Mahremiyet Sorunlarının Önlenmesinde Mahremiyet Etki Değerlendirmesi (MED)

Doç. Dr. Muhittin TATAROĞLU
Muğla Üniversitesi, İ.İ.B.F., Kamu Yönetimi Bölümü, MUĞLA

ÖZET

Demokrasinin gelişmesi açısından oldukça büyük fırsatlar sunan e-devlet süreci ve kullanılan teknolojiler, kişi mahremiyeti bakımından önemli sakıncalar da doğurmaktadır. Mahremiyet ise devlet ve birey ilişkilerinde önemli bir sorun alanı olarak karşımıza çıkmaktadır. Bilgi ve iletişim teknolojileri gibi muazzam güç kaynaklarının cazibesi karşısında devlet ve hükümetler karşısında kişi mahremiyetinin korunması, demokrasi açısından yaşamsal önem kazanmaktadır. Teknoloji kullanımından doğan mahremiyet sorunları özel sektörde de söz konusu olmakla birlikte, devletin kişi mahremiyetine yönelik ihlalleri önemli artış sergilemektedir. Çalışmada e-devlet sürecinin kişi mahremiyeti açısından yarattığı tehlike ve olumsuzluklara karşı Mahremiyet Etki Değerlendirmesi önerisi geliştirilmiştir.

Anahtar Kelimeler: *Teknoloji, mahremiyet, e-devlet, Mahremiyet Etki Değerlendirmesi (MED)*

JEL Sınıflaması*: D730, O380, H83*

Privacy Impact Analysis (PIA) in Preventing Privacy Issues

ABSTRACT

In terms of democratic development, e-government and technology offer great deals; but also raises very important privacy drawbacks. Privacy is encountered as an important problem area in that way of the relationship state and individual. While information and communication technologies provide enormous power of attraction of state and government; it is vital for democracy to protect people's privacy. In this study, privacy impact assessment against the privacy concerns in the e-government process is proposed as a solution alternative.

Key Words*: Technology, privacy, e-government, Privacy Impact Assessment (PIA)*
JEL Classification*: D730, O380, H83*

Giriş

Mahremiyetin bir insan hakkı olduğu, genel kabul görmüş bir anlayıştır. İnsanlar kendileri hakkındaki bilgilerin adil bir şekilde işleneceği ve muamele göreceğinden emin olmalıdır. Bu talep kamu kurumlarının elindeki kişisel olarak tanımlanabilir bilgileri de kapsamaktadır. Kamuya hizmet sunumunda ve çeşitli işlevlerin yerine getirilmesinde kamu kurumları vatandaşlarla ilgili kişisel bilgileri toplar ve kullanır (sağlık kayıtları, vergi iadeleri, sabıka kayıtları, ehliyet verileri vs gibi). Elektronik veri yönetimi ve enformasyon toplumuna geçişle birlikte veri toplama, işleme ve saklama işlevleri olağanüstü bir biçimde artmıştır. Devletin vatandaşlar hakkındaki kişisel verileri toplaması, saklaması ve yönetmesi, mahremiyet sorununu giderek daha önemli hale getirmektedir.

Kişi mahremiyetinin temel haklar kapsamında yer alması ve toplumsal yaşam ve demokrasi ilkeleri bakımından kritik öneme sahibi olması gibi

nedenlerle özel ilgi gösterilmesi gereken haklardandır. Bu bakımdan bilgi iletişim teknolojilerinin yaygınlaşması ve e-devlet süreçlerinde mahremiyetin zarar görme dereceleri de önemli farklılıklar göstermektedir. 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 kalıp, zaman içinde unutulacakken; bu mahrem bilgilerin internette yayınlanmasıyla tüm dünyaya 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 ihlalinden daha önemli bir sorun da vatandaş devlet ilişkilerinde ortaya çıkmaktadır. Kamu hizmeti sunumunda vatandaş ile devlet arasındaki ilişki, eşitsizlik esasına dayalıdır. Sunulan hizmet, hizmete erişim şartları ve ilişki biçimini devlet belirler ve vatandaş bunlara uymak durumundadır. E-devlet kurumlarında hizmet alımı esnasında pek çok kişisel bilgi talep edilir. Vatandaşlık numarası, yaş, eğitim, banka hesabı, adres vs gibi istenen bilgilerin herhangi birinin eksik olması durumunda ilişki ve erişim kesilir. Öte yandan, kişisel bilgilerin çoğu MERNİS, ADNKS, TAKBİS gibi sistemlerde toplanır ve kullanılır. Bilgi teknolojileri öncesi fiziki arşivlerde ve kağıt üzerinde bulunan kişisel bilgiler; e-devlet bünyesinde birbirine ağlarla 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. Öte yandan, devlet veya iktidar tarafından da kötü amaçlı kullanılma olasılıkları söz konusudur.

Devletin egemenlik gücüne dayanarak bireylerin rızası olmadan toplanan bilgilerin hem diğer bireyler hem de devlet tarafından istismar örneklerine değinilmiştir. Yine e-devlet kurumlarında toplanan kişisel bilgilerin korunamaması, birey aleyhinde sonuçlar doğuracak şekilde kullanılması ve ilgili kurumlar tarafından "bilgi saçılması" şeklinde yayılması tehlikesi, bireylerde yerleşik bir korku hissine neden olmakta ve olumsuz davranış ve duygu değişimlerine yol açabilmektedir.

Siyasi iktidarlar kendilerine güç sağlayacak veya güçlerini artıracak araçlar ve teknolojilerin cazibesi karşısında zaafiyet gösterirler. İktidarların kendilerine büyük güçler sağlayan araçlara karşı bu güç hırsı ya da zaafiyeti (temptation of power) (Dobel, 1999: 23), demokratik rejimlerin aşınmasına yol açabilmektedir. Bilgi iletişim teknolojileri de izleme, gözetleme gibi bazı alanlarda iktidarları baştan çıkaran yetenekler sunmaktadır. Bu araçların baskıcı, totaliter ve antidemokratik eğilimleri tahrik etmesi olasıdır. Bu bakımdan e-devlet sunduğu olumlu gelişmelerin yanında kişi mahremiyeti ve demokrasi açısından olumsuz pek çok kritik tehlikeyi bünyesinde barındırmaktadır.

Modern devlette egemenliğin meşruluğunun en önemli dayanaklarından biri de devletin vatandaşlarını koruması ve hukuku uygulamasıdır. 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(Tataroğlu, 2009: 113-116). Bu durum ise vatandaşların e-devlete olan güven duygularını aşındırmakta; davranışlarını ve ruh hallerini olumsuz yönde etkilemektedir.

E-devletin yarattığı bu sakıncaların giderilmesi gereklidir. Kamu kurumlarında toplanan kişisel bilgilerin saklanmasında, kullanılmasında ve yayınlanmasında sorunlar belirlenmeli; mahremiyet hakkının zarar görmesini engellemek için gerekli düzenlemeler yapılmalı ve bu süreci teminat altına alacak prosedürel önlemler ve ihtisas kurumları oluşturulmalıdır.

Güven unsuru, ister e-ticaret, ister e-devlet alanında olsun herhangi bir online programın başarılı olmasında yaşamsal önemdedir. Mahremiyet online güvenin sağlanmasında anahtar unsurdur. Böylelikle, kamu hizmetlerinin online sunulmasını kolaylaştırma çabasında olan ülkeler, topladıkları bilgilerin mahremiyeti ve güvenliğini sağlamak zorundadırlar.

Yöntem

Çalışma alanı birden fazla disiplini kapsamaktadır. Mahremiyet kavramı günümüzde hukuk ve insan hakları alanları, bilgi iletişim ve yazılım teknolojileri, bilgisayar gibi geniş ve sofistike alanlarla ilgili hale gelmiştir. Kişisel verilerin güvenliği ise başta insan hakları olmak üzere kamu hukuku, ceza hukuku, kamu yönetimi ve anayasa hukuku gibi farklı alanları ilgilendirmektedir. Bu bakımdan çalışma ile ilgili kavramsal çerçeveyi oluşturmak için çok sayıda disiplin alanında literatür taramasını gerekli kılmıştır. Konu ile ilgili hukuki mevzuat ve mahremiyeti etkileyen bilgi teknolojilerinin kullanıldığı kurumlar incelenmiş; bunların işlevleri, eksiklikleri ve sakıncaları araştırılmıştır. E-devlet sürecinde teknoloji kullanımını, insan hakları, demokrasi, yönetim bilimi ve siyaset psikolojisi boyutlarından inceleyen ilgili literatür henüz yeni gelişmektedir.

Bilgi çağı toplumu ve kamu hizmeti sunan kurumların yapı ve işleyişleri, artık Newton'cu-mekanik yaklaşımlarla açıklanamayacak derecede karmaşıklaşmıştır. Günümüz toplumlarını ve kamu yönetimlerini anlayabilmek için, kuantum, kaos, karmaşıklık gibi post-modern yaklaşımlardan yararlanmak zorunlu hale gelmektedir. Günümüz bilgi iletişim teknolojileri de karmaşıklık temeli üzerinde kurulmuştur. Böyle olmakla, kamu hizmetlerinin denetiminde de post-modern yaklaşım ve uygulamalar kaçınılmaz hale gelmektedir. "Etki Değerlendirme" süreçleri, günümüzde kamu yönetimi süreçlerinde gittikçe yaygınlaşan yöntemler haline gelmiştir.

Bilgi iletişim sistemlerinin ve sanal yazılımların en önemli karakteristiklerinden olan karmaşıklık, hiçbir zaman tam bir güvenlik sunamaması ve sorumluluk sorunu, kişi mahremiyeti bakımından kritik alanları oluşturduğundan, örnek olay ve incelemelerle etraflı bir şekilde ele alınmıştır. Kamu yönetiminde uygulanan gözetim ve arşivleme amaçlı bilgi iletişim teknolojilerinin yarattığı mahremiyet sorunları incelenmiştir. Çözüm önerisi geliştirmek amacıyla kamu yönetiminin çevresel etki değerlendirmesi, düzenleme etki değerlendirme, sağlık etki değerlendirme ve sosyal etki değerlendirme gibi etki değerlendirme süreçleri incelenmiştir. Bu uygulamaların incelenmesinden

yararlanarak, mahremiyet etki değerlendirmesi modeli çözüm olarak önerilmiştir.

I- Yeni Kamu Yönetimi Anlayışında Etki Değerlendirme Yöntemi ve Türleri

Teknolojinin gelişmesinin de katkısıyla günümüz toplum yapıları ve işleyişleri gittikçe karmaşık görünüme bürünmektedir. Kamu yönetiminde alına kararların, uygulamaya konan proje ve programların, kullanılan teknolojilerin ve yürürlüğe konan düzenlemelerin topluma ne tür etkide bulunacağını kestirebilmek, modern dönemin mekanik-Newtoncu yaklaşım (Saylı, 2008: 183) ve teknikeriyle mümkün olmamaktadır. Post modern veya bilgi çağı toplumu olarak adlandırılan toplumlarda kamu yönetimlerinin faaliyetlerini modern yöntemlere dayalı yöntem ve uygulamaları geçersiz kalmakta ve sistemin tıkanmasına kadar giden sakıncalar barındırmaktadır.

Gelişen ve karmaşıklaşan toplum yapılarını anlayabilmek ve değişime uygun yöntem ve tedbirler geliştirmek amacıyla toplumların yapı ve işleyişlerini analiz etmeye yönelik "kaos teorisi" (Aktaş, 2003: 45)", "kuantum teorisi" (Overman, 2012: 76), "sibernetik kuramı" (Overman ve Lorraine, 1994) ve biyolojiden yararlanılarak geliştirilen "açık sistem yaklaşımı" (Bayri, 2003: 151) gibi yeni açıklama çabaları ve yönetişim, kamu yönetiminde kalite, şeffaflık, etkinlik ve verimlilik, katılımcılık, sonuç odaklılık (Eryılmaz, 2010: 178) gibi işleyişe yönelik yeni uygulamalar ve değerler geliştirilmesi kaçınılmaz olmuştur.

Modern dönemde düzenleme, proje, program gibi girdilerin toplumu nasıl etkileyeceğine dair tahminlerde bulunmak, olumsuz etkiler söz konusu olduğunda da telafi yoluna gitmek görece kolay ve etkin olabiliyordu. Ancak günümüz karmaşıklaşan toplum yapısı ve gün geçtikçe sofistike hale gelen kamu yönetimi uygulamaları bu klasik yöntemleri geçersiz kılmaktadır. Günümüzde kamu yönetiminde siyasi idari veya teknik girdilerin olumsuz etkilerini tahmin etmek güç; ayrıca ortaya çıkan zararlı etkiler çok vahim olabilmekte ve telafisi de kolay olmamaktadır.

Bu bakımdan kamu ve özel sektör alanında düzenleme, proje, program gibi teşebbüslerin sonuçlarının önceden iyi ve detaylı olarak tahmin edilmesi, olumsuzluk ihtimallerinin iyi değerlendirilmesi, süreçlerden etkilenecek olanların bilgilendirilmesi, karar ve uygulama süreçlerine paydaşların katılımının sağlanmasına yönelik yeni arayışlar söz konusu olmuştur. Bu arayışlar "Etki Değerlendirme" yöntem veya süreçleri şeklinde yeni uygulamalar olarak ortaya çıkmaktadır.

Etki değerlendirme, karar vericilerin düzenleme yapma, proje, program veya teknoloji uygulama süreçlerinde önceden farklı alternatifler geliştirmelerini ve sonuçlara dair güvenilir bilgi elde edilmesini sağlayan bir süreçtir (Küçükyumuk, 2012: 7). Kamu veya özel sektördeki girişimlerin etki değerlendirmesini yapmak, sağlıklı politikalar belirlemek, toplumsal amaçların başarılmasını sağlamak açısından önem taşımaktadır.

Sonuçlarının kestirilmesinin güç olduğu girişimler öncesinde henüz karar aşamasında topluma getireceği etkilerin önceden incelenmesi ve değerlendirilmesi, hedef gruplar, paydaşlar ve etkilenecek olan kesimlere

düzenleme sürecine katılma fırsatı tanınması, yönetişim ve demokrasi açısından olumlu bir gelişmedir. Öte yandan süreçler ve girişimler hakkında etkilenen kesim ve paydaşların bilgi edinmesi mümkün olur. Bu sayede saydamlık, katılımcılık, olası sorunların önceden tespit edilmesi ve önlenmesi, etkin katılım sayesinde verimlilik ve etkinliğin sağlanması ve hedef kitlenin değişime hazırlanması mümkün olur (SGB, 2008: 3)

AB ile 35 başlık altında yürütülen müzakere süreci kapsamında, tarama safhasından sonraki aşama olan fiili müzakerelerde AB müktesebatının etki analizlerinin yapılması da kararlaştırılmıştır. Etki analizleriyle benimsenmesi düşünülen müktesebatın vatandaşlar, kamu yönetimi, iş dünyası, sivil toplum ve toplumun diğer kesimleri üzerindeki olası sosyal, ekonomik ve çevresel etkileri değerlendirilmektedir (Ekici, 2006: 144).

1- Bütçe Etki Değerlendirmesi

Başlı başına ayrı bir yöntem olarak mevzuatlaştırılmasa da "bütçe etki değerlendirmesi" yöntemi, idarelerin yasa tasarılarında bütçeye getireceği yükler ve gelir azalması bakımından etkilerini açıklayan bir ek şeklinde uygulanır. Bu uygulama 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunun 14. Maddesinde düzenlenmiştir. Maddeye göre merkezi yönetim kapsamındaki kamu idareleri; kamu gelirlerinin azalmasına veya kamu giderlerinin artmasına neden olacak ve kamu idarelerini yükümlülük altına sokacak kanun tasarılarının getireceği mali yükü, orta vadeli program ve mali plan çerçevesinde, en az üç yıllık dönem için hesaplar ve tasarılara ekler. Sosyal güvenliğe yönelik kanun tasarılarında en az yirmi yıllık aktüeryal hesapların yapılması gerekir. Ayrıca henüz yasal zorunluluk olmamasına rağmen bazı kamu kurumları yeni uygulama ve girişimleri için bütçe etki analizi yapmaktadırlar. Örneğin Sağlık Bakanlığında yeni bir ilacın veya tedavi-teşhis yönteminin uygulamaya alınması durumlarında diğer tıbbi-teknik değerlendirmeler yanında söz konusu ilaç için ilaçtan yararlanacak tahmini hasta sayısı; geri ödeme talep tahminleri; provizyon, reçete veya hasta başına parasal maliyet; fabrika, toptan ve eczane çıkış fiyatları; her yıl için tahmini geri ödeme talepleri; yeni ilacın kullanılması ve kullanılmaması durumlarında toplam maliyet ve bütçeye etkisi gibi unsurları içeren "bütçe etki değerlendirmesi" uygulamalarına başlamıştır (Ökem, 2008: 12).

2- Sağlık Etki Değerlendirmesi

Toplumun sağlığını etkileyen faktörlerin sayı ve kapsam bakımlarından artması ve toplum sağlığını etkileyen dolaylı süreçlerin klasik yöntemlerle fark edilememesi ve ortaya telafisi zor vahim sonuçlar çıkması, önemli ve büyük ölçekli projelerin topluma etkilerini hesaplamakta yeni yöntemler geliştirilmesini zorunlu kılmıştır. Sağlık Etki Değerlendirmesi (SED), bir politikanın, stratejinin, programın veya projenin nüfusun ve nüfus gruplarının sağlığı üzerindeki dolaylı ve dolaysız etkilerini tanımlamak, olası zararlı etkileri tespit etmek, alternatif çözüm önerileri geliştirmek, proje çıktılarının olumlu yanlarını belirlemek ve hayata geçirmek için araştırma tekniklerini uygulama sürecidir (Harris, 2012: 3).

SED bir proje, politika veya strateji teklifinin bir nüfus grubu üzerindeki etkilerini belirler ve karar vericilere karar alma sürecini daha iyi hale getirebilmeleri için bilgi sağlar. Bu şekilde karar alma süreci tamamlanmadan önce olumsuz sağlık etkilerinin asgari boyutlara indirilmesi ve olumlu etkilerin en üst düzeye çıkarılması mümkün olur. SED sırasıyla şu aşamalardan oluşur: projenin analizi; etkilenecek toplumların profili; paydaşlardan bilgi toplanması; beklenen etkilerin önemi, derecesi ve olasılıklarının değerlendirilmesi; seçeneklerin öncelik sıralamasına tabi tutulması ve eyleme yönelik öneriler geliştirilmesi.

SED süreçlerine paydaşların katılımının sağlanmasıyla saydamlık, şeffaflık ve demokratiklik; sadece nüfusun geneli üzerindeki etkilerin değil, nüfus gruplarının ayrımında değerlendirmeler (kadın, çocuk, yaşlı vb) yapılarak eşitlik; uzun ve kısa dönemde gelişmeler izlendiği için sürdürülebirlik; eldeki veriler ve yöntemler bilimsel yollarla elde edildiğinden bilimsellik gibi kazanımlar sağlar SKPO, 2012: 2). SED hem ulusal hem de yerel düzeyde ve çeşitli uluslar arası kuruluşlarda farklı isim ve işlevlerle uygulanmaktadır. Tek başına gerçekleştirilebildiği gibi ÇED, Sosyal Etki Değerlendirme (SED) ve Tümleşik Etki Değerlendirme (TED) gibi başka etki değerlendirme türleri içerisine de dâhil edilebilmektedir.

AB'nin yasal zemine kavuşturulması tavsiyesine karşın Türkiye'de SED henüz yasal altyapıya kavuşmamıştır. Ancak Sağlık Bakanlığı(Sağlık, 2012), Yerel yönetimler (Nilüfer, 2012), Üniversiteler gibi kurumlar AB ve DSÖ'nün desteğiyle eğitim programları uygulamaya başlanmıştır. Adnan Menderes Üniversitesi'nce AB desteği ve ortaklığıyla hazırlanan "Yeni Üye Ülkeler ve Geçiş Sürecindeki Ülkelerde Sağlık Etki Değerlendirmesi" projesi kapsamında "Turizmde Sağlık Etki Değerlendirmesi: Kuşadası" projesi gibi çalışmalar artarak devam etmektedir (ADÜ, 2012).

3- Çevresel Etki Değerlendirmesi ÇED

Çevresel etki değerlendirmesi, kamu ve özel sektör girişimlerinin gerçekleşmeden önce çevresel uzantılarının dikkate alınmasını temin eden bir prosedürdür. Süreç çevre üzerinde oluşacak muhtemel etkilerin analiz edilmesi, bu etkilerin bir rapor ile kaydının tutulması, bu Rapora danışılması, nihai karar alınırken yorumların ve raporun dikkate alınması ve sonrasında bu kararın halka duyurulmasını kapsar (2872 sayılı Çevre Kanunu). Bir başka tanımla ise ÇED, herhangi bir faaliyetin doğabilecek tüm çevresel ve sosyal etkilerin değerlendirilmesinde kullanılan idari ve teknik bir süreçtir (Üstün ve Büyükgüngör, 2003: 508). ÇED raporu ise gerçekleştirmeyi planladıkları faaliyetleri sonucu, çevre sorunlarına yol açabilecek kurum, kuruluş ve işletmelerin çevreye yapabileceği tüm olumsuz etkileri göz önünde bulundurarak, çevre kirlenmesine sebep olabilecek artık ve atıkların ne şekilde zararsız hale getirileceğini ve bu konuda alınacak tedbirleri belirleyen rapordur.

Çevre bilincinin oluşmaya başlamasının ardından 1970'li yılların başlarından itibaren "çevresel etki değerlendirme" ismiyle kapsamlı bir denetim mekanizması duyulur olmuştur (Üstün ve Büyükgüngör, 2003: 507). AB'nin 1985

yılında yayınladığı direktif ile yasal dayanağa kavuşmuştur. Uygulama daha sonra başta gelişmiş ülkeler olmak üzere dünya genelinde yaygınlaşmıştır. Türkiye'de söz konusu faaliyetler, ÇED uygulamaları Çevresel Etki Değerlendirmesi İzin ve Denetim Genel Müdürlüğü tarafından yürütülmektedir (Bayındırlık, 2012).

4- Stratejik Çevresel Etki Değerlendirmesi (SÇED)

Stratejik Çevresel Değerlendirmesi, ÇED'den farklı olarak teklifler hakkındaki karar alım sürecinin daha erken bir aşamasında başlayan ve çevreyi ve sağlığı ilgilendiren meselelerin tartışılması için daha fazla zaman tanıyan bir değerlendirme yöntemidir. Stratejik çevresel değerlendirme, özellikle insan sağlığına etkiler de kapsam içine alınarak, çevresel etki değerlendirmedeki mevcut durumdan farklı olarak sağlığın çevresel değerlendirme içerisinde derinlemesine düşünülmesi için fırsat sağlar (Küçükyumuk, 2012). Stratejik çevresel değerlendirme henüz çoğu ülkede kurumsallaşmamış olmakla birlikte, sadece projelerle kalmayıp; politika ve programlara da uygulanmakta ve durumlara tepki vermek yerine, durum yaratmakta ve bunlar üzerinde kontrol sağlamaktadır. SÇED, ÇED'den farklı olarak prosedürler konusunda esnekliğe sahip, çeşitli kamu otoritelerine yer veren, mesele ve uzantıları üzerinde odaklanan, geniş kapsamlı ve daha az ayrıntılı bir süreçtir. Ülkemizde 2872 sayılı Çevre Kanunun 2. Maddesinde yapılan değişiklikle yasal dayanağa kavuşmuştur

5- Sosyal Etki Değerlendirmesi (SOED)

Sosyal etki değerlendirmesi bir teklifin toplum üzerindeki muhtemel sosyal etkilerini değerlendirir. Sosyal etki değerlendirmesi, tekliflerin sosyal etkilerini analiz etme özelliğine sahip olmayan çevresel etki değerlendirmesini tamamlamak üzere geliştirilmiştir. Sosyal etki değerlendirmesi, eğitim, kültür ve bir toplumun üyesi olmak için gerekli yaşam faktörlerini içerir. Bu değerlendirme kapsamındaki diğer faktör ya da belirleyiciler arasında bir toplumun normları, inançları ve değer yargıları bulunur (Franks, 2012: 4). Sosyal etki değerlendirmesi etkilerin nüfus üzerinde yayılmasına dayalı tekliflerin analiz edilmesini içerir. Yalnızca toplumun bütününü analiz etmek yeterli değildir; çünkü bir tasarı çeşitli grupları farklı şekillerde etkilemektedir. Bu yüzden farklı nüfus toplulukları üzerinde oluşan etkiler büyük önem taşımaktadır. Sosyal etki değerlendirmesinde, nüfus karakteristikleri, siyasal ve toplumsal meseleler, kamusal ve kurumsal kaynaklar vurgulanmaktadır (Misra, 2012: 3).

6- Tümleşik Etki Değerlendirmesi (TED)

Tümleşik etki değerlendirmesi çevresel, ekonomik ve sosyal etkilerin tamamını göz önünde bulunduran bir yaklaşımdır. Bu yaklaşımda herhangi bir anahtar faktörün göz ardı edilmesinden kaçınılmakta ve sürdürülebilir kalkınma ve çevre desteklenmekte veya geliştirilmektedir. Tümleşik etki değerlendirmesi ayrıca sonuçlarının çeşitli nüfus toplulukları için analiz edilmesi ve bunların takdim edilmesini amaçlamaktadır (Küçükyumuk, 2012: 8). Tümleşik etki değerlendirmesi pek çok ülkede hem ulusal hem yerel düzeyde var olsa bile her bir tasarı ile ilgili tüm belirleyicilerin değerlendirilmesi için yeterli kaynak ve zaman elde etmek, toplumsal, çevresel ve ekonomik meselelerin doğru ve eşit olarak ele alınmasında olduğu gibi güç olabilmektedir.

7- Düzenleyici Etki Analizi

Düzenleyici Etki Analizi; düzenleyici politikaların kalitesini geliştirme amacıyla yeni teklif edilen ve mevcut düzenlemelerin olumlu ve olumsuz etkilerinin sistematik olarak değerlendirmesini sağlayan, aynı zamanda düzenleyici ve politika yapıcıları daha sistemli bir şekilde düşünmeye ve herhangi bir sorunun alternatif çözümleri arasında seçim yaparken daha geniş ekonomik ve dağıtıcı amaçlara karşı dengeli karar almaya teşvik eden, düzenleyici eylem ve işlemlerde hesap sorulabilirliği arttıran bir araçtır (Ekici, 2006: 14).

Türkiye'de yasal dayanağa kavuşması, ilk kez, veto edilen 5227 sayılı Kamu Yönetiminin Temel İlkeleri ve Yeniden Düzenlenmesi Hakkında Kanun'da "yapılacak düzenlemeler ve kurulacak yeni birimler için düzenleyici etki analizi yapılır" hükmünün yer almasıyla söz konusu olmuş; ancak yasanın yürürlüğe girememesi sebebiyle ancak 2006 tarihinde yürürlüğe giren "Mevzuat Hazırlama Usul ve Esasları Hakkında Yönetmelik" ile mümkün olmuştur. Yönetmelik, kamuda yeniden yapılanmanın, ekonomik alanda hızlı kalkınmanın ve uluslararası alanda Avrupa Birliği'ne entegrasyon gibi önceliklere vurgu yaparak, kanun, kanun hükmünde kararname, tüzük yönetmelik ve diğer alt düzenleyici metinlerin hazırlanması sürecini günün gereklerine uygun hale getirmekte ve OECD ve AB ülkelerinde yaygın olarak kullanılan düzenleyici etki analizini uygulamaya koymaktadır. Esasen düzenleyici etki analizinin alt bileşenlerini oluşturan maliyet-fayda ve maliyet-etkinlik analizleri 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ile mevzuata girmiştir.

II- Kişi Mahremiyeti

Mahremiyet, insan hakları içinde tanımlanması zor olanlarından biridir. Kavram, 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 davranışları, kişilik bilgileri, özellikleri ve kişi ile ilgili olan her şeyden başkalarının ne kadar haberdar olacağı da kişisel mahremiyet ile ilgilidir. Flaherty (1989: 3), mahremiyeti yalnızlık, samimiyet ve anonimliği yaşama hakkı olarak tanımlamaktadır.

Mahremiyeti farklı boyutlarıyla ele almak mümkündür. Gizlilik şeklinde mahremiyet; bireylerin kendileri hakkındaki bilgileri, belirli eylemlerini, herkese veya seçtiği bazı kişilere karşı gizli tutmayı istemesidir. Anonim mahremiyet; bireylerin bazı davranışları (toplum içerisinde yapılmış olsa dahi) bireyle ilişkilendirilemeyecek şekilde yapma isteği, yani anonim olabilme arzusudur. Otonomi mahremiyeti ise, bireyin bazı davranışlarının aleni veya gizli kalması tercihinin kendine bağlı olması, devlet veya diğer kişilerin ilgisine kapalı kalmasını tercih etmesidir (Teh, 2001-2002: 14-15).

Devlete karşı mahremiyet hakkı, diğer kişilere karşı mahremiyet hakkından iki bakımdan ayrılır. İlki, kişiler arasında hırsızlık vb yollarla diğerinin rızası olmadan başkasının mahremiyet alanlarını ihlal etme durumları söz konusu olsa da, birbirleriyle olan ilişkileri genelde gönüllü ve iradi olur. Birey diğerine

açıklayacağı kişisel bilgileri üzerinde kontrol sahibidir. Birey, diğer kişilere karşı mahremiyetini koruyacak güce ve önlemlere sahiptir. Ancak devlet oldukça çok geniş bir alanda kişi mahremiyetine karşı cebri müdahaleler 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 koruyabilir, kilit ve hırsız alarmları gibi tedbirler alabilir); ancak devlete karşı kendini ve kişisel bilgilerini koruması söz konusu olduğunda 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 düşünülür ise; o zaman kişisel mahremiyet, kamu görevlilerinin iyi olanı yapmalarını zorlaştıracak demektir. Ancak öte yandan devletin vatandaşlar aleyhine davranabileceği düşünülürse, o durumda devlete karşı kişisel mahremiyet ve bunun korunması kesinlikle iyi bir şeydir. Mahremiyetin, kişisel suçların saklanmasında kullanılabileceği kabul edilse de; devlete karşı korunması gerektiği görüşü oldukça geniş kabul görmektedir.

1- Türkiye'de Mahremiyetle İlgili Yasal Ve Kurumsal Görünüme Özet Bakış

Bir ülkede yaşayan vatandaşların kişisel verilerin büyük çoğunluğu çeşitli kamu kurumlarınca saklanır ve işlenir. Nüfus idaresi, kişilerin doğum, ikamet soy gibi bilgilerini; sağlık kurumları, sağlık bilgilerini; yargı kurumları, sabıka kayıtlarını; SGK, çalışma, meslek, emeklilik ve maaş gibi bilgileri barındırır. Ayrıca, kural olarak kamu hizmeti talep edilirken bireylerden, vatandaşlık numarası, isim, adres, doğum tarihi, anne-baba adı vb kişisel bilgiler talep edilir. Bu bilgilerin güvenli bir şekilde saklanması, işlenmesi ve ifşa edilmesi gibi sorunlar için yasal ve kurumsal düzenlemeler gerçekleştirilmiştir.

AB'nin bilgi iletişim teknolojileri kullanımında mahremiyet konusu kapsamındaki temel mevzuatı şöyledir:

85/46/AB sayı ve 24.10.1995 tarihli Elektronik İletişimde Kişisel Verilerin Korunması Talimatı,

2002/58/AB sayı ve 12.7.2002 tarihli Kişisel Verilerin Korunması Hakkında Talimat,

2006/24/AB sayı ve 15.3.2006 tarihli ek talimat,

97/66/AB tarih ve 15.12.1997 Telekomünikasyon Alanında Kişisel Verilerin İşlenmesine Dair Talimat.

1982 Anayasasında kişisel verilerin korunmasına yönelik hükümler yer almaktadır. Anayasa'da kişiliğe bağlı dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlerin varlığı (Md. 12) ve kişi hürriyeti ve güvenliğinin teminatı (Md. 19) yer almıştır. Kişilerin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkı 20. maddede düzenlenmiştir.

21. madde, konut dokunulmazlığını düzenlemektedir. Kimsenin konutuna dokunulamayacağı; milli güvenlik, kamu düzeni, suçun önlenmesi, genel sağlık

ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması gibi nedenlerle yargı kararı olmadıkça, gecikmesinde sakınca bulunan hallerde ise kanunla yetkili kılınmış merciin yazılı emri haricinde kimsenin konutuna girilemeyeceği, arama yapılamayacağı ve eşyaya el konulamayacağı hükümleri yer almaktadır. Gecikme ihtimali bulunan durumlarda yetkili merciin vereceği kararın ise 24 saat içinde yargıya bildirilmesi zorunluluğu getirilmiştir. 22. maddede ise haberleşme hürriyetinin gizliliğinin esas olduğu belirtilmiştir.

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 (Mobil Elektronik Sistem Entegrasyonu) Emniyet Genel Müdürlüğü araçları için tasarlanmış, iletişim altyapısı olarak GPRS teknolojisini kullanan, yazılım ve mobil donanım birimlerinden oluşan, coğrafi bilgi sistemleri ve bilgi yönetim sistemlerinin entegrasyonu ile oluşan sistem, trafik akışının takibi ve düzenlenmesine yönelik olarak geliştirilmiş; 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 ve araç sahibi ile bağlantı 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. Sistem süreç içinde bir "Kent Güvenlik Sistemi"ne dönüşmektedir (MOBESE, 2012)

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 İletişim Başkanlığı tarafından gerçekleştirilecektir. Telefon dinleme ve izleme faaliyetleri TİB tarafından yürütülecek; Milli İstihbarat Teşkilatı (MİT), Emniyet Genel Müdürlüğü (EGM) ve Jandarma kuruluşlarından da birer temsilci kurumda görev alacaktır. TİB başkanının, başbakan tarafından atanması öngörülmüştür. Kurumun faaliyetleri hakkında başbakanlığa bilgi vermekle yükümlü tutulmuştur. 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.

Hakkında yasal dinleme kararı alınanlarla birlikte, onların iletişimde bulundukları kişilerin konuşmalarının da dinlenmesi; önemli bir mahremiyet sorunu olarak karşımıza çıkmaktadır. Bu "üçüncü" kişiler ne yetkili makam, ne de yargı kararı olmamasına rağmen dinlenmekte ve kayda alınmaktadır. İletişimde bulunulan kişi hakkında dinleme kararı olması, kendisinin de dinlenmesine yol açmakta ve hiçbir meşru karar olmadan mahremiyeti ihlal edilmektedir.

Mahremiyet ihlali Türk Ceza Kanununda suç olarak tanımlanmıştır. Hukuka aykırı olarak kişisel verileri kaydedenlerin cezalandırılması öngörülmüştür (TCK, Md. 135/1). Yine aynı Kanunda kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri hukuka aykırı olarak kişisel veri olarak kaydeden kimselerin cezalandırılacağı hükmü yer almaktadır. Bu suçlar, şikâyete bağlı suçlardır ve şikâyet olmadan savcıların kendiliğinden harekete geçmesi söz konusu olmaz. Hâlbuki dinlenen kişiler kendilerinin dinlendiğinin farkında değildir ve bu yüzden de şikâyetçi olmaları mümkün değildir. Bu durum ise hukuka aykırı dinleme yapanlara koruma sağlamakta ve teşvik edici olmaktadır. Dinlemelerin gizli olması, ilgili kurumları keyfi yollara başvurma eğilimine yol açabilmektedir. Bu keyfiliklerin önlenmesini sağlayacak güvencelerin temin edilmesi gereklidir.

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.

Kamusal bilgi sistemlerinde gittikçe daha fazla kişisel veri toplanması ve işlenmesi beraberinde bu verilerin güvenliği sorunlarını da getirmiştir. Bu sistemler, "hack" denilen bilgisayar ve internet korsanlıklarına karşı güvenlik açısından zaafiyetler sergilemektedirler. Güvenlik teknolojilerinin devamlı olarak geliştirilmesine rağmen, dışarıdan izinsiz saldırılarla kişisel bilgilerin kopyalanması veya değiştirilmesine dair örnek vakalar gözlenmektedir.

MERNİS Merkezi Nüfus İdare Bilgi Sisteminin adı olup İçişleri Bakanlığına bağlı Nüfus İdaresinin tüm işlemlerini gerçekleştirmek amacıyla proje edilmiştir (NVİ, 2010). 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 olumsuzluklar gözlenmiştir. 2004 yılında yapılan bir incelemede 77.756 kişiye

aynı vatandaşlık numarasının verildiği tespit edilmiştir. Aynı araştırmada sistemin, kurum personeli tarafından oluşturulan sanal kimliklere gerçek vatandaşlık numaraları vererek resmileştirebileceği gibi istismar olasılıkları tespit edilmiştir (Milliyet, 2006). Ayrıca, vatandaşlık numaralarının yaratılmasında kullanılan algoritmanın çözülerek vatandaşların tüm kişilik ve soy bilgilerine ulaşıldığına dair haberler ise endişe vericidir (Milliyet, 2010).

SEÇSİS (Seçmen Bilgi Sistemi) Programının hazırlanmasında bazı aksaklıklar olduğunu söylemek mümkündür. Seçmen Bilgi Sisteminin oluşturulmasında yeni bir veritabanı oluşturulması yerine MERNİS ve ADNKS verilerinin birleştirilip işlenerek oluşturulması, hem güvenlik ile ilgili tereddütler yaratmış, hem de bazı seçmenlerin listede yer almaması, ikamet yerlerinden uzak hatta başka illerdeki seçmen listelerinde yer alması, olmayan seçmenlerin ortaya çıkması gibi sakıncaları yaratmıştır. Esasen teorik olarak sanal programların mutlak güvenliğinden söz etmek mümkün değildir. Bu sistemde görülen aksaklıklar, hem seçimlerin meşruiyetinin sorgulanmasına yol açabilmekte; hem de seçmen-sandık sorgulama esnasında seçmenlerin kişisel bilgilerinin üçüncü kişiler tarafından elde edilmesi tehlikesini yol açmaktadır (Ketizmen ve Ülküderner, 2007).

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 bilgilerine ulaşılabilir. 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 vatandaşlık 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 erişmek mümkündür. Üçüncü kişilerin bu bilgileri, kredi kartı yolsuzlukları, sahte nüfuz cüzdanı çıkarmak, dolandırıcılık, sahte isimle şirket kurmak gibi pek çok illegal işlerde kullanması mümkündür.

Burada bahsedilen olumsuz örnekler, bilgi teknolojileri öncesinde de karşılaşılan durumlardır. Ancak bilgi iletişim teknolojileri kullanımı daha önce görülmedik çapta ve etkide olumsuz sonuçlar yaratacak istismar imkânları 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 (Hürriyet, 2009).

2- Kişisel Verilerin Korunması Hakkında Kanun Tasarısı

Kamu yönetiminde bilgi iletişim teknolojileri kullanımının etik yönünü kapsayan en kapsamlı ve önemli yasal girişim "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı"dır. Bu tasarı hazırlandığı andan günümüze değin yasalaşmamış olmakla beraber, bu zamana değin yapılan düzenlemeler de kısmi ve yeterli olmaktan uzaktır.

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 Gazetede yayımlanarak içselleştirilmiş BM İnsan Hakları Beyannamesinin 12. maddesi, 1982 Anayasasının 20, 21 ve 22. maddesi, CMUK'nda yer alan 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 Sözleşmesi'nin 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.

"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

a- Tasarının Olumlu Yönleri

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, 7- 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 soruşturmakla görevli olacaktır. Sorumlular hakkında savcılığa suç duyurusu ve doğrudan para cezası verme gibi yetkilere sahip olacaktır.

b- Tasarıya Yönelik Eleştiriler

Kanun tasarısı, vatandaşların tüm özel bilgilerinin ortak bir havuzda toplanmasını ve istisnai hükümlerle de olsa verilere ulaşımın kolaylaşmasını sağlamaktadır. Hâlihazır uygulamada her bir kamu kurumu kendi gereksinimi olan kişisel bilgilerin sadece belirli kısmını toplamaktadır ve bu bilgiler, ilgili kamu kurumu ölçeğinde bağımsız ve birbiri ile ilişkisiz sistemler içerinde kalmaktadır. 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 ulaşabilmesi mümkündür. Bu durum, sistemin siyasi iktidarlar tarafından istismar edilmesi ihtimali düşünüldüğünde daha vahim endişeler yaratmaktadır. Hâlbuki 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 imkân sağlamaktadır. Bu istisnalar net olarak tanımlanmadığından her düzeyde kamu görevlisinin kayıt altında işlenmesi yasak olan kişisel verileri öğrenmesi mümkün olabilir.

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 istisnalar hak ihlallerine zemin hazırlama riski taşımaktadır. 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.

III- Kişisel Verilerin Korunmasında Mahremiyet Etki Değerlendirmesi (MED)

Kamu yönetiminde bilgi iletişim teknolojilerinin giderek yaygınlaşması, mahremiyet sorunlarının da önemli boyutlara ulaşmasına yol açmıştır. Tarihsel sürece bakıldığında teknolojideki gelişmelerin pek çok fayda sağlamasının yanında beraberinde istenmeyen sonuçlar, etkiler veya yan ürünler oluşturduğu gözlenmektedir.

Toplumların modernleşme sürecinde yapılan düzenlemelerin, geniş ölçekli teknoloji uygulamalarının sonuçlarının kestirilmesinin gittikçe güçleşmesi ve ortaya çıkan olumsuzlukların tahribatının yüksek ve telafisinin zor olması karşısında yeni arayışlar söz konusu olmuştur. Yeni düzenleme, teknoloji uygulaması, proje, girişimlerden önce, olası olumsuz sonuçların uygulama öncesi sistemli bir şekilde gözden geçirilip tespit edilmesi ve tedbirlerin önceden alınması amacına yönelik olarak geliştirilen "etki değerlendirme" yöntemleri gittikçe yaygınlaşan bir uygulamadır.

Sanayi tipi üretim tarzının yaygınlaşması, kitlesel üretime geçilmesi süreci, doğal kaynakların çok yoğun şekilde kullanılması ve tüketilmesi sonucunu doğurdu. Öte yandan, kitlesel üretim sonucu ortaya çıkan istenmeyen ürünler ve yan etkiler, çevre kirliliğinin kitlesel boyuta ulaşmasına yol açtı. Sanayi üretiminden kaynaklanan çevre kirliliğinin sanayileşmiş ülkelerde hava, su ve toprak kirliliğine yol açması ve hatta kanser gibi hastalıkların olağanüstü artması ve kitlesel ölümlerin ortaya çıkması neticesinde çevre kirliliği sorununa karşı kapsamlı önlem arayışları kaçınılmaz oldu.

Çevresel etki değerlendirmesi, çevre sorunlarına yol açabilecek her türlü faaliyetin tasarlama ve planlama aşamasından başlayarak, işletme ve inşaat aşamasında ve faaliyetin sona ermesinden sonra meydana gelebilecek etkilerin, proje yapım kararı alınmadan önce incelenmesi, varsa olumsuz etkilerin önlenmesi, gerekli önlemlerin belirlenmesi, sürecin tüm uygulama aşamalarında çevresel etkilerin izlenmesi ve denetlenmesidir. Çevresel Etki Değerlendirme uygulaması, toplumsal açıdan önemli sonuçlar yaratacak diğer uygulamalar için de ilham kaynağı olmuştur. Bir politika, strateji programı veya projenin nüfusun ve nüfus gruplarının sağlığı üzerindeki etkileri değerlendirmeyi amaçlayan Sağlık Etki Değerlendirmesi; (Arık, 2007: 53); politika, program ve proje gibi planlı müdahale ve girişimlerin umulan ve beklenmeyen sonuçlarını analiz etme, izleme ve yönetme süreci olan Sosyal Etki Değerlendirmesi (Vanclay, 2003: 5); düzenleyici etki analizi gibi uygulamalar, ÇED uygulamalarının sağladığı gelişme örnek alınarak ortaya çıkmıştır. Bu örneklerden yola çıkarak gelişen ve karmaşıklaşan toplumlarda teknoloji kullanımının yaygınlaşmasıyla ortaya çıkan

mahremiyet sorunlarına benzer yöntemle çözüm aramak mümkündür

1- Mahremiyet Etki Değerlendirmesinin Tanım Ve Tarihi Gelişimi

Literatürde "Mahremiyet Etki Değerlendirmesi" (privacy impact assessment) kavramına 1980'lerden itibaren rastlanmaktadır ve ilk olarak 1990'lı yıllarda uygulanmaya başlanmıştır (Stewart, 2010). Bilgi iletişim teknolojilerinin mahremiyet etkisi boyutundan önce de "teknoloji etki değerlendirme" uygulamalarının var olduğu gözlenmektedir. Teknoloji etki değerlendirmesi uygulamalarına 1970'li yılların başından itibaren rastlanmaktadır (Clarke, 2004).

Kişi mahremiyetini etkileme ve zarar verme olasılığı olan bilgi iletişim sistemlerinin, süreçlerin, teknolojilerin, yasama faaliyetlerinin ve politikaların öncesinde uygulama esnasında ve uygulamadan sonra mahremiyet açısından kontrol edilmesine yönelik uygulama ve denetim mekanizmaları öncelikle ABD'de ortaya çıkmış; daha sonra gelişmiş ülkeler başta olmak üzere yaygınlaşmıştır. Mahremiyet etki değerlendirmesi, ABD, Kanada ve Yeni Zelanda, Avustralya gibi ülkelerde yaygın olarak uygulanmaktadır.

Kanada mahremiyet etki değerlendirmesini zorunlu kılan ilk devlettir. Bu ülkede kamu kurumlarının mahremiyetle ilgisi olabilecek tüm program ve hizmet önerileri için mahremiyet etki değerlendirmesinin yapılması zorunlu kılınmıştır. MED'in temel gerekçesi olarak e-Devlet sürecinde kişi mahremiyeti ve vatandaş güveninin korunması gösterilmektedir (GIPI, 2003: 7).

Bu ülkelerde, yeni teknoloji uygulamaları, sistem yükseltme, yeni politika ve yasa oluşturma süreçleri, idari düzenlemeler, geliştirilen MED prosedürleri ile olası mahremiyet risklerini belirlemek ve gerekli önlemleri almak amacıyla incelenir. Kamu kurumları kendi MED prosedürünü farklı ve kurumun özelliklerine göre düzenlemiştir. Yasama organları; sağlık, eğitim, maliye, içişleri, nüfus idareleri, ulaştırma bakanlığı, göçmenlik dairesi, ordu, dışişleri, tapu kadastro daireleri gibi kurumlar kendi kurumsal yapı ve işleyişlerine uygun MED uygulamalarını geliştirmişlerdir.

a- Mahremiyet Etki Değerlendirmesinin Tanımı

Mahremiyet Etki Değerlendirmesi kurumdan kuruma farklılıklar gösterse de, bireyin mahremiyeti üzerinde gerçek veya olası etkileri olacak olan eylem, öneri, teknoloji, sistem uyarlaması gibi süreçleri incelemek, sorunları tespit etmek ve sorunları giderici veya önleyici yolları belirleme sürecidir (Blair, 1996). Bu şekilde çevresel etki değerlendirme yöntemiyle baraj veya otoyolların çevresel etkilerinin belirlenmesi gibi kamu kurumları tarafından teklif edilen yasa önerileri, veri toplama ve bilgisayar projelerinin mahremiyet etkilerinin değerlendirilmesi mümkün olur.

ABD'de 2002 yılında kabul edilen e-Devlet kanununda MED, bilgilerin işlenmesinde yasal, idari ve siyasi mahremiyetin korunmasına uygun olarak işlenmesini sağlamak; verilerin toplanması, saklanması ve dağıtılmasındaki mahremiyet risklerini ve etkilerini belirlemek; olası mahremiyet risklerini azaltmak için gerekli güvenlik önlemlerini ve alternatif süreçleri incelemek ve değerlendirmek amacıyla gerçekleştirilen bir analiz olarak tanımlanmıştır (Whitehouse, 2010). Benzer ancak daha kapsayıcı bir tanım ise şöyledir: "Olası

uygulamaların mahremiyet etkilerini değerlendirme ve farkına varma süreci; bir öneri veya uygulamanın kişisel mahremiyet açısından yaratacağı sakıncaları ve bunları önleme yollarının değerlendirilmesi" (Stewart, 1996: 61).

Bilişim teknolojilerinin öncelikle gelişmiş ülkelerin kamu yönetimlerinde yaygınlaşmasıyla, yine bu ülkelerde ortaya çıkan mahremiyet sorunlarının öneminin fark edilmesiyle bu alanda düzenleme çabaları 1980'lerin başından itibaren gözlenmektedir. Bilişim uygulamalarının mahremiyet boyutunu gözeten ilk genel düzenleme, OECD tarafından 1980 yılında "Adil bilişim uygulamaları" adıyla ilkesel çerçeve şeklinde oluşturulmuştur (OECD 1980). OECD'nin belirlediği adil bilişim uygulamalarının ana ilkeleri şunlardır:

- Veri toplama sınırlılığı: işlemin tamamlanması için gerekenden fazla veri toplanmaması, verilerin hukuki ve amaçla uygun şekilde toplanması ve bireyin rızası ve bilgisi dahilinde toplanması.
- Veri kalitesi: toplanan kişisel verilerin kullanılan amaca uygun olması, tam, eksiksiz ve güncel olması.
- Amaç kısıtlaması: kişisel verilerin sadece beyan edilen amaçlar için kullanılması ve başka amaçlarla kullanılmaması.
- Kullanım kısıtlanması: kişisel verilerin, toplama amacı dışında kullanılmaması, bireyin rızası ve hukuki yetkiye dayanmadan açıklanmaması.
- Güvenlik: kişisel verilerin izinsiz erişim, kayıp, silinme, tahribat, tahrifat ve izinsiz erişime karşı yeterli güvenlik önlemleriyle korunması.
- Açıklık: veri toplama yöntemlerinin gizli olmaması. Veri toplama araçlarının açık ve bilinir olması; kişilerin veritabanları ve sorumlular hakkında bilgilendirilmesi.
- Bireysel katılım: bireylerin kendileri hakkındaki toplanan ve saklanan verilere ulaşma hakkına sahip olması. Bu hak, bireylerin verilerin kendilerine ait olup olmadığını onaylama, verilerin bir kopyasını alma, gerekli gördüğü takdirde itirazda bulunma, gerekli durumlarda verilerin silinmesi, düzeltilmesi ve tamamlanmasını isteme hakkı.
- Sorumluluk: Veri toplayan kişilerin sayılan ilkelere uymasını sağlayacak yasal yaptırımların olması.

Bu ilkeler, sonraki dönemlerde kamu kurumlarının kişisel verilerin toplanması süreçlerinde gerekli mahremiyet önlemlerini almada rehber çerçeve oluşturmuştur.

Kamu kurumlarında kullanıma giren bilişim sistemleri, yeni teknolojiler, sistem veya teknoloji yükseltilmesi, uygulamaya konulan yasa, politika ve idari kararların yanında henüz daha uygulamaya konmamış, teklif, öneri aşamasındaki yasama veya idari düzenlemelerle, kullanıma girmeden önceki yeni bilişim sistemleri veya teknolojilerin de mahremiyet etkileri bakımından incelenmesi sürecidir. Bu sayede uygulanması ve satın alınması söz konusu olan teknoloji, sistem, değişiklik ve teknolojiler, yasama ve politika taslaklarında yer alan mahremiyet sorunlarından kaçınılabilir ve sorunları önlemek için gereken çözümler tespit edilebilir.

MED uygulamasının kanun, düzenleme, proje ve politikaların henüz oluşturulup uygulamaya geçmeden önce kuruluş ve oluşturma aşamalarında gerçekleştirilmesi, yasa, politika, sistem ve teknolojilerin mahremiyet sorunları yaratmasını engeller, hatalı ve insan hakları ihlalleri içeren sonuçların engellenmesine yardımcı olur. Bu şekilde telafisi zor olan mahremiyet ihlalleri ortaya çıkmadan önlenmiş olur.

MED, projeler ve teknolojiler uygulamaya girdikten sonraki aşamalar için söz konusu olan "*uygunluk denetimi*"nden farklıdır. Uygunluk denetiminin konusu, yeni uygulamaya giren sistem veya teknolojilerin, mahremiyet yasalarıyla uyumlu olup olmadığı, herhangi bir mahremiyet ilkesiyle çatışma içinde olup olmadığının tespitidir. MED, mahremiyet mevzuatına uygunluğun denetiminin yanında mahremiyet olasılıklarını belirleyerek, uygulama esnasında bariz eksikliklere karşı çözüm önerileri sağlayarak yasal denetimin ötesinde karar alıcılara proje veya programlar hakkında tam bilgi sağlar.

MED süreci kurumdan kuruma göre farklılıklar gösterse de şu beş aşamadan oluşur:

- Projenin tanımlanması: projenin amaçları ve kişisel verilerin toplanıp toplanmayacağını da kapsayan genel bir değerlendirme;
- Enformasyon akışının ve mahremiyet çerçevesinin belirlenmesi: Projede kişisel veri akış şemasının ve ilgili tüm yasal ve kurumsal mevzuatın tespit edilmesi;
- Mahremiyet Etki değerlendirmesi: Projenin mahremiyet etkilerinin belirlenmesi ve analizi;
- Mahremiyet yönetimi: Mahremiyet etkilerinin nasıl yönetileceği ve mahremiyet korunurken projenin amaçlarının da gerçekleştirilmesini sağlayacak alternatiflerin belirlenmesi;
- Tavsiyeler: Yukarıdaki aşamaları ve tavsiyeleri de içeren nihai MED raporunun hazırlanması (PIAG, 2010: xiv).

b- Mahremiyet Etki Değerlendirmesinin Amacı

Mahremiyet etki değerlendirmesinin öncelikli amacı, bir örgütsel yapının veya kişisel bilişim sisteminin ilgili veri koruma mevzuatına uygun olup olmadığını denetlemektir. İkinci bir amaç olarak da toplumun mahremiyet ve kişisel verilerinin korunmasına yönelik beklenti ve taleplerine yanıt vermektir (Flaherty, 2000: 85). Gerekli testlerden ve denetimden geçmediği için mahremiyet sorunlarına yol açan bir sistem veya teknolojik yapılanma, çok önemli yararlar sağlasa da kullanışlı değildir. Ortaya çıkardığı mahremiyet sorunları ve sosyal maliyetler, etkinlik ve verimlilik gibi kazançlarının önüne geçebilir ve sağladığı yarardan çok daha fazla zarara yol açabilir. Bu bakımdan kişisel verilerle ilgili düzenleme, yapılanma ve teknolojilerin önceden denetimden geçirilmesi zaruridir.

MED'in bir başka amacı da yönetici personel ve bağımsız veri koruma kurumlarının, sistem operatörlerinin eğitiminde ve yönetilmesinde kullanmak üzere araçlar sağlamaktır. Mahremiyet etki değerlendirmesi amir ve personelin sistemin nasıl çalıştığını ve mahremiyet risklerinin neler olduğunu anlamalarına imkân sağlar.

2 - Mahremiyet Etki Değerlendirmesinin Süreci Ve Uygulama Alanları

MED, her türlü e-devlet uygulamasında, kamu yönetiminde kullanılacak tüm sistem yazılım, teknoloji uygulamalarında ve mahremiyet ile ilgili tüm yasama ve idari faaliyetlerde kullanılabilir. Ana hatlarıyla MED şu alanlarda gerçekleştirilmelidir:

- Kamusal veri tabanları oluşturulmasında, var olan veri tabanlarının birbirileriyle irtibatlandırılmasında veya kamusal kayıtların daha büyük kayıt sistemi şeklinde bütünleştirilmesinde;
- Yeni geliştirilen ve uygulamaya konulan izleme, takip sistemlerinde;
- Ulusal kimlik kartlarının uyarlanması önerilerinde veya var olan sistemlere yeni biyometrikler eklenmesinde, kolluk güçlerine bilgisayar sistemlerine ulaşım konusunda yeni yetkiler öneren tekliflerde;
- Özel sektör ve ticari şirketlerin kişisel verileri toplamasını gerektiren yeni kanun önerilerinde (örneğin mobil telefon şirketlerinde hat satın alan kullanıcıların kimlik verilerinin şirket tarafından alınması ve kamu kurumlarına bildirilmesini zorunlu kılan yasal düzenlemelerde);
- Kamu personel tanımlayıcı işaretlerin kullanılmasında;
- Yeni veri tabanlarının oluşturulmasında veya kişisel veri içeren veri tabanlarının kapsamlarının genişletilmesinde veya erişim yetkisinin genişletilmesinde;
- Var olan kamu programlarında köklü değişimler öneren planlarda;
- Büyük ölçekli donanım ve yazılım geliştirilmesi ve yükseltgenmesi süreçlerinde;
- Kamusal alanların kapalı devre televizyon yayını ile izlenmesinde (MOBESE vb);
- Otoyol ücret toplama sistemlerinin oluşturulmasında.

MED uygulamasının formel çıktısı "Mahremiyet Etki Değerlendirmesi Raporu"dur. MED, uygulandığı kurumlara göre farklılıklar gösterse de büyük ölçüde ortak bileşenler tespit etmek mümkündür (Privacy.org, 2010). Bunlar;

- Projenin amaçları ve hangi tür kişisel verilerin toplanacağını kapsayan genel bir değerlendirme
- Kullanılan değerlendirme süreçleri ve hedef kurumun mahremiyet politikalarını tespit eden bir inceleme,
- Kişisel verilerin belirli kategorilerine kimlerin erişim yetkisine sahip olduğunun belirlenmesi ve sadece görevle ilgili erişimin sağlanması. Sürece her türlü yetkisiz erişimin engellenebilmesi,
- Yeni proje ve uygulamaların bireysel mahremiyet üzerinde ne kadar etkili olduğunun belirlenmesi. Mahremiyetle ilgili kanun, uluslararası düzenlemeler ve politikalar ile çatışma ve ihlallerinin belirlenmesine yönelik analizler,
- Belirlenen mahremiyet risklerini listeleyen bir risk değerlendirmesi ve bu risklerin projenin başarısı ve bireyleri nasıl etkileyeceğinin analizi,

- Mahremiyeti koruyacak veya destekleyecek teknik, süreç veya diğer koruma önlemlerinin değerlendirilmesi.

3- Mahremiyet Etki Değerlendirmesinin Yararları

Kamu kurumları yasalara uygun faaliyet göstermek zorundadır. Günümüzde mahremiyetle ilgili pek çok yasal düzenleme vardır. MED uygulaması, kurumların ve uygulamaların mahremiyet mevzuatına uygun faaliyet göstermesine, yasa ihlallerinden kaçınmasına yardımcı olur. MED süreçleri kişisel verilerin mahremiyet hakkına zarar vermeden nasıl işleneceğine dair talimatları içerir. Bu şekilde kurumların gerekli düzenlemeleri yapmaları da mümkün olur.

Mahremiyet yasalarına uygunluğun sağlanması, mahremiyet etkilerinin yönetilmesinde temel amaçtır. Ancak sadece yasalara uygunluk yeterli değildir. İnsanlar genellikle mahremiyetleri konusunda hassastır. Mahremiyet, insan onurunun bir parçası olmakla birlikte dış dünya ile ilişkilerde kişisel bilgilerin ne kadarının bilineceğinin belirlenmesini sağlar. Kamuoyu kişisel mahremiyetin korunması konusunda duyarlıdır ve mahremiyet ihlalleri karşısında hoşnutsuz olur. Ayrıca insan hakları konusunda gelişmeler, toplumların mahremiyet konusundaki hassasiyetlerini de arttırmaktadır.

Bireyler kişisel gereksinimleri ve amaçlarıyla mahremiyetleri arasında denge kurmak isteğindedirler. Bu bakımdan kendileri hakkında başkaları tarafından bilinecek kısmı ve miktarını belirlemek eğilimindedirler. MED uygulamaları kurumların mahremiyet, güven, dürüstlük, saygı, kişisel özgürlükler ve sorumluluklar gibi toplumsal değerlerin gözetilmesine katkı sağlar.

Öte yandan, MED, projelerin amacına uygun mahremiyet çözümleri geliştirmesine imkân sağlar. İşlevsel aksaklıklar, yeni teknolojiler ve yasal düzenlemelerden kaynaklanan sorunların tespit edilmesini mümkün kılar. Projelerin konsültasyon süreçlerinin geliştirilmesine, mahremiyet sorunlarının karşılaştırmalı olarak tanımlanmasına ve kamuoyunun süreç konusunda daha iyi bilgilendirilmesine imkan sağlar.

İleri aşamalarda projenin mahremiyet risklerinin nasıl yönetileceğine dair tartışmalar açısından MED raporu ve tavsiyelerin kamuya açık olarak yapılması gereklidir. MED bulgularının kamuya açıklanması, yeni sistemi uygulayacak olan kamu kurumuna olan güven ve desteği artırır. Raporun daha geniş kitlelere ulaşması, teknik bilgisi yetersiz olanlar tarafından kolay anlaşılacak şekilde ifade edilmelidir. Bulguların kamuya açıklanmasına ilave olarak bazı durumlarda kamusal konsültasyonlar da tavsiye edilebilir.

Taslak şablon, mahremiyet etkisi olabilecek yasa önerisi, proje, program,, sistem yükseltme, bilişim uygulamaları gibi süreçlerden sadece yeni bir sistem uygulanması süreci için geliştirilmiş çerçeve bir taslak rapor olarak geliştirilmiştir. Farklı kurumlarda yasa önerileri, projeler, girişimler, programlar, teknoloji yükseltme, sistem entegrasyonları süreçleri için farklılıklar göz önüne alınarak farklı MED şablonları geliştirmek, yöntemin doğası gereği daha yararlıdır. Örnek taslağın hazırlanmasında ABD içişleri Bakanlığının MED taslağı (Homeland Security, 2012), AB Maliye Bakanlığı MED taslağı (OMB, 2012)

kaynaklarında yararlanılmıştır.

Mahremiyet Etki Değerlendirmesi İçin Taslak Şablon

Sorular	Açıklamalar
-Sistemin kullanılacağı kurum:	İlgili kurum adı
-Sistem sahibi, yetkilisi, analizcisi, geliştiricileri	Sistemi gerçekleştiren, geliştiren ve kullananların isimlerin listelenmesi
-Kişisel veri kullanımı gerektiren /etkileyen sistem tanımı	Öneri, sistem, proje veya girişimin ve sistemde kullanılacak verilerin kısaca tanımlanması
-Sistem hangi aşamada?	Seçim, dizayn/planlama, geliştirme/uygulama, işletme/bakım vb aşamalarından hangisinde olduğunun açıklaması
-Sistemin bilgi kaynakları nelerdir?	Sistem girdisi verilerin nereden sağlandığı; kullanıcılardan mı sağlandığı veya başka sistemlerden otomatik olarak mı elde edildiği.
-İlgili kurumun hangi bilgileri ve veritabanları kullanılacak?	Kurumun sahip olduğu hangi veriler veya veritabanlarının veri kaynağı olarak kullanılacağı
-Sistemin kullanımı için hangi kurumlar veri sağlayacak?	Sisteme veri sağlayan kurumların listesi
-Veri toplanacak üçüncü taraflar?	Var ise üçüncü tarafların listesi
-Hangi kişisel veriler sisteme kayıt edilecek?	Bireylerden toplanacak verilerin listesi (isim, yaş, adres, vatandaşlık no vs.)
-Kamu kurumları haricindeki kaynaklar ve bireylerden verilerin nasıl toplanacağı ve verilerin güncelliğinin nasıl sağlanacağı	Kişisel verilerin güncelliğinin, geçerliliğinin ve güvenilirliğinin nasıl sağlanacağının açıklaması
-Verilerin güvenilirliğinin nasıl kontrol edileceği	Verilerin tam, doğru ve eksiksiz olmasının nasıl sağlanacağının açıklaması
-Verilerin birleştirilmesi, güncelleştirilmesinde ve yetkisiz erişim durumlarında alına tedbirler nelerdir?	Veri güncellemesi söz konusu ise alınacak tedbirler ve yetkisiz kişilerin erişimine karşı alınan önlemlerin anlatılması
-Verilerin birleştirilmesi, işlenmesi, diğer sistemlere servis edilmesinde olası mahremiyet etkileri nelerdir ve alına önlemler nelerdir?	İlgili durumlarda bireylerin mahremiyet haklarının nasıl korunacağının açıklanması. Mahremiyetin korunmasına dair tedbirleri listesinin açıklanması
-Sistemin bireylere adil ve eşit muamele etmesinin nasıl sağlanacağını açıklayınız?	Sistemin kişi ve kişisel verileri işlerken eşit ve adil davranmasını sağlayacak tedbirlerin açıklanması
-Veriler sistemde hangi sürelerle saklanacak?	Sistemde hangi verilerin ne kadar süre ile saklanacağı. Güncelliği geçen verilerin arşive alınıp alınmayacağı gibi saklama süreçlerinin açıklanması
-Sistem daha önce kamu kurumlarında kullanılmayan yeni bir teknoloji mi?	Evet ise, veri toplama ve işleme teknolojilerini açıklanması
-Sistem bireylerin yerini tespit etme ve izleme imkanı sağlıyor mu?	Evet ise bireylerin izlenmesi ve yer tespiti süreçlerinin gerekçelerinin açıklanması
-Sistemin dayandığı yasal mevzuat nelerdir?	Sistemin dayanağı olan kişisel veri mevzuatının sayılması
Sistem toplanan verilerden daha önce mümkün olmayan kişisel veriler türetebiliyor mu?	Daha önce elde edilmesi mümkün olmayan, ancak sistem sayesin de toplanan verilerden türetilen yeni kişisel olarak tanımlanabilir verilerin açıklanması.

4- Mahremiyet Etki Değerlendirmesi Uygulamasında Olası Sorun Alanları

Mahremiyet etki değerlendirmesinin kurumsal yapı ve işleyişi ile ilgili olarak bazı olumsuzluklar ve çatışma alanları söz konusu olabilir. Bu sorun alanlarının bilinmesi, kurumsal yapılanma, MED'in uygun konumlanması ve işleyişinde gerekli tedbirlerin alınması bakımından önemlidir (Bamberger ve Mulligan, 2008).

Kişisel verilerin mahremiyetine dair süreçlerin eksik uygulanması, mahremiyet etkisi olabilecek yasal düzenlemelerin gerekli detayı içermemesi, dolayısıyla idareye geniş takdir yetkisi verilmesi durumlarında çatışma alanlarının oluşması kaçınılmazdır. Güçler ayrılığında yasama, yürütme ve yargı erklerinin temsil yetkisi ve idari sorumluluğu sağlama ve denetleme bakımından çatışmalar söz konusu olabilir.

- Yasaların gerekleriyle çatışma: Yasama organında genel olarak düzenlenmiş yasalarla idareye verilen görevler, kamu bürokrasisine geniş takdir yetkisi sağlanması anlamına gelir. Bürokrasiler yasada belirtilen birincil amaçlara odaklanırken, mahremiyet boyutunu ihmal edebilirler. Kurumlara verilen mahremiyeti gözetme gibi ikincil görevler ve talimatlar, kurumun asli amaçlarıyla çatışma içine girebilir. Yasama organından çıkmış bir yasayı her kurum farklı derecelerde uygulayabilir. Dolayısıyla MED süreçleri de kurumlar tarafından farklı şekillerde uygulanabilir.

- Denetim önündeki engeller (Bamberger ve Deindre, 2008: 85): Yasama ve yürütme organları kamu bürokrasileri üzerinde önemli denetleme araçlarına sahiptirler. Meclis, komiteler ve bütçe denetimi, meclis araştırması gibi yollarla kanunların idare tarafından uygulanmasını denetleme gücüne sahiptir. Bunun yanında yargı da, yargısal denetim yoluyla bürokrasi üzerinde güçlü bir denetim uygulama imkânına sahiptir. Ancak bununla birlikte MED süreçlerinin ağırlıklı olarak teknolojiye dayalı olmaları, denetlenen sistem ve teknolojilerin karmaşık ve sofistike nitelikte olması, teknoloji hakkındaki kararların net olmaması gibi olumsuz etkenler, bu denetim yollarını zayıflatmaktadır.

Kamuoyunda kişisel verilerin istismarına dair endişeler bilişim teknolojilerinin yaygınlaşmasıyla paralel olarak gittikçe artmaktadır. Ancak mahremiyet konulu siyasi kararlar, etkinlik ve güvenlik endişeleri ile zafiyete düşebilir. Kamu yönetiminde etkinlik, verimlilik, asayiş ve ulusal güvenlik ile ilgili endişeler, siyasi karar alma süreçlerinde kişisel verilerin mahremiyetinin ihmal edilmesine ve zarar görmesine yol açabilir. Siyasi kurumların talimatları ve hedeflenen amaçlara ulaşma endişesi ile mahremiyet ihlallerinden kaçınma gereği çatışma alanları yaratabilir. Mahremiyet ile güvenlik uygulamaları arasındaki denge durumunda, mahremiyet hakkına ağırlık verilirse bu defa önemli toplumsal güvenlik zaafiyetleri söz konusu olacaktır. Öte yandan güvenlik ve asayiş politikaları da kişi mahremiyeti bakımından önemli ihlallere yol açabilir. Örneğin ABD'de kişi mahremiyetinin korunması amacıyla FBI ve CIA'in bazı yetkilerinin kısıtlanmasının 11 Eylül saldırılarının en temel gerekçesi olduğunu savunan iddialar, bu yaklaşımı destekler niteliktedir (Bamberger ve Deindre, 2008: 86).

E-devlet süreçlerinde genellikle mevzuatta MED uygulaması açıkça öngörülse dahi, kamusal, danışma ve istişare eksiklikleri söz konusu olmaktadır. Bir kamu kurumuna bilişim uygulamaları ve teknolojisine geçiş yolunda bir siyasi talimat verildiğinde, bilişim sistemlerinin alımı veya geliştirilmesi genellikle bir idari mesele olarak ele alınır ve bu süreçte daha çok informel araçlar kullanılır. Böylelikle teknoloji satın alınıp uygulanıncaya kadar mahremiyet etki değerlendirmesi veya başka kamusal denetim türüne açık olmaz.

E-devlet sürecinde karmaşık teknolojiler arttıkça, uzman teknokratlar ve teknolojik birimler üzerinde denetim zayıflamaktadır. Sofistike ve karmaşık teknolojiler, kullanılan teknik dil, anlamayı ve erişmeyi zorlaştırmaktadır. Teknolojiler genellikle değerler bakımından "nötr" olarak bilinir. Ancak uzmanlık bilgisine sahip teknokratlar, teknik karmaşıklığın arkasına sığınarak kendi değerlerini veya politikalarını sisteme empoze etme niyetlerini gizleyebilirler. Teknolojik sistemin kişi mahremiyetini ihlal edici uygulama ve özellikleri, sistemi geliştiren teknokratlar tarafından "sistemin öyle gerektirdiği, kaçınılmaz olduğu" gibi gerekçelerle müdafaa edilebilir. Kamu bürokratlarının ise kendiliğinden kişi mahremiyetini koruma eğiliminde olacağını söylemek ise mümkün değildir.

Bu konuda ilginç bir örnek ABD'de e-pasaport uygulaması sürecinde pasaportlarda RFID teknolojisinin kullanılmasıdır. Güvenlik ve etkinlik gibi gerekçelerle, Amerikan pasaportlarının sayfalarına kullanıcının kişisel verilerinin RFID[1] teknolojisine dayalı mikro-çipler yerleştirildi (Bamberger ve Deindre, 2008: 95). Süreçle ilgili MED uygulamaları da gerçekleştirilmesine rağmen uygulama aşamasına geçinceye değin mahremiyet risklerini tespit etmek mümkün olmadı. Pratikte ise pasaport sayfalarına iliştirilmiş mikro-çiplerde kişisel verilen toplandığı; çipe erişim ile kişisel verilerin tümüne erişimin mümkün olduğu; hatta RFID teknolojisi sayesinde pasaporta dokunmadan dahi çipteki verilere uzaktan erişmenin mümkün olduğu görüldü. Bunun üzerine Amerikan Standartlar ve Teknoloji Enstitüsü'nün (NSID) gerçekleştirdiği kapsamlı MED çalışması ise tatmin edici sonuçlar elde edilememiş ve henüz sorun tam anlamıyla çözülememiştir.

Sonuç

Kamu yönetiminde bilgi ve iletişim teknolojisi uygulamaları hızla yayılmaktadır. Bu elektronikleşme süreci hem kamu kurumlarının yapılarında, işleyişleri ve hizmet sunumlarında ortaya çıkmaktadır. Kamu hizmetleri sanal ortamda sunulmakta, kişisel veriler elektronik ortamlarda toplanmakta, saklanmakta, işlenmekte ve dağıtılmaktadır. Bu süreçte vatandaş-devlet ilişkilerinde boyut değiştirmektedir. Vatandaşlar, web siteleri vasıtasıyla kamu kurumlarıyla sanal ortamda iletişim kurmakta ve hizmet almaktadır.

[1] RFID (Radio Frequency Identification). Radyo frekansı ile tanımlama.. Üzerinde mikroişlemci ile donanmış etiket taşıyan bir nesnenin, bu etiketteki kimlik yapısı ile hareketlerinin izlenebilmesine imkân veren teknoloji (Yüksel ve Odabaşı, 2009).

Özellikle kamu yönetiminde uygulamaya giren teknoloji, sistem ve yazılımların ne tür eksik, hata ve sakıncalarının olduğunu önceden kestirmek mümkün değildir. Bu sakıncaların en başında kişi mahremiyeti gelmektedir. Genellikle hata, eksik ve açıklar telafi edilemez sonuçlar doğurduktan sonra fark edilmektedir.

E-devlet sürecinde kişi mahremiyetine daha önceden var olmayan mahremiyet tehditleri ortaya çıkmaktadır. Kişilerin mahremiyetleri gittikçe daha fazla zarara görebilir hale gelmiş, mahremiyet tehditleri artmıştır. Mahremiyetin korunmasına yönelik klasik tedbirler ve yaptırımlar artık etkisini yitirmiştir.

Parçalı ve entegre olmayan teknik, hukuki ve siyasi tedbirler ve riskleri giderme sürecinde tepkisel yaklaşımlar yeterli değildir. Bu bakımdan kamu yönetiminde bilgi teknolojisi uygulamalarında, yasal ve siyasi düzenlemelerde süreçlerin uygulamaya girmeden önce, olası mahremiyet sakıncalarını ve olası riskleri belirlemek, gerekli önlemleri almak amacıyla mahremiyet etki değerlendirmesi uygulaması, gecikmeden benimsenmesi gereken yararlı bir yöntemdir.

Her kamu kurumunun kendine özgü mahremiyet etki değerlendirmesi standartları hazırlamak amacıyla oluşturulacak temel ilkelerin belirlendiği rehber çerçeve yol gösterici ve kolaylaştırıcı katkı sağlayacaktır. MED uygulamasını benimsemiş Kanada, ABD gibi ülkelerde bu rehber çerçeveler, Gelirler İdaresi (ABD), Hazine bakanlığı gibi kurumlar tarafından önceden hazırlanmıştır (Flaherty, 2000). Ayrıca NASA gibi tamamen teknoloji odaklı kuruluşlar ise kişisel olarak tanımlanabilir verilerin korunmasına dair çerçeve talimatlar yanında, her aşama ve teknoloji için farklı MED süreçleri geliştirmektedirler (NASA, 2008). Amerikan Nüfus İdaresi (Census Bureau) gibi kritik kişisel veri barındıran kurumlar ise kayıt altındaki verilerin güvenliği ve doğruluğu ile şeffaflık, etkinlik ve verimlilik gibi değerler arasında denge sağlayacak özenli MED süreçleri düzenlemektedir (Census Bureau, 2010).

Günümüzde kamusal uygulama ve düzenlemelerin öngörülen etki ve sonuçlarının yanında beklenmeyen olumsuz etki ve olumsuz sonuçlarının kestirilmesi gittikçe daha güçleşmekte, geleneksel yöntemler ise yetersiz kalmaktadır. Bu ihtiyaç neticesinde ortaya çıkan "etki değerlendirme" uygulamaları anlayışı temeline uygun olarak mahremiyet etki değerlendirmesi yöntemi gittikçe daha gerekli hale gelmektedir.

KAYNAKÇA

ADÜ (2012) http://www.adu.edu.tr/tr/index.asp?job=news&i=25735

AGOPC (2006) "Privacy Impact Assessment Guide", *AGOPC*, www.privacy.gov.au (12.3.2010)

Aktaş, Nail (2003) "Karmaşıklık Bilimleri: Kaosun Kıyısında Bilim ve Yönetim", (Editörler: M. Acar ve H. Özgür), *Çağdaş Kamu Yönetimi -I*, Nobel Yayın Dağıtım, Ankara, ss. 45-74.

Arık, Hale (2007) "Sağlık Etki Değerlendirmesi; Teknik mi, Politika mı?" *Memleket-Mevzuat Dergisi,* YAYED, Cilt 3, Sayı 27, ss. 53-59.

Başbakanlık (2008) http://www.basbakanlik.gov.tr/Forms/pDraftOfALaw.aspx (12.10.2010).

Bamberger, Kenneth A. and Mulligan, Deirdre (2008) "Privacy Decisionmaking in Administration Agencies", *Chicago Law Review*, Vol. 75, No. 1, pp. 75-107.

Bayındırlık (2012) https://www.bayindirlik.gov.tr/gm/ced/ (2.6.2012)

Bayri, Osman (2003) "Kamu Yönetimi ve Örgütlenmesinde Sistemsel Bir Yaklaşım", (Editörler: M. Acar ve H. Özgür), *Çağdaş Kamu Yönetimi -I*, Nobel Yayın Dağıtım, Ankara.

Blair, Stewart (1996) "Privacy Impact Assessment", *Privacy Law and Policy Reporter*, http://www.astlii.edu.au/au/journals/PLPR/1996/39.html (2.3.2010).

Census Bureau (2010) "An Introduction to the Census Bureau's Privacy Impact Assessments (PIA)", *U.S. Census Bureau*, http://www.census.gov/po/pia/pia_intro.html (12.3.2010).

Clarke, Roger (2004) "A History of Privacy Impact Assessments", http://www.rogerclarke.com/DV/PIAHist.html (3.3.2010)

Eryılmaz, Bilal (2010) *Kamu Yönetimi*, Okutman Yayıncılık, İstanbul.

Flaherty, David H. (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States,* University of North Carolina Press, Chapel Hill.

Flaherty, David H. (2000) "Privacy Impact Assessments: An Essential Tool for Data Protection", *Privacy Law and Policy Reporter*, No. 2000/45, pp. 85-104.

Franks, Daniel (2012) "Social Impact Assessment of Resource Projects", *International Mining for Development Centre*.

http://im4dc.org/wp-content/uploads/2012/01/UWA_1698_Paper-02_Social-impact-assessment-of-resource-projects1.pdf (31.5.2012)

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

GIPI (2003) "Privacy and E-Government: Privacy Impact Assessment and Privacy Commissioners: Two Mechanisms for Protecting Privacy to Promote Citizen Trust Online" *GIPI,* http://www.internetpolicy.net/practices/030501pia.pdf (12.2.2010), pp. 1-11.

Harris, Amanda (2012) Hızlı Sağlık Etki Değerlendirmesi Araştırma Rehberi, New Deal for Communities, Nottingham.

Homeland Security (2012) http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_template.pdf

Hürriyet (2009) "687 Bin Öğretmenin Kimlik Bilgileri Çalındı", *Hürriyet*, (12.2.2009)

Kaymak, Hasan (2004) "Düzenleyici etki Analizi", *Maliye Dergisi*, Sayı 146, ss. 107-131.

Ketizmen, Çağlar ve Ülküderner, Muammer (2007) "E-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması", *XII. "Türkiye'de İnternet" Konferansı*. http://inet-tr.org.tr/inetconf12/bildiri/2.pdf

Küçükyumuk, Mehmet (2012) *Yerel Yönetimler ve Etki Değerlendirmesi Çalışmaları*, http://www.belgeler.com/blg/29nt/yerel-yonetimler-ve-etki-degerlendirmesi-calismalari

Milliyet (2006) "MERNİS Skandalı", *Milliyet* (11.12.2006)

Milliyet (2010) "TC Kimliklerinin Algoritması Çözüldü", *Milliyet* (4.8.2010).

Misra, Vivek (2012) "Social Impact Assessment Methodology", SASANET, http://www.sasanet.org/documents/Tools/Social%20Impact%20Assessment%20Methodology.pdf (31.5.2012).

MOBESE (2012) İstanbul Emniyet Müdürlüğü, http://mobese.iem.gov.tr/ (6.6.2012)

NASA (2008) "Rules and Consequences Policy Relative to Safeguarding Personally Identifiable Information (PII)", *NASA*, http://www.nasa.gov/pdf/209815main_NITR-1382-2-NASA-PII-Rules-Consequences-Policy.pdf (12.3.2010)

Nilüfer (2012) "Sağlık Etki Değerlendirmesi (SED)", http://www.nilufer.bel.tr/alt/index.php?o=4&i=goster&id=40 (30.5.2012)

NVİ (2010) *MERNİS Projesi*, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, www.nvi.gov.tr (12.2.2010)

OECD (1980) "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (30.5.2012).

OECD (1995) Recommendation of the Council of the OECD on Improving the Quality of Government Regulation, OECD. http://www.oecd.org/officialdocuments/displaydocumentpdf/?cote=OCDE/GD(95)95&doclanguage=en (24.5.2012)

OMB (2012) http://www.whitehouse.gov/omb/memoranda_m03-22

Overman, E. S. and Lorraine, D. T. (1994) "Information for Control: Another Management Proverb?", *Public Administration Review*, Vol. 54, No. 2, pp. 193-196.

Overman, E. Sam (2012) "The New Science of Management: Chaos and Quantum Theory and Method", *Journal of Public Administration and Theory*, Vol. 22, No. 2, pp. 75-89.

Ökem, Z. Güldem (2008) "İlaç Geri Ödeme Kriterleri, Kanıta Dayalı Yöntem", *Sağlık Sektörü Çalıştayı*, 12 Kasım 2008, TOBBB-Ekonomi ve Teknoloji Üniversitesi Ankara.

PIAG (2012) *Privacy Impact Assessment Guide*, Australian Government Office of the Privacy Commissioner, Sydney.

Privacy.org (2010) "Privacy Impact Assessment Handbook", http://www.privacy.org.nz/comply/pia.html. (10.3.2010)

Sağlık (2012) Sağlığın Teşviki ve Geliştirilmesi Alanındaki Değerlendirmeler, Sağlık Bakanlığı ve DSÖ, http://sbu.saglik.gov.tr (30.5.2012)

Saylı, Halil (2008) "Geleneksel Yönetim Paradigmasının Sınırlayıcı Alanlarına Karşı Post-Modern Yönetim Paradigmasının Geliştirici Alanları", *Afyon Kocatepe Üniversitesi, İİBF Dergisi*, Cilt 10, Sayı 2, ss. 180-200.

SGB (2008) *Yasa Hazırlama Sürecinde Etki Değerlendirmesi*, Finlandiya Adalet Bakanlığı, (Çev.: Sami Sarvilinna ve Edite Oyj), www.sgb.gov.tr (30.5.2012)

SKPO (2012) *Sağlık Etki Değerlendirmesi*, http://skpo.izmir.bel.tr/UserFiles/File/saglik%20etki%20degerlendirmesi.pdf (28.5.2012)

Stewart, Blair (1996) "Privacy Impact Assessment", *Privacy Law & Policy Reporter*, Vol. 3, No. 4, pp. 61-64.

Stewart, Blair (2010) "Privacy Impact Assessment: Towards a Better Informed Process for Evaluating Privacy Issues Arising from New Technologies (1)", http://www.privacy.org.nz/privacy-impact-assessment-towards-a-better-informed-process-for-evaluating-privacy-issues-arising-from-new-technologies-1/?highlight=pia

Tataroğlu, Muhittin (2009) "E-devlette Kullanılan Gözetim ve Kayıt Teknolojilerinin Mahremiyet Üzerinde Etkileri, *Abant İzzet Baysal Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi*, Sayı 2009/1, ss. 95-120.

Teh, Jeanette (2001-2002) "Privacy Wars in Cyberspace: An Examination of the Legal and Business Tensions in Information Privacy", *Yale Journal of Law & Technology*, Vol. 2001-2002, pp. 4-96.

Üstün, S. ve Büyükgüngör, H. (2003) "'Çevresel Etki Değerlendirmesi (ÇED)' Uygulamaları ve Sorunları", *V. Ulusal Çevre Mühendisliği Kongresi*, Ankara, ss. 506-513.

Vanclay, Frank (2003) "International Principles for Social Impact Assessment", *Impact Assessment and Project Appraisal*, Vol. 21, No. 1, pp. 5-11.

Whitehouse (2010) http://www.whitehouse.gov/omb/memoranda_m03-22/ (10.2.2010)

Yüksel, Mehmet (2003) "Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar", *Ankara Üniversitesi, SBF Dergisi,* Cilt 64, Sayı 1, 276-298.

Yüksel, M. Erkan ve Odabaşı, Şafak D. (2009) "Nesneler İzlenebilir ve Yönetilebilir mi? Çözüm: RFID", *Akademik Bilişim,* Harran Üniversitesi, 11-13 Şubat 2009. www.ab.org.tr/ab09/bildiri/163.pdf (12.3.2010)