimi örgütleri vatandaşların kişisel verilerini izlemek, toplamak ve işlemek için gittikçe daha fazla bilgi ve iletişim teknolojileri kullanmaktadır. Türkiye'de kişisel bilgilerin, toplanması, işlenmesi ve yayınlanması ile ilgili bazı kurum ve teknoloji sistemleri şöyledir:

*** MOBESE:** Trafik akışının takibi ve düzenlenmesine yönelik olarak geliştirilmiş bu sistem, özellikle büyük kentlerin ana caddeleri ve meydanlarında başlamış; daha sonra diğer şehirlere, şehir giriş çıkışlarına ve kritik yol noktalarına yaygınlaştırılmıştır (Cilingir ve Kushchu, 2004: 2). Bu sistem, araçların plakalarını okuyabilmekte araç sahibi ile ilişki kurabilmektedir. Kişilerin özel hayatlarını da kayıt eden bu sistemin henüz yasal bir yapıya kavuşmaması, önemli bir eksikliktir. Başlangıç amacının yanında suçluların takibi ve tanımlanması, trafik suçlarının belirlenmesinde de kullanılmaya başlamıştır. Kuruluş amacından sapma gösterdiğine dair bir örnek, son günlerde gittikçe yaygınlaşan bir uygulama ile somut şekilde gözlenmektedir. Ekonomik sıkıntı nedeniyle artan icra ve haciz uygulamaları, araçlara yönelik haciz kararlarının bilgisayar sistemine girmesiyle, herhangi bir kontrol noktasında aracın plakasının okunmasıyla bilgisayar uyarı vermekte ve araç durdurularak el koyma işlemi gerçekleştirilmektedir.

*** TİB** (Telekomünikasyon İletişim Başkanlığı): 23.7.2005 tarihli 5397 sayılı kanunla telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına yönelik işlemleri tek bir merkezden yürütmek; interneti izleme ve kayıt etmek; amacıyla kurulmuştur. Kurumun oluşturulmasıyla güvenlik, istihbarat ve yargı kuruluşlarından gelen dinleme talepleri Telekomünikasyon iletişim Başkanlığı tarafından gerçekleştirilecektir. Telefon dinleme ve izleme faaliyetleri TİB tarafından yürütülecek; MİT, EGM ve Jandarma kuruluşlarından da birer temsilci kurumda görev alacaktır TİB başkanının, başbakan tarafından atanması öngörülmüştür. Faaliyetleri hakkında başbakanlığa bilgi vermekle yükümlüdür. Görev ve yetkileri 5271 sayılı Ceza Muhakemeleri Kanunu, 5237 sayılı Türk Ceza Kanunu, 2813 sayılı Telsiz Kanunu, 2559 Sayılı Polis Vazife ve Salahiyet Kanunu, 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Kanunu, 2803 sayılı Jandarma Teşkilat Görev ve Yetkileri Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, "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", "Ceza Muhakemesi Kanununda öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik"ten oluşan mevzuatla düzenlenmiştir.

İletişim araçlarının dinlenmesi ve izlenmesi Ceza Muhakemesi Kanunu, Anayasa gibi başka hukuk kurallarına da konu olmuştur. Ancak Telekomünikasyon İzleme Başkanlığı'nın yapı ve işleyişinde mahremiyet açısından bazı önemli sakıncalar vardır. Kurumun başbakanlığa bağlı olması hem denetleyen hem denetlenenin yürütme erkine bağlı olması anlamına

gelmektedir. Dinleme yetkisine sahip olan kurumlar; MİT, EGM ve Jandarma, yürütmenin bir parçası olan kurumlardır. Bu kurumların dinleme faaliyetlerini denetleyen TİB'in başkanını atama ve hesap sorma yetkisi başbakanlığa verilmiştir. Bu durumda denetleyenler ile denetlenenlerin aynı kurumda olması bağımsız ve tarafsız bir şekilde görev yapması bakımından sakıncalar yaratmaktadır.

Bu sakıncalı durum, Anayasa Mahkemesi tarafından alınan iptal kararıyla kısmen telafi edilmiştir. Anayasa Mahkemesi, başbakanın TİB başkanını atama yetkisini iptal etmiştir. Bununla birlikte 5397 tarihli kanunun yürürlüğe girdiği zaman ile (3.7.2005), iptal edildiği zamana değin (29 1.2009) arasında bu sakıncalı durum devam etmiştir. Öte yandan başbakan tarafından atanan kurum başkanı ise görevine devam etmektedir.

Hakkında yasal dinleme kararı alınanlarla birlikte onların iletişimde bulundukları kişilerin konuşmalarının da dinlenmesi; önemli bir mahremiyet sorunu olarak karşımıza çıkmaktadır. Bu kişinin dinlenmesine dair ne yetkili makamlar, ne de yargı kararı olmamasına rağmen dinlenmekte ve kayda alınmaktadır. Bu durumda konuştuğu kişi hakkında dinleme kararı olması, kendisinin de dinlenmesine yol açmaktadır ve hiçbir meşru karar olmadan mahremiyeti ihlal edilmektedir.

Bu tür kurumların, özellikle siyasi iktidarların nüfuzundan korunması gereklidir. Elektronik iletişimin izlenmesi ve kaydedilmesi faaliyetlerine gerçekleştiren kuruluşların denetiminin siyasi iktidarların etkisi altında kalabilecek kuruluşlar tarafından gerçekleştirilmesi, demokrasi açısından ve temel hakların devlete karşı korunması bakımlarından önemli zaafiyetler yaratacaktır.

Mahremiyet ihlali Ceza Kanununda suç olarak tanımlanmıştır. Hukuka aykırı olarak kişisel verileri kaydedenlerin cezalandırılması öngörülmüştür (TCK Md.135/1). Yine aynı kanunun 2. fıkrasında kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimseler cezalandırılır hükmü vardır. Bu suçlar şikayete bağlı suçlardır ve şikayet olmadan savcıların kendiliğinden harekete geçmesi söz konusu olmaz. Halbuki dinlenen kişiler kendilerinin dinlendiğinin farkında değildir ve bu yüzden de şikayetçi olmaları mümkün değildir. Bu durum ise hukuka aykırı dinleme yapanlara koruma sağlamakta ve teşvik edici olmaktadır. Dinlemelerin gizli olması ilgili kurumları keyfi yollara başvurma eğilimi göstermelerine yol açabilmektedir. Bu keyfiliklerin önlenmesini sağlayacak güvencelerin alınması gerekliliği ortaya çıkmaktadır.

Elektronik iletişimin dinlenmesi ve kayıt edilmesinin sakınca ve

istismarlarını önlemek için yapılan düzenlemelerde, dinleme izni kapsamı dışında kalan konuşma ve haberleşme bilgilerinin kayıt edilmemesi, kayıt edildiyse silinmesi,, kayıtlarda suç unsuru bulunmadığı durumlarda, kayıtların imhası ve dinlenen kişiye dinlendiğine dair bilgi verilmesi hükümleri yer alsa da, uygulamada bu tedbirlerin alınmadığı görülmektedir. Örneğin, dinlenen ve suç unsuru bulunmayan kişilere, yargı organları tarafından dinlenmesine karar verildiği ve dinlendiğinin bildirildiği bir örneğe henüz rastlanmamıştır.

*** MERNİS** (Nüfus kayıt sistemi), **ADNKS** (Adrese dayalı nüfus kayıt sistemi), **SEÇSİS** (Seçmen Bilgi sistemi) **SGBS** (Sosyal Güvenlik Bilgi Sistemi), **KPBS** (Kamu Personeli Bilgi Sistemi), **TAKBİS** (Tapu Kadastro Bilgi Sistemi) **İLSİS** (Milli Eğitim Müdürlükleri Yönetim Bilgi Sistemi) gibi kamusal hizmet bilgi istemleri.

Kamusal hizmetlerin sunulmasında ve düzenlenmesinde süreç içinde her hizmet birimi, daha sonra birbiriyle entegre edilmesi düşünülen ayrı ve bağımsız bilgi sistemleri oluşturmak ve hizmetlerini sanal ortamda sunmak amacıyla pek çok bilgi sistemi oluşturulmuştur. Bu bilgi sistemlerinde gözlenen genel sorunlar, değişik mahremiyet risklerini de barındırmaktadır. Öncelikle bu sistemler, "hack" denilen bilgisayar ve internet korsanlıklarına karşı güvenlik açısından zaafiyetler sergilemektedirler. Dışarıdan izinsiz saldırılarla kişisel bilgilerin kopyalanması veya değiştirilmesine dair örnek vakalar gözlenmektedir. 648.000 öğretmenin kimlik bilgilerinin kopyalanıp internet ortamında sergilenmesi, İLSİS uygulamasının güvenlik açığına sahip olduğunu göstermektedir (Hürriyet, 2009a)

MERNİS, Merkezi Nüfus İdare Bilgi Sisteminin adıdır. İçişleri bakanlığına bağlı Nüfus İdaresinin tüm işlemlerini gerçekleştirmek amacıyla proje edilmiştir (www.nvi.gov.tr). KPS (Kimlik Paylaşım Sistemi) ise MERNİS'de yer alan vatandaşlık bilgilerinin kamu kurumları tarafından paylaşımını sağlamak amacıyla oluşturulmuştur. Ancak uygulama aşamasında kimlik bilgilerinin dışarıya sızma olasılıkları, bir kişiye birden fazla vatandaşlık numarası verilmesi, hayali-sanal kişilikler ve kimlikler yaratma olanaklarının bulunduğu gibi şikayetler gözlenmiştir. 2004 yılında yapılan bir incelemede 77.756 kişiye aynı vatandaşlık numarasının verildiği tespit edilmiştir. Ayrıca sistemin, kurum personeli tarafından oluşturulan sanal kimliklere gerçek vatandaşlık numaraları vererek resmileştirebileceği gibi istismar olasılıkları tespit edilmiştir (Milliyet, 2006).

Seçmen Bilgi Sistemi (SEÇSİS), Seçmenlerin belirlenmesi, mükerrer yazımın önlenmesi, listelerin hazırlanması, seçmenin kolay, hızlı oy vermesi, seçimin çabuk sonuçlanması, siyasal hakların kullanımının kullanılmasının desteklenmesi, seçim süreci ve sonuçlarının internet üzerinden izlenmesi ve gerçekleştirilmesini amaçlayan bir bilgi sistemidir. Gelecekte elektronik seçimin

bu sistem üzerinden gerçekleştirilmesi düşünülmektedir. Seçmen aday olanların kısıtlılık ve adaylık hakkını engelleyen durumların belirlenmesi için İçişleri, Adli Sicil ve ASAL gibi kurumlarla bütünleştirilme aşaması henüz gerçekleştirilmemiştir. Ancak 2009 yerel seçimlerinin seçmen kütükleri ve seçmenlerin oy kullanacakları sandıkların sorgulanması ilk defa sistem sayesinde internet üzerinden mümkün olmuştur.

Ancak bu sistemin faaliyete başlaması pek çok sorunu ve aksaklığı ortaya koymuştur. SEÇSİS veritabanı, seçmenlerin sokağa çıkış yasağı konularak evlerde sayılmaları şeklindeki klasik seçmen sayımı yerine MERNİS ve ADNKS'den elde edilen verilerin işlenmesi ve düzenlenmesiyle oluşturulmuştur. Bu yöntem seçmen listelerinin sağlığıyla ilgili değişik sorunların ortaya çıkmasına sebep olmuştur. Seçmen listelerinde yıllar önce ölen vatandaşların dahi yer aldığı gözlenmiştir (Milliyet, 2008). 2009 mahalli seçimleri için askıya alınan ve Yüksek Seçim Kurulu'nun internet sitesinde yer alan verilere göre, bazı seçmenleri ikamet adresleri kaybolmuş, seçim sandıkları resmi ikametlerinin bulunduğu ilden başka illerde gösterilmiş ve bir dairede elliden fazla seçmen kayıtlı gösterilmiştir. Samsun'un, Çarşamba ilçesinin, Çınarlık beldesinin tüm seçmenleri seçmen listesinin dışında kalmıştır Ekip Gazetesi, 2008).

Bahsedilen bu sorunların çoğunluğunun, Seçmen Bilgi Sistemi'nin yeni oluşturuluyor olmasından ve veritabanı oluşturulmasında daha güvenilir yöntemler yerine MERNİS ve ADNKS verilerinin birleştirilip, işlenerek sağlanmasından kaynaklandığını söylemek mümkündür. Ancak uygulamadaki aksaklıklar sistemin güvenilirliği konusunda şüphe uyandırmaktadır. Esasen teorik olarak sanal programların mutlak güvenliğinden söz etmek mümkün değildir. Bu sistemde görülen aksaklıklar, hem seçimlerin meşruiyetinin sorgulanmasına yol açabilmektedir. Hem de seçmen- sandık sorgulama esnasında seçmenlerin kişisel bilgilerinin üçüncü kişiler tarafından elde edilmesi tehlikesini yol açmaktadır (Ketizmen ve Ülküderner, 2007:191-192).

Vatandaşlık numarası, özel ve kamu kurumlarıyla ilişkide en çok talep edilen kişisel bilgidir ve ulaşılması oldukça kolaydır. Bir kurumun internet sitesinin ilgili kısmına yazılan TC kimlik numarasıyla kişinin adı, soyadı, doğum tarihi gibi bilgilere erişmek mümkündür. Bu bilgilerle de o kişinin adres bilgilerini elde etmek mümkündür. Elde edilen bilgiler yoluyla zincirleme olarak vergi numarası, SGK numarası gibi bilgilere de ulaşmak mümkündür.

Sosyal Güvenlik Kurumunun www.sgk.gov.tr adresinden kişinin sosyal güvencesinin olup olmadığı, adı, soyadı, doğum tarihi, anne ve baba adı,kızlık soyadı, işe giriş tarihi, aldığı maaş ve zamlar, sigortalılık süresi, devamsızlığı, hangi işyerlerinde çalıştığı gibi bilgilere ulaşmak mümkündür

Kişinin anne ve baba adı ile birlikte bu verilerle Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün internet sitesinden aile sıra no, cilt no, birey sıra no, mahalle ve köy bilgilerine ulaşılabilmektedir. Yine TC numarasıyla ÖSYM'nin internet sitesinden kişinin lise diploma notu, ÖSS puanı, LES ve KPSS puanları, burs durumu, mezun olduğu okul ve bölümü öğrenmek mümkündür:

Vatandaşların kişisel bilgilerinin parça parça, değişik kurumların internet sitelerinden elde edilmesiyle bir kişi hakkında yüzlerce kişisel bilgiye ulaşmak mümkündür. Üçüncü kişilerin bu bilgileri, kredi kartı yolsuzlukları, sahte nüfuz cüzdanı çıkarmak, dolandırıcılık, sahte isimle şirket kurma gibi pek çok illegal işlerde kullanması mümkündür.

Burada bahsedilen olumsuz örnekler, bilgi teknolojileri öncesinde de karşılaşılan durumlardır. Ancak bilgi iletişim teknolojileri kullanımıyla daha önce görülmedik çapta ve etkide olumsuz sonuçlar yaratmaktadır. Örneğin geleneksel yolla bir kişi, bir kamu kurumunda saklanan kişisel bilgilerin ne kadarına ulaşabilir? Ancak, bilgi iletişim teknolojileri bir kişinin bir anda ve çok uzak coğrafyada iken yüz binlerce öğretmenin kişisel bilgilerini kopyalamasını, milyonlarca kredi kartı bilgilerini çalmasını mümkün kılmıştır.

1- Kişisel Verilerin Korunması Hakkında Kanun Tasarısı

Kamu yönetiminde bilgi iletişim teknolojilerinin mahremiyet hakkı açısından yarattığı sakıncaları önlemeye yönelik kapsamlı bir hukuki düzenleme henüz gerçekleşmemiştir. Mahremiyet hakkını korumaya yönelik olan hukuk normları ise 27.5.1948 tarihli Resmi Gazete ‘de yayınlanarak içselleştirilmiş BM İnsan Hakları Beyannamesinin 12. maddesi, 1982 Anayasasının 20, 21 ve 22. maddesi, CMUK'da bazı ek maddeler, Kolluk ve istihbarat güçlerinin yetki ve görev tanımlarını yapan kanunlarda yer alan maddeler, Basın Yayın Kuruluşları ile ilgili kanunlar içerisindeki bazı maddeler, TMK'nun 24. Maddesi, TCK 135. maddesi ve Türkiye'nin de taraf olduğu Avrupa İnsan Hakları Sözleşmesinin 8. maddesidir. Bilgi iletişim teknolojilerinin de gözetilip, kişisel bilgilerin korunmasına yönelik hem nispeten kesin tanımlar yapan, somut müeyyideler getiren, ilgili kamu kurumlarının idari düzenlemeleri yapmalarını içeren ve kişisel verileri korumaya yönelik yeni kurumsal yapılar öngören kapsamlı bir kanun tasarısı hazırlanmış olmakla birlikte henüz yasalaşmamıştır. Avrupa Konseyi'nin hazırladığı “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması”na dair 108 Sayılı Sözleşme'ye Türkiye imza atmış olsa da sözleşmenin onaylanmış sayılması için sözleşme ilkeleri doğrultusunda kabul edilmesi gereken yasa henüz çıkartılmamıştır.

Anayasa’nın 20.21.22. maddeleri kişi mahremiyetinin kişi ve malları üzerinde arama yapılması ve el konulması, konut dokunulmazlığı ve haberleşme hürriyeti ve gizliliği boyutlarını düzenlemiştir. İlgili maddeler kişi

mahremiyetini korumaya yönelik olmakla birlikte, anayasa tekniği gereği genel nitelikte düzenlenmiş ve Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve ahlakın korunması ve başkalarının hak ve özgürlüklerinin korunması gibi geniş ve muğlak olabilecek gerekçelerle kişi mahremiyetine kamunun müdahale edebilmesine imkan sağlamıştır. Bu hükümlerin tam bir koruma sağlayacağını söylemek mümkün değildir.

"Kişisel Verilerin Korunması Kanunu Tasarısı" 22.4.2008 tarihinde Meclis'e gönderilmiş; gün itibariyle Avrupa Birliği Uyum Komisyonu'ndan geçmiş ve Adalet Komisyonunda görüşülmektedir. Özellikle kamu kurumlarının bilgi iletişim teknolojileri kullanması sebebiyle ortaya çıkan mahremiyet sorunlarına vurgu yapması bakımından, bilgi çağında mahremiyet hakkının korunmasını hedef alan ilk kapsamlı kanuni düzenleme olarak tanımlamak mümkündür. Tasarının günümüze değin kanunlaşmamış olması, ve uzun bir süre sürüncemede kalması, kişi mahremiyetine gereken önemin verilmediğin göstergesi olarak değerlendirmek mümkündür

2- Mahremiyet Hakkına Tasarıyla Getirdiği Olumlu Etkiler

Tasarı metninin genel ve özel gerekçelerinde, teknoloji kullanımının yaygınlaşmasının yarattığı sorunların ve bu teknolojileri kullanan devlete karşı kişi mahremiyetinin korunması gerektiğine dair etraflıca vurgu yapılmıştır (Başbakanlık:2008:1)

Tasarının sunuş gerekçesinde kamusal mal ve hizmetlerin üretimi ve sunumunda etkinlik ve verimliliğin sağlanması amacıyla kişisel veri sicillerinin oluşturulmasının gerekliliği vurgulanmış, ancak bu tür sicillerin kullanılmasının mahremiyeti gözeten düzen ve ilkelere bağlanması gerektiğine dikkat çekilmiştir. Kişisel verilerin sınırsız ve gelişigüzel toplanması, denetimsiz olarak açıklanması, yetkisiz kişilerin eline geçmesi halinde kişilik hakları ihlallerinin ortaya çıkabileceği, bu sakıncaların giderilmesi ve faaliyetlerin denetim altına alınması gerektiği belirtilmiştir.

Tasarının genel gerekçesinde OECD'nin 1980 yılında kişisel verilerin korunmasına yönelik belirlediği rehber ilkelere atıfta bulunulmuş; tasarının hazırlanmasında referans olan ilkeleri şöyle sıralamıştır: 1- Kişisel veri toplanması ve işlenmesinin sınırlı olması ve ilkelere bağlılığı, 2-Kişisel verilerin belirli kalite standartlarında olması, 3-Kişisel verilerin toplanması ve işlenmesinde amaçların belirli olması ve kullanımının da bu amaçlarla sınırlı olması, 4-Kanunun yetki verdiği durumlar ve kişinin rızası hariç, amaçlar dışında kullanılmaması, 5- Kişisel verilerin korunması için gereken tedbirlerin alınması, 6- Kişisel verilerle ilgili yürütülen politika, uygulamalar ve gelişmeler hakkında açıklık politikasının izlenmesi, kişilerin kendisi hakkındaki verilere ulaşabilmesi, ulaşamayacağı durumlarda ise sebeplerini öğrenme, itiraz edebilme, verileri sildirebilme, düzelttirebilme tamamlama ve değiştirme

hakkının sağlanması ve 8- Kişisel verileri kullananların sorumlu tutulabilmesi. Tasarı ayrıca Avrupa Konseyinin kişi mahremiyetinin korunmasına yönelik pek çok sektöre yönelik Bakanlar Konseyi kararlarına da atıfta bulunmuştur.

Tasarı, özel yaşamın gizliliğini sağlamaya yönelik olarak düzenlenmesiyle mahremiyetin korunması açısından önemli gelişmeler sağlamaktadır. Tasarı, yasaya aykırı fişleme yapan kamu görevlilerine hapis ve para cezası öngörmektedir. Kişilerin din, dil, ırk, siyasi düşünce ve özel yaşamlarıyla ilgili dosya oluşturulması yasaklanırken; bu hükmü ihlal eden güvenlik görevlilerine para ve hapis cezaları öngörmektedir.

Haklarında dosya oluşturulan bireyler, istedikleri takdirde bu dosyaları inceleyip yanlışlıkların düzeltilmesini isteyebileceklerdir. Vatandaşların bilgi edinme hakkı "ulusal güvenlik" gerekçesi dışında engellenmeyecektir Kişilerin bilgi edinme taleplerini yerine getirmeyen, dosyalardaki verileri yasalara aykırı şekilde üçüncü kişilere aktaran kamu görevlileri hakkında dava açılacaktır.

Tasarı, özel hayatın gizliliğini korumaya yönelik olarak "Kişisel Verileri Koruma Kurulu"nun oluşturulmasını içermektedir. Bu kurul Kişisel verilerin uygun koşullarda tutulup tutulmadığını denetlemek, kişilik hakları ihlal şikâyetlerini soruşturacaktır. Sorumlular hakkında savcılığa suç duyurusu ve doğrudan para cezası verme gibi yetkilere sahip olacaktır.

3- Tasarının Olumsuz Yönleri

Kanun tasarısı, tüm vatandaşların tüm özel bilgilerinin ortak bir havuzda toplanmasını ve istisnai hükümlerle de olsa verilere ulaşımın kolaylaşmasını sağlamaktadır. Geleneksel uygulamada her bir kamu kurumu kendi gereksinimi olan kişisel bilgilerin sadece belirli kısmını toplamaktaydı ve bu bilgiler, ilgili kamu kurumu ölçeğinde bağımsız ve birbiri ile ilişkisiz sistemler içerinde kalmaktaydı. Tasarının öngördüğü ortak havuzda tüm vatandaşların tüm kişisel verilerinin toplanması değişik sakıncalar yaratacaktır. Örneğin havuza girebilen art niyetli, bir kimse hedeflediği her bireyin tüm özel bilgilerine ulaşabilecektir. Bu durum, sistemin siyasi iktidarlar tarafından istismar edilmesi ihtimali düşünüldüğünde daha vahim endişeler yaratmaktadır. Halbuki eski sistemde her bir kamu kurumu vatandaşların sadece kendilerini ilgilendiren kişisel bilgi parçalarını topladıkları için herhangi bir kurumda kişisel bilgilerin dışarı sızması veya istenmeyen kişilerin eline geçmesinin olumsuz etkileri de sınırlı kalmaktaydı. Bu durumda kişisel verilerin korunması yerine ortak bir havuzda toplanarak, erişimin kolaylaştırılmasından ve istismar girişimlerinin daha büyük zarara yol açmasından bahsetmek mümkündür

Tasarıda "kişisel veri" kavramı, kimliği belirlenebilir bütün bilgiler olarak tanımlanmakla, ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, dernek, vakıf, sendika üyeliği, sağlık ve özel hayatla ilgili verilerin

işlenmesine, kanunun öngördüğü zorunluluk, kamu yararı veya resmi olarak verilmiş bir görevin yerine getirilmesi gibi belirsiz ve net olmayan istisnailiklerle kayıt altında işlenmesine imkan sağlamaktadır. Bu istisnalar net olarak tanımlanmadığından her düzeyde kamu görevlisinin kayıt altında işlenmesi yasak olan kişisel verileri öğrenmesi mümkün olabilecektir.

Tasarıda "Kişisel Verileri Koruma Kurulu" üyelerinin hükümet tarafından atanması da bir diğer sakıncalı durumu oluşturmaktadır. Kurul üyeliklerinde uzman olma şartı aranmamış ve yetkiler tam olarak belirtilmemiştir. Kurul üyelerinin hükümet tarafından atanması, kurulun bağımsız bir denetleme görevi yapmasının önünde en önemli engel olarak görünmektedir. Kurumun hem bağımsız olarak işlemesi, hem de kurul üyelerinin bakanlar kurulu tarafından seçilmesinin öngörülmesi çelişik bir durumdur. Kurumun bağımsız bir idari otorite olarak çalışacağının ifade edilmesi, seçimi, yapılanması, yetkilerinin belirlenmesi ve bağımsızlığı gibi konularda kurulun kendisinin yetkili olmasını gerektirmektedir. Kurulun siyasi otoriteye bağlı olması, yetkilerini bağımsız bir şekilde kullanabilmesinde önemli bir engeldir.

Tasarıda oldukça geniş istisna durumları sayılmıştır. Ulusal güvenlik ve savunma, kamu düzeni ve güvenliği, suçun işlenmesinin veya devamının önlenmesi, suçların ve meslek ahlakı kurallarını ihlal eden eylemlerin kovuşturulması, devletin para bütçe, vergi ve istihdam konuları gibi önemli ekonomik veya mali menfaatlerinin gerektirmesi, ilgili kişi veya başkalarının hak ve özgürlüklerinin korunması gibi hallerde istisnalar öngörülmüştür. Kişisel verilerin korunmasında yer verilen istisnaların kapsam genişliği de bir başka olumsuzluk olarak görünmektedir. Bu istisnaların hak ihlallerine zemin hazırlama riski taşıdığını söylemek mümkündür. Kişisel verilerin üçüncü kişilere aktarılması kıstasları içinde, kişisel verilerin aktarılmasını isteyen gerçek ve tüzel kişiler için belli bir olayda ve kanundan doğan bir görevin yerine getirilmesi amacıyla kişisel verilerin aktarılması uygun görülmektedir. Ancak bu aktarımların genel tanımlarla veya kanundan doğan görevin yerine getirilmesi gibi, muğlâk ifadelerle açıklanması, mahremiyet ihlallerine açık kapı bırakmaktadır. Kişisel verilerin ancak özel amaçlarla kullanılması söz konusu olmalıdır. Verilerin amaca aykırı olarak açıklanması engellenmelidir. Taslakta demokratik toplum düzeni ilkelerine aykırı olarak veri açıklamasını mümkün kılan muğlâk ifadeler yer almıştır. "Kişilerin din, dil, ırk, siyasi düşünce, felsefi inanç, din mezhep ve diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık sorunları ve özel yaşamları ile her türlü mahkûmiyetleri kişisel veri olarak işlenemez" ilkesi yer alsa da, bu ilkeyi oldukça esneten istisnalar, bu ilkeleri aşındırmaya oldukça elverişli bir ifade biçimiyle anlatılmıştır.

II- Gözetim ve Kayıt Teknolojilerinin Kullanımından Kaynaklanan Mahremiyet Sorunları

Kamu yönetiminde bilgi iletişim teknolojilerinin kullanılmasından kaynaklanan pek çok sorun vardır. Örneğin sanayi çağında ortaya çıkan bireyin yabancılaşması sorunu (Ofluoğlu ve Büyükyılmaz,2008:114) günümüzde vatandaşların ilişkide bulunduğu kamu kurumlarının insansızlaşması, fiziki görünümden çıkıp, sanal varlıklara dönüşmesi, sofistike karmaşıklıkta yazılım programlarından oluşması sürecinde daha da büyümüş olarak karşımıza çıkmaktadır. Ancak kamu yönetiminin kişilerin özel hayatlarının en ince detaylarına ulaşabilecek güce ulaşması, sadece vatandaşlar açısından değil; iktidarın niteliği ve demokrasi açısından da sorunlar yaratmaktadır. İktidarların elleri altında güçlerini çok arttıracak bu teknoloji ve cihazlara sahip olmaları, iktidar hırsını, gücün baştan çıkartıcılığını daha da kışkırtabilir.

A- Gücün Baştan Çıkarıcılığı ve BİT'nin Sağladığı Güç

Kamusal gücün kullanılması bireylerin algılarını, inançlarını ahlaki değerlendirmelerini değiştirme ve makamın yükümlülüklerine ihanet etme eğilimine sokar. İktidar gücünün bu başlatan çıkarıcılığı, iktidarın gücünü daha da arttırabilecek cihazlara sahip olmasıyla daha da artar. Günümüzde bilgi iletişim teknolojileri iktidarlara, toplum üyelerini izlemek, kişisel bilgilerini en ince detaylarına kadar öğrenebilmek, bunları saklamak ve en geniş ölçeklerde de olsa işlemek gücünü sağlamaktadır. İktidarların güçlerini artıracak, ve otoriter rejime doğru evrilmelerine yol açacak bu teknolojilerin cazibesine karşı direnme güçleri gittikçe azalmaktadır.

19. yüzyılda Alman bürokrasi, Fransa, Amerika gibi gelişmiş ülkelerden daha güçlü ve gelişmiş durumdaydı.(Encyclopedia Britannica, 2004). Modern Weberyen bürokrasi, geleneksel bürokrasilere göre üstünlük sergiler. Bu üstünlüğü, emir komuta hiyerarşisi, yazılı kurallara dayalı olmak ve gayrı-şahsilik gibi örgütsel teknik özelliklerinden kaynaklanır. Modern bürokrasinin üstünlüğü, makine ile yapılan üretimin el ile yapılan üretime üstünlüğüyle kıyaslanabilir. Bu yönüyle gelişmiş bir bürokrasi siyasi iktidarların gücünü muazzam arttıran bir makine veya cihaz işlevi görebilir (Eryılmaz, 2008:37). Nazi Almanya'sında gerçekleşen insani dramın bir gerekçesini de gücün baştan çıkarıcılığı ile açıklamak mümkündür. Elinde gelişmiş ve güçlü bir bürokrasi bulan iktidarın bu gücün baştan çıkarıcılığına kapılması ve bürokrasinin kötücül amaçlarla kullanılmasını da içeren uğursuz düşünce ve ideolojilere meyil göstermesi mümkündür. (Arendt, 2003:40)

Kamusal gücün kullanımı da esasında başlı başına baştan çıkarıcı bir özelliğe sahiptir. İktidar gücünün kullanılması, bireyin algılarını, ahlaki değerlerini inançlarını ve davranışlarını bulunduğu makamın yükümlülüklerine ve sorumluluklarına ihanet eğilimini güçlendirir. Bu sorun insan doğasından kaynaklamaktadır. (Dobel, 1999: 24)

Gücün baştan çıkarıcılığı, özgürlükçü ve demokratik değerleri,

yükümlülükleri ve yetenekleri aşındıran güç sahibi olmanın psikolojik deneyimlerinden kaynaklanır. Bu çevresel deneyimler, uyumsuzluk stres, hayal kırıklığı ve kızgınlık, itaat ve üstünlük, gayrı-şahsileşme ve grup etkisini kapsar. Kamusal yararı sağlamakla yükümlü olan siyasiler pek çok dirençle karşılaşırlar. Bazı toplum kesimleri hedefleri sorgular veya muhalefet eder. Demokratik ve liberal sistemler, bu tür çatışmalara imkân sağlar ve esasında demokratik bir sistem, ancak muhalefetin varlığıyla mümkün olabilir. Demokratik sistemlerde çıkar çatışmalarının meşru yollarla yapılması ve uzlaştırılması özendirilir. Ancak bu tür engeller karşısında iktidar gücüne sahip olanlar kendi beklentilerini gerçekleştiremediklerinde hayal kırıklığına uğrarlar. Engellenme hissine dayalı hayal kırıklıkları, özellikle siyasi yöneticiler saldırıların art niyetli yapıldığını veya dürüstlüklerinin sorgulandığını düşündüklerinde, büyük öfkelere yol açar. Bireylerin özgüvenlerinde olumsuz etkiler yaratan bu gerilimler, kendini beğenme, aşırı önemseme gibi tepkisel-duygusal hezeyanları arttırır (Dobel, 1999:29).

Liderlerin sahip oldukları gücü kaybetmeme veya devam ettirme ve amaçlarını gerçekleştirme istekleri, demokratik ve liberal değerleri ihlal etmelerine yol açabilir. Lider, kendisi, başkaları ve kamu kurumlarıyla olan ilişkilerinde ahlaki değişiklikler göstermeye başlar (Kakabadse vd,2004:204). İktidarın kullanımında en önemli ahlaki sorun kişinin kendini aşırı önemsemesi ve yüceltmesidir. Kendini aşırı önemsemenin sonucu olarak lider, kanunları, kurumları ve kamusal bütçeleri kendi malı mülkü, toplumu da kendi tebası olarak görebilir.

İktidar gücü liderin kibir duygusuna kapılmasına yol açabilir. Seçim kazanmak ve başkalarına hükmetmek, başkalarına üstün gelmenin bencilliğine ve tatmin duygusuna sebep olabilir. Gücün, bireyin ahlaki değerlerini değiştirmesi sağduyulu kararlar almak ve yargıda bulunmak açısından önemli sorunlar yaratabilir. Kendi kendini yüceltme, keyfi davranma eğilimi, ahlaki ayrıcalık talebi, maddi çıkar gütme ve adil yargı yeteneklerinde bozulmalara yol açar.

Muhalefet, demokratik sistemler için yaşamsal önemde bir unsurdur. Taraflar, birbirlerine karşı kıyasıya kampanyalar yapabilirler. Ancak seçimler sonuçlandığında kaybeden kazananın gücünün meşruluğunu kabul eder. Öte yandan muhalefet ekalanların misilleme veya kin gütmeye maruz kalmayacağından da emin olması gerekir. Muhalefet, çıkar mücadelelerinde şiddet yöntemlerine başvurulmaması ve toplumun farklı düşünce ve alternatiflerin serbestçe hazırlanıp örgütlenerek mücadele edeceğinden emin olması bakımından önemlidir. Ancak biriken hayal kırıklıkları, muhalefetin "düşman" olarak algılanmasına da yol açabilir. "Şeytani düşmanlar" veya "tehlikeli ötekiler" anlayışı liderlerin ahlaki ve duygusal dünyasının sığlaşmasına yol açar.

İktidar gücü, İktidarda bulunanların muhalifleri düşmana, danışmanlarını da dalkavukluk seviyesine indirgemesine yol açabilir. Bu durum, gizlilik eğilimlerini arttırır. Muhaliflerin düşman olarak görülmeye başlanması, kişisel özgürlükleri, demokratik ve özgürlükçü değerleri tahrip edebilecek eylemlerin meşrulaşmasına yol açar. Liderler, eylemlerinin insani sonuçlarına karşı daha duyarsız olabilir. Nazi Almanya'sında iktidarın elinde muktedir ve güçlü bir bürokrasi cihazının olması, "nihai çözüm"e giden politika belirleme süreçlerinde teşvik edici bir etken olmuştur (Sherrer, 2000:249-250).

E-devlet, kamu yönetimi süreçlerinde ve kurumlarında bilgi iletişim teknolojilerinin yaygın şekilde kullanılması süreci olarak da tanımlanmaktadır. Bilgi iletişim teknolojileri, e-bürokrasi gibi örgütler, Weberyen bürokrasi cihazından çok daha büyük güçleri vaat etmektedir (Perri;2001:220)). Bilgi iletişim teknolojilerinin sağladığı muazzam ve eşsiz gücü elinde hisseden iktidarların bu gücün baştan çıkartıcılığına temayül etmeleri tehlikesi, ihmal edilemeyecek bir risk oluşturmaktadır. Kamu yönetiminde bilgi iletişim teknolojilerinin kullanılması ilk olarak kişi mahremiyetini ve mülkiyet hakkını ihlal eder görünmektedir.

B- Panoptikon ve Big Brother: Özgürlükçü Demokrasiden; Gözetim Toplumuna

Bilgi iletişim teknolojilerinin kişi mahremiyeti ve özgürlüğüne yönelik tehlikeleri ve liberal demokrasiler açısından taşıdıkları riskler, en iyi, bilim kurgu romanlarında tasavvur edilmiştir. Teknolojinin insan özgürlüğüne ve mahremiyetine yönelik zararları; henüz bilgi çağının başlarında olmamız ve ampirik çalışmalarla aşırı karmaşıklık sergileyen teknolojilerin toplumsal ve bireysel etkilerini belirlemenin zorluğu sebebiyle tespit etmek oldukça güçtür. Keza günümüzde kullanılan gerçek teknolojiler dünün bilim kurgu ürünlerdir.

Jeremy Bentham, 1791 yılında Panoptikon adlı bir hapishane planı yayınlamıştır. Bu hapishane, merkezinde bir denetleme mekânı, çevresinde de hücrelerin dizili olduğu yarım ay şeklinde bir yapıdır (bkz: Bentham, Pease-Watkin ve Werret, 2008). Tek tek hücrelerde kalan mahkûmlar, gardiyanlar tarafından gözlenebiliyorlardı. Ancak, kendilerinin gardiyanları görmeleri optik düzenleme sayesinde mümkün değildi. Mahkûmların saklanacak bir alanları yoktu ve izlenip izlenmediklerini bilmeyen mahkûmlar; her zaman için izlendiklerini varsaymak durumundaydılar. Böyle bir ortamda süreç içinde bireylerin özgüvenleri aşınmaya başlar, kişiliklerinin değeri azalır. Her an izlendikleri varsayımıyla mahkûmlar uysallaşarak teslimiyetçi bir şekilde her zaman kendilerinden istenen davranışta bulunmak zorunda kalırlar.

Bilgi iletişim teknolojilerinin kamu yönetimleri tarafından kullanımı, iktidarların gücünü muazzam arttıran güç cihazları işlevi görmektedir (Akın,

2009). İktidarın elinde kendisini her an izleyebilecek teknolojiler olduğunu bilen bireyler, mahremiyetlerinin kalmadığı hissine kapılırlar ve süreç içinde muhalif anlama gelecek davranışlardan ve düşüncelerden kaçınmalarına yol açacak bir oto-sansür uygulamasına girerler. Demokratik bir rejimde siyasi iktidarın elindeki teknolojileri vatandaşları izlemek için kullanması, vatandaşları birer Panoptikon mahkûmuna dönüştürebilir. Devamlı izlendiklerinin bilincinde olan bireylerde mahremiyet duygusunda kayıp hissi, stres, belirsizlikte artış, bireylerin birbirleriyle iletişiminde azalma, yöneten ve yönetilen arasındaki ilişkilerin bozulması gibi olumsuzluklara rastlanmaktadır (Botan, 1996) İşletmelerde yapılan bir başka araştırmaya göre ise izlemenin çalışanlar üzerindeki olumsuz etkileri, moral azalması, iş kotalarının devamlı artışı, verilerin cezalandırma amaçlı kullanılması, stres ve stres kökenli hastalıklar şeklinde gözlenmiştir (Yılmaz, 2005:12).

Orwell'in "1984" adlı eserinde kitle iletişim teknolojileri ile totaliter bir yapı oluşturularak toplumun kontrol edilmesini anlatmıştır (Orwell; 1999). Devletin her şeyi denetim altında tuttuğu, en küçük bir aykırılığa ve bireyselliğe izin vermediği, resmi ideolojinin bütün tarih ve dili kendine göre kurguladığı bir toplum ütopyasından bahseder. Romanda, insanları sürekli gözetleyip baskı ve denetim altında tutan "Ağabey" adında bir merkezi güç bulunmaktadır. Romanda sürekli denetimin sağlanmasında aracı olan "tele ekran" adlı bir teknoloji de bulunmaktadır. Bu toplumda düşünmek bile suç olabilmektedir. "Düşünce polisi", suç oluşturacak şeyler düşünenleri tespit edip tutuklamaktadır.

Bilgi iletişim teknolojileri günümüzde iktidarlara bir tür "düşünce polisi" oluşturma imkanı da sağlamaktadır. Kişilerin internette hangi siteleri ziyaret ettikleri, hangi gazeteleri okudukları, kredi kartlarıyla hangi kitapları aldıkları gibi verilerden siyasal eğilimleri belirlemeye dair kişilik profilleri çizmek mümkündür. Bu şekilde bireyin sadece internetteki davranışlarından siyasi eğilimini bilmek söz konusu olacaktır. Bireylerin bilgi iletişim teknolojileri ile izlenmeleri, siber-uzayda yaptıkları her türlü eylemin dijital olarak kayıt edilmesi, bu verilerin analiz edilip tasnif edilebilmesi, onları "veritabanı vatandaşları" haline dönüştürebilmektedir. Veritabanı vatandaşlarının bütün kişisel özellikleri bu kişisel verilerin işlenmesiyle tespit edilebilir. 11 Eylül'ün hemen ardından havaalanındayken ailesiyle telefon konuşmasında El Kaide şakası yapan bir vatandaşın, "Echelon" sisteminde yer alan kilit kelimeler takibine takılması ve nihayetinde terör şüphelisi olarak değerlendirilip gözaltına alınması bu duruma örnektir (Laidler, 2008:2).

"Echelon" ve benzer teknolojiler, günümüzde Orwell'in düşünce polisi işlevini görmektedir. Oldukça geniş bir yazılım sistemi olan "Echelon", tüm dünyadaki elektronik iletişim bilgilerini dinlemekte, yazılımda yer alan anahtar kelimeler vasıtasıyla kişileri potansiyel suçlu veya şüpheli olarak

tanımlayabilmektedir (European Parliament:1999:ii).Bu teknolojinin hemen tüm ülkeler tarafından elde edilmesi veya geliştirlmesinin önünde hiçbir engel yoktur.

İktidarlar bu teknolojileri kullanmasalar dahi kullanılabileceği olasılığının bireyler tarafından bilinmesi, davranış ve düşüncelerinde etkiler yaratacaktır (Laidler, 2008: 207). Bu bakımdan "saklayacak bir şeyi olmayanların izlenmekten korkmaması gerektiği söylemi, dünyada iktidar partileri arasında oldukça yaygın bir söylemdir (Solove, 2007:745). Laidler'in anlattığı örnek, saklayacak bir şeyi olmayan bireyin, tamamen masum olsa da, kamunun elinde bulunan kişisel bilgileri nedeniyle başına pek çok akıbet gelebileceğini ve korkması gerektiğini vurgulamaktadır.

Öte yandan iktidarlar da meşru veya hukuk dışı şekilde izlemenin var olduğunun kamuoyu tarafından bilinmesinden rahatsız olmayabilirler. Aksine bundan gizli bir hoşnutsuzluk duyarlar. Panoptikon'da önemli olan mahkûmların her zaman izlendiklerini bilmesidir. İzlenmese dahi her zaman izlenebileceğini düşünen birey, kendi kendine bir oto kontrol mekanizması geliştirir ve kendini denetlemeye başlar. Tabii ki, referans alacağı değerler, kendisini izleyenlerin veya iktidarın tercihleri, ideolojileri; duymaktan ve görmekten memnunluk duyacağı söz ve davranışlardır.

Türkiye'de durum daha da kritik bir görünüm sunmaktadır. Gelişmiş ülkelerdeki gibi iktidar mücadelesi, sistemin temel ilkeleri ve özellikleri üzerinde uzlaşmış tarafların daha iyi program, daha iyi icraat rekabeti üzerinde yürümez. Rejimin temelleri üzerindeki uzlaşmanın henüz sağlam biçimde oluşturulamaması; ayrıca iktidar talebinde bulunan tarafların bireylerin yaşam biçimlerini dahi söylem konusu yapması veya tarafların özel yaşam biçimlerine müdahale edileceği endişesi, bu kritik boyutu oluşturmaktadır.

C- E-devlet Bilgi Sistemlerinin Bilgi Sızdırması ve Açıklar Yoluyla Kişisel Bilgilerin Elde Edilmesi

Kamu kurumlarının hizmetlerini bilgi sistemleri yoluyla internet üzerinden sunmaları, sistemlerin tasarım, güvenlik ve işleyiş yapılarından kaynaklanan zaaflar yüzünden kişisel bilgilerinin saçılması, çalınması, ve üçüncü kişilerin erişimine açık olması sorunlarını doğurmaktadır. Vatandaşların kişisel bilgilerinin bazılarının elde edilmesi, kamu kurumlarının internet siteleri, vasıtasıyla diğer kişisel bilgilerinin elde edilmesinde kullanılabilmektedir.

Bu sorun ile ilgili en çarpıcı örnek, Konut Edindirme Yardımı geri ödeme listelerinin internet üzerinden yayınlanması ve yarattığı olumsuz sonuçlardır. Yıllardır bekleyen konut edindirme yardımı kesintilerinin hak sahiplerine iade edilmesinde ilgili makamlar kolaylık olması için ödemeye hak kazanan kişileri ve alacakları miktarları internet üzerinde yayınlamayı düşünmüştür. Bu doğrultuda bir internet listesi hizmete konulmuş (

(www.keyodemeleri.com) Bu şekilde kimin ne kadar ödeme alacağını zahmetsizce öğrenmesi hedeflenmiştir. Aslında oldukça yararlı olan e-devlet uygulaması, kastedilmemesine rağmen kişisel bilgilerin saçılmasına sebep olmuştur. Bu şekilde vatandaşların kimlik numaralarını elde eden bazı art niyetli kişiler sahte belge ve reçete düzenleyerek, SGK'yı yüz binlerce lira dolandırmışlardır. Benzer şekilde kimlik numaralarının bazıları 27 Temmuz 2008 tarihli resmi gazetede de yayınlanmış ve buradan elde edilen kimlik numaraları vasıtasıyla SGK numaralarına ulaşılmış ve buradan sahte reçetelerle ilaç yazdırılıp eczanelerden alınma yoluyla yolsuzluk gerçekleştirilmiştir. Burada, sisteme kasıtlı olarak girilmese dahi, sistemin bu bilgilere ulaşılması bakımından zaafiyet göstermesi ve kişisel bilgileri saçması söz konusudur (Hürriyet, 2009b).

Öte yandan pek çok kamu kurumu internet sitelerinde kendi personeli hakkındaki kişisel bilgileri detaylı olarak yayınlamaktadır. Özellikle özgeçmiş bilgilerinin internet ortamında yayınlanması konusunun özenli bir şekilde düşünülmesi gerekmektedir. Mesleğe liyakat anlamında eğitim ve, beceri ve tecrübeler bakımından önemli olan özgeçmişlerin kişisel nitelikteki bilgilerin yer alması değişik riskler yaratabilir.

D- Mahremiyet İhlalinin Birey Üzerindeki Olumsuz Etkileri

E-devlet sürecinde kişisel bilgilerin istismarı ve mahremiyet hakkının zarar görmesi sorunu, anlamak ve açıklamak bakımından çeşitli zorluklar taşır. "Mahremiyetin zarar görmesi, özel bilgilerin başkalarına açıklanmasıyla ölçülür" koşullu önkabulü, kişisel bilgiler açıklanmasa dahi sadece izlenmekten dolayı bireyin gördüğü zararı ve olumsuz etkileri ihmal etmektedir. Kişisel bilgilerin kamu kurumları tarafından toplanması, işlenmesi ve depolanmasında bilgi iletişim teknolojilerinin yaygınlaşması vatandaşlar ile devlet arasındaki, güç ilişkilerini etkilemektedir. Kamu kurumlarının dijital ortamda tuttuğu bilgilerin işlenme ve korunması sırasında ortaya çıkan güvenlik ve istismar tehlikesi karşısında birey kendini güçsüz ve çaresiz hisseder. Öte yandan kendi yaşamı hakkında önemli kararlar alan kamu kurumlarıyla olan ilişki biçiminin değişmesi sosyal yapıda da önemli değişimler yaratır.

Mahremiyet sorunlarını anlamakta Solove'nin tasnif çalışması yararlı görünmektedir (2007:758). Solove'ye göre mahremiyet sorunlarını dört kategoriye ayırmak mümkündür.

1- Bilgi toplama: izleme ve sorgulama süreçleri ile ilgili sorunları,
2- Bilgi işleme: gereksiz detaylı bilgilerin toplanması, tek başına anlamsız verilerin kişilerin siyasi görüş, inanç vb gibi özelliklerinin tanımlanmasında kullanılması, bilgilerin toplanma amaçlarının dışında kullanılması, kategorize edilen bireylerin dışlanması, kişisel bilgilerin işlenmesi sonucunda şüpheli veya riskli olarak tanımlanan bireylerin bilgilerinin istismar edilmesi ve ayrımcı

davranışla karşılaşma olasılığı.
3- Bilginin yayınlanması ve dağıtılması: bilgilerin korunması ve saçılması, ifşa edilmesi, istenmeyen kişilerin erişimine açık olması, şantaj amacıyla kullanılması ve bilgilerin çarpıtılması.
4- Mahremiyet İstilası: kişisel bilgilere izinsiz ve kanunsuz ulaşım, keyfi müdahaleler.

Bu tasnif, meseleyi anlamakta kılavuz olabilecek bir çerçeve sunmaktadır. Ancak mahremiyet sorunlarının tümünü açıklamak bakımından yeterli değildir. Tamamen masum olan insanların kişisel bilgileri üçüncü kişilere geçmese dahi mahremiyet sorunları ortaya çıkmaktadır. Genel kabul gören mahremiyet anlayışı gizlilikle ilişkilidir ve bireylerin kişisel bazı şeyleri saklama hakkını kapsar. Ancak bilgiler açıklanmasa dahi devlet kişi mahremiyetine zarar verebilir. Örneğin ABD'de bir kan davası sonucu hasmın kamu kurumlarının web sitelerinden (Sosyal Güvenlik, Nüfus İdaresi, Vergi Dairesi, Seçmen kaydı vb) adres bilgilerine ulaşılarak bulunup, öldürülmesi örneği, riski açıklamaktadır Burada karakteristik sorun, bu tür açıkların ancak gerçekleştikten sonra gündem konusu olması ve sakıncaların giderilmesi çalışmalarına gecikmiş olarak başlanmasıdır.(Solove, 2007:762)

Siber-uzayda yapılan her türlü davranış dijital olarak gerçekleşir ve dijital evrende silinmeyen bir iz bırakır. Devlet, egemenlik gücünü kullanarak bu izlerin her birine ulaşabilir. E-devletin kişisel bilgileri her zaman kayıt etmesi ve bunun bireyler tarafından bilinmesi ve devamlı olarak izlendiğini düşünmesi, bir Panoptikon işlevi görmektedir. Zaman içerisinde bireyde yerleşen kronik korku, bireylerin davranışlarını, düşüncelerini, değerlerini ve tercihlerini de yönlendirmeye başlayacaktır. Nihayetinde izleme gücünü elinde tutanların hoşlanmadığı şeyleri dahi düşünmeyeceklerdir. İşte, evde, televizyon izlerken, internette dolaşırken, her yerde mahremiyetin kalmadığı bir ortam da yaşadığını bilen, hastalık, eğitim durumu, maddi varlıklar, neleri tükettiği gibi her türlü mahrem bilginin devletin elinde olduğunu her zaman hatırlayan birey, özgürlüğünü ve serbestçe davranma, düşünme ve yargılama yetisini yitirir ve iradesini iktidara teslim eder.

3. SONUÇ

E-devlet, kamusal hizmetlerde etkinlik ve verimlilik bakımlarından dramatik artışlar sağlamakta, kamu hizmetlerinin yürütülmesi ve vatandaşlar açısından vazgeçilemez faydalar sunmaktadır. Demokratikleşme açısından sunduğu imkânlar da oldukça büyük vaatler sunmaktadır Bilgi ve iletişim teknolojilerinin kamu yönetiminde ve özel sektörde ve vatandaşlar arasında yaygınlaşması, toplumu tüm boyutlarıyla dönüştürme sürecine girmiştir. E-devletin sağladığı yararlar yanında olumsuz etkilerine karşı genel yaklaşım; elde edilen büyük faydanın yanında tahammül edilebilir veya ihmal edilebilir bazı olumsuz çıktıların olabileceği şeklinde özetlenebilir.

Kamu yönetiminde kullanılan bilgi iletişim teknolojilerinin tam bir güvenlik sağladığını söylemek mümkün değildir. Bu sistemlerin yapısı gereği denk veya daha gelişmiş teknolojiler kullanarak güvenlik önlemlerinin bertaraf edilmesi söz konusu olabilmektedir. Öte yandan bilgi iletişim teknolojilerinin açıklar, boşluklar ve zayıf noktalar bırakmayacak şekilde tasarım ve dizaynının yapılması da mümkün değildir. Anılan vakalarda görüldüğü üzere kamu kurumlarının web sitelerine saldırı amaçlı müdahaleler olmasa dahi., bu sitelerden kişisel verilere ulaşılmasına imkan sağlayan, öngörülemeyen açıklar ve tasarım eksiklikleri söz konusu olmaktadır.

Kamu kurumlarında kişisel verilerin toplanması, işlenmesi ve saklanmasına dair klasik uygulamalar, neredeyse yüzyıllar boyunca süren bir olgunlaşma süreci akabinde güvenilirlik kazanmıştır. Geleneksel dönemde kamu kurumunda tutulan kişisel verilerin istismar edilmesi, çalınması veya kopyalanmasına karşı günümüze göre daha fazla güvenlik sağlanmaktaydı. Örneğin kağıt ve dosyalarda tutulan kişisel bilgilerin çalınması, genellikle korunan bir kamu binasının bekçisinin atlatılması, kilitlerin kırılması, binaya gizlice girilmesi, binlerce dosya veya evrak arasında hedeflenenin bulunması, gibi yakalanma riski yüksek ve zor bir teşebbüs gerektirmektedir. Geleneksel kağıda dayalı kamusal arşivlerde geçerli ve etkin güvenlik teknikleri uygulanmaktayken, günümüzde bu tür etkin önlemler henüz daha gelişmemiştir. Eski dönemde bu tür eylemleri önlemeye yönelik ceza yasaları da detaylı ağır cezalar öngörmekteydi. Halbuki günümüzde teknoloji vasıtasıyla, muhtemelen klasik kağıt-dosyaya dayalı arşivleme sisteminde yüzlerce kamyonu doldurabilecek kişisel bilgilere, ülke dışında dahi olsa ulaşmak, kopyalamak veya tahrifat yapmak, saniyelerle sürecek bir eylem olmakta ve yakalanma riski ve zorluk dereceleri kat kat azalmaktadır. Yine bilgisayar vasıtasıyla işlenebilecek suçlara yönelik hukuki yaptırımlar da önceki döneme göre caydırıcı olmaktan uzaktır.

Devletin bilgi iletişim teknolojileri kullanarak vatandaşların en mahrem kişisel bilgilerine ulaşabilmesi, depolaması ve işlemesi imkanına kavuşması, siyasi iktidarlarda bu gücü istismar etme, baskıcı ve otoriter amaçlarla kullanma eğilimlerini teşvik edici niteliktedir. Etkinlik ve verimlilik gibi sayılabilir ve somut faydaların yanında, toplumun tüm bireylerinin mahremiyetlerinin zarar göreceği korkusuna kapılması, demokrasinin aşınması ve otoriter eğilimlerin güç kazanması gibi teknoloji ile gelen faydaları kat kat aşan maliyetlerin de ortaya çıkabileceğini hesaba katmak gereklidir.

Kamu kurumlarının kullandığı bilgi iletişim teknolojilerinin tümü henüz uzun bir geçmişi ve zamana dayalı sınanmışlığı olmayan teknolojilerdir. Sofistike ve karmaşık doğaya sahip bu teknolojilerin karakteristik güvenlik zaafları ve eksikleri, belli bir zaman geçtikten ortaya çıkabilmektedir. Kamu

yönetiminde kişisel bilgilerin korunması gibi kritik işlevleri görmek bakımından güvenilir olduklarını söylemek mümkün değildir. Yazılım programı üretmenin temel ortak özelliklerinden biri de tutarlılık, güvenilirlik çalışmaları yapıldıktan sonra, hesap edilemeyen, gözden kaçan zaafiyet ve güvenlik eksiklerinin tamamlanması için "deneme sürümü" (beta versiyon) olarak kullanıcıların deneme amacıyla kullanmalarını sağlamak ve kullanım esnasında "mümkün olduğu kadar çok sayıda kullanıcı" tarafından bulunan sorunları düzelterek, asıl ürünü ortaya çıkarmaktır. Akabinde yazılımlar eksikleri ve açıkları açısından sürekli olarak güncellenir. Tam bir güvenlik sunan yazılım programı yoktur. En güvenli olması gereken bankacılık hizmetlerine yönelik yazılım programları dahi güvenlik açıklarını henüz gideremememekte; bilgisayar korsanlarının, hesap boşaltma gibi eylemleri sonucunda tespit edilen açıkları kapatmaya çalışmaktadırlar. Kamu kurumlarının kişilerin mahrem bilgilerini bu tür açıklara doğası gereği sahip olan yazılımlarla toplaması ve saklaması, önemli bir sorundur.

Kamu kurumlarında saklanan kişisel bilgilerin korunmasına yönelik hukuki düzenlemeler ve yaptırımlar olsa dahi henüz yeterli seviyede olduğunu söylemek mümkün değildir. Öncelikle kişisel bilgilerin korunması, üçüncü kişiler veya devlet tarafından istenmeyen amaçlarla kullanılmasına karşı yeterli hukuki düzenlemelerin gerçekleştirilmesi gereklidir.

Kişi mahremiyetini etkileyebilecek kanun yapma, kamu politikası belirleme, yeni kamusal örgütler oluşturma ve yeni teknolojileri satın alma, ruhsatlama ve kullanma süreçlerinde, kanunlar hazırlanıp yayınlanmadan, teknolojiler kullanılmadan veya örgütler oluşturulmadan önce, mahremiyet bakımından olası sakıncaları ve zararları ortaya çıkmadan önce tespit edecek ve önerilerde bulunacak ve "mahremiyet etki değerlendirmesi" yapacak siyasi açıdan bağımsızlığı gözetilen bir denetim kurumunun ve standartların oluşturulması zaruri derecede gerklidir.

Gerçek dünyadan farklı olarak bireylerin siber-uzayda yaptıkları her tür hareket, bireyin kendisiyle ilişkili bir iz bırakmaktadır. İzleme, kayıt etme, veri madencilik ve veri eşleştirme gibi tekniklerle bireylerin, kişilik özelikleri, siyasi eğilimleri, müzik, sanat, spor tercihleri, gibi en detaylı kişilik profillerini oluşturmak mümkün hale gelmiştir. Bireyler istenen kriterlere göre kategorize edilebilir. Ekran üzerinde CBS (Coğrafi Bilgi Sistemleri) vasıtasıyla, atanmış renk veya semboller vasıtasıyla izlenebilir veya işlemlere maruz bırakılabilir. Neticede bireyin en derin ve gizli mahremiyet alanları dahi güvenliğini yitirmektedir. Mahremiyet alanları, bireyin kendi bütünlüğünü koruduğu, geliştirdiği veya gerektiğinde iyileştirdiği kritik psikolojik değeri olan alanlardır. Bu alanların ihlalinin ortaya çıkaracağı sorunların büyüklüğünü kestirmek, tam olarak mümkün olmamakla birlikte korunması gereklidir. Bu tür risklere karşı yasal düzenlemeler kapsamlı bir şekilde geliştirilmelidir.

KAYNAKÇA

Akın, H. Bahadır**,** (2009) "Küresel Panoptikon: Yeni Teknolojiler, Gözetim ve Bilimkurgu Romanları Çerçevesinde Toplumsal Endişeler Üzerine Bir Değerlendirme", http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=260

Arendt, Hannah (2003) *The Portable Hannah Arendt* (Ed: Peter Baehr), Penguin Books, NY.

Başbakanlık (2008) Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, 22.4.2008 tarih ve 1812 sayı ve "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı" konulu Başbakanlık belgesi.

Bennett, Colin J. (2009) "Privacy in the Political System: Perspectives from Political Science and Economics", (Ed: A. Westin), *Privacy and Freedom Updated: Social Science Perspectives on Privacy*. http://scholar.google.com.tr/scholar (4.3.2009)

Bentham, Jeremy; Pease-Watkin, Catherine ve Werret, Simon (2008) *Panoptikon, Gözün İktidarı*, (Çev. Barış Çoban, Zeynep Özarslan), Su Yayınları, İstanbul.

Botan, C. (1996) "Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects", *Communication Monographs*, C:63/4: 293-313.

Cilingir Demir ve Kushchu, İbrahim (2004) "E-Government ve m-Government: Concurrent Lepas by Turkey", *mGovlab*, www.mgovlab.org:1-10

Craven, John (1982) "Liberalism and Individual Preferences" *Theory and Decision*, C:14/4: 351-360.

Dobel, Patrick, (1999) *Public Integrity*, The Johns Hopkins University, Baltimore.

Ekip Gazetesi (2008), "Unutulan Belde", 7. 12.2008

Encyclopedia Britannica, (2009) http://info.britannica.co.uk/ (3.3.2009)

Eryılmaz, Bilal, (2008). *Kamu Yönetimi*, Seçkin Yayıncılık, Ankara.

European Parliament (1999) "Development of Surveillance Technology and Risk of Abuse of Economic Information", *STOA Panel*- Luxemburg, Ocak 1999, EP, http://www.fas.org/irp/program/process/docs/981401-5en.pdf, (4.3.2009).

Friedman, David (2000) "Privacy and Technology", *Social Philosophy & Policy*, C:17:186-212

Fromm, Erich (1995) *Özgürlükten Kaçış*, (Çev: Şemsa Yeğin) Payel Yayınları, İstanbul

Gürbilek Nurdan (2001) *Vitrinde Yaşamak*, Metis Yayınları, İstanbul.

Hurriyet Gazetesi (2009) "150 bin İstanbulluya Telefon Şoku", 28.2.2009.

Hurriyet Gazetesi (2009a) "687 bin öğretmenin kimlik bilgileri çalındı", (12.2.2009)

Hurriyet Gazetesi (2009b) "KEY ödeme listesini çalıp, dolandırmışlar", (16.3.2009)

Kakabadse, A. P vd (2004) "Three Temptations of Leaders", *Leadership and Organization Development Journal*, C:28/3: 196-208

Ketizmen M. ve Ülküderner, Ç. (2007) "E.devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması", *XII "Türkiye'de İnternet" Konferansı*, 8-10 Kasım 2007, Bilkent Üniversitesi, Ankara: 189.193.

Laidler, Keith (2008) *Surveillance Unlimited: How We've Becom the Most Watched People on Earth*, Iconbooks, Cambridge.

Lukes, Steven (1995) *Bireycilik*, (Çev: İsmail Serin) Ark yayınları, Ankara.

Mill, John Stuart (2004) *Hürriyet Üstüne*, (Çev. Mehmet Osman Dostel) Liberte Yayınları, Ankara.

Ofluoğlu, G. ve Büyükyılmaz, O. (2008) "Yabancılaşmanın Teorik Gelişimi ve Tarihsel Süreç İçinde Farklı Alanlarda Görünümleri", *Kamu-İş*, C:10/1:113-144.

Orwell, George, (1999*) Bin Dokuz Yüz Seksen Dört,* (Çev:Nuran Akgören), Can Yayınları, İstanbul

Milliyet, (2006) "MERNİS Skandalı", 12.10.2006.

Milliyet (2008) "Seçmen Listelerinde Pes Dedirten Skandallar", 25.12.2008.

Mills, Jon L (2008) *Privacy: The Lost Right*, Oxford Unversity Pres, Oxford.

Perri, 6 (David Ashworth) (2001) "E-governance: Weber's Revenge", *Challenges to Democracy: Ideas, Involvement an Isntitutions: the PSA Yearbook*, Basingstoke, Palmgrave: 220-236.

Sherrer, Hans, (2000) "The Inhumanity of Government Bureaucracies", *The Independent Review*, C:2/2000: 249-264.

Solove, Daniel J (2007) ""I've Got Nothing to Hide" and Other Misunderstanding of Privacy", *San Diego Law Review*, C:44: 745-772.

Yılmaz, Gözde (2005) "Elektronik Performans İzleme Sistemlerinini Çalışanlar ve İşletmeler Üzerindeki Etkileri", *İstanbul Ticaret Üniversitesi, Sosyal Bilimler Dergisi*, C: 4/7:1-19.
Yüksel, Mehmet (2003) "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi", *AÜ SBF Dergisi*, C:58/1:181-213.
www.keyodemeleri.com
www.nvi.gov.tr