Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi, Cilt 16, Sayı 2, 2007, s.219-236

E-DEVLET UYGULAMALARINDA BİLGİ VE PAYLAŞIM GÜVENLİĞİ

Öğr. Gör. Akın EFENDİOĞLU
Çukurova Üniversitesi
Eğitim Fakültesi
İlköğretim Bölümü
e-posta: eakin@cu.edu.tr

Öğr. Gör. Emre SEZGİN
Çukurova Üniversitesi
Eğitim Fakültesi
Bilgisayar ve Öğr. Tekn. Eğt. Bölümü
e-posta: esezgin@cu.edu.tr

ÖZET
Günümüzde bilişim teknolojileri pek çok alanda etkisini göstererek ilerlemektedir. Bu alanlardan birisi de devlet yönetimidir. Her sektörde artan bilgi ve hizmet ihtiyacı hızlı bir şekilde karşılanmalıdır. E-devlet; devlet-vatandaş, devlet-iş dünyası ve devlet-devlet arasında açık bir iletişim sağlanması için kullanılan bir hizmet uygulamasıdır. Kamu kurum ve kuruluşlarının, vatandaşların ve özel kurumların bilgilerinin saklandığı bu uygulama büyük bir veri bankası gibi düşünülebilir. Vatandaşlar bu veri bankasından hizmet alırken istenilen/istenilmeyen birçok bilgiye erişebilmektedir, ancak bu durum bazı sorunları da beraberinde getirmektedir. Bilgiye erişimin belirli kurallara bağlanması, bilginin güvenliği ve gizliliği açısından bir zorunluluk olmalıdır.

Anahtar Sözcükler: e-devlet, bilgi ve paylaşım güvenliği, e-devlette bilgi gizliliği, e-devlette bilgi güvenliği.

ABSTRACT
Nowadays, the effects of information technologies are increasing and seen at lots of areas. One of these areas is public management. The needs for information and service increasing at all areas are must be met. E-government is a kind of public service that provides an open communication between government-citizen, government-business areas and government-government. E-government may be imagined as a large data base in which the informations of citizens, public and private institutions or foundations are stored. The citizens may get some needed and secret or forbidden informations from this data base. Because of getting secret informations, some problems may occur. There must be some rules about getting information in the context of necessity of privacy and security of information.

Keywords: E-government, information and secure sharing, privacy of information in e-government, confidence of information in e-government.

GİRİŞ

İçinde bulunduğumuz çağın bilgi çağı olmasının nedenlerinden biri, günlük yaşam içinde bilgi gereksiniminin ve öneminin çok artmış olmasıdır. Bilgi gereksiniminin bu kadar ön plana çıkması bilginin düzenli bir biçimde saklanması ve gerektiğinde saklanan bilgilerin içinden istenilen bilginin tekrar alınarak işleme konulması gereksinimini de beraberinde getirmektedir. Günümüzde bilgisayar ve internet teknolojilerinin de sürekli bir gelişme içerisinde olduğu bilinmekle birlikte bu iki faktörün bir arada kullanılması kaçınılmaz bir hal almıştır. Nitekim bilgisayarlar büyük miktarlarda bilgileri düzenli bir şekilde depolayabilmekte ve istenildiğinde depolanan bilgiler içerisinden aranan bilgiyi çok kısa bir zaman içinde bularak kullanıcıya sunabilmektedir. Bilgisayar ve bilginin bu uyumlu işbirliği, bilgilerin saklandığı her ortamda bilgisayar kullanımını zorunlu hale getirmektedir. Tapu dairesinde saklanan tapu bilgileri, vergi dairesinde saklanan vergi kimlik bilgileri, nüfus idaresinde saklanan nüfus bilgileri vb. örnekleri çoğaltabilmek mümkündür. Her kurum kendi bilgilerini depolamak ve düzenlemek durumunda kalmakla birlikte internetin tüm dünyayı birbirine bağlayan büyük bir ağ olması ve internet dünyasındaki baş döndürücü gelişmeler sayesinde tüm kurum bilgisayarları bu ağa bağlanmış ve böylece kurumlar arasında elektronik bir bilgi paylaşımı başlamıştır. Devlet kurumlarının bilgi paylaşımına başlamaları hantal olan devlet yapısını biraz olsun bu hantallıktan kurtarmıştır. Fakat bilgiye olan gereksinim sadece devlet kurumları ile sınırlı değildir. Vatandaşların da bilgiye olan gereksinimleri artmakta ve devlet kurumları bu hantal yapı içerisinde vatandaşların isteklerine ve ihtiyaçlarına yanıt vermekte çok zorlanmaktadır. Bu aşamada tüm bu isteklere hızlı ve güvenilir bir şekilde yanıt verebilecek e-devlet altyapısının kurulması ve hizmete girmesi gerekmektedir. Bu yapı kurulduğu ve hizmete girdiği anda kurum bilgisayarlarında depolanan tüm bilgiler elektronik ortama taşınmış olacaktır.

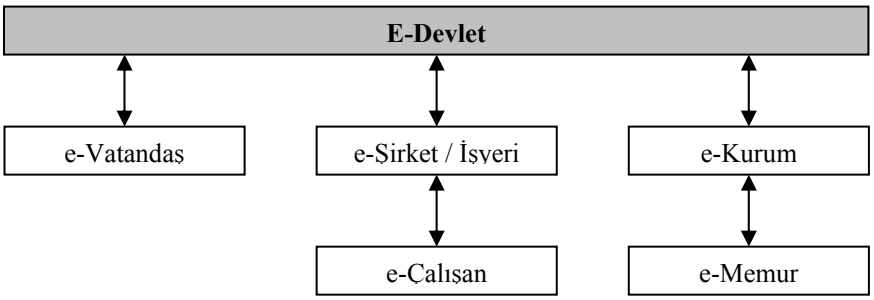
1. E-devlet nedir?

E-devletin farklı birçok tanımı bulunmaktadır; devletin vatandaşlarına karşı yerine getirmekle yükümlü olduğu görev ve hizmetlerle, vatandaşların devlete karşı olan görev ve hizmetlerinin karşılıklı olarak elektronik iletişim ve işlem ortamlarında kesintisiz ve güvenli olarak yürütülmesidir (Arifoğlu ve Diğerleri, 2002). Vatandaşların, ticari sektörlerin ve devlet kurumlarının, kamu yönetiminde, bilgi ve iletişim teknolojilerinin kullanılmasıyla, kamu bilgilerine ve hizmetlerine ulaşmalarını kolaylaştıran sistemin ifadesidir (Lambrinousdakis ve Diğerleri, 2003). Farklı bir tanımla E-devlet, devletin tüm bürokratik, ekonomik ve hukuksal işlemlerini bilgisayar aracılığıyla iletişim ağları üzerinden doğrudan yapabilmesini sağlayan, vatandaşların devlete karşı görevlerini güvenle yürütebildikleri ve istedikleri hizmetlerden yararlandıkları, zaman ve mekân kavramlarını ortadan kaldıran elektronik bir yapıdır. Bu yeni yapı eski yapının işlevinin ortadan kalkması anlamına gelmemekle birlikte, eski devlet yapısının yükünü hafifletmesi açısından çok daha kullanışlı ve hızlı bir işleyişe sahiptir. Bilgi teknolojileri, bilgi ağları ve paylaşılmış veri bankaları tüm ekonomi ve toplum içinde bilginin üretim, dağıtım ve tüketim ilişkisini kolaylaştıracak şekilde bireyleri, şirketleri ve hükümetleri birbirine bağlamaktadır (Baykal, 2007). Geleneksel devlet yapısının işleyişi ile e-devlet yapısının işleyişi arasındaki farklılıklar Tablo 1'de görülmektedir.

Tablo 1:Geleneksel Devlet Anlayışı ile E-devlet Anlayışının Karşılaştırılması

Geleneksel Devlet Anlayışı	**E-Devlet Anlayışı**
Bürokratik kontroller.	Bireye hizmet ve toplumun güçlendirilmesi.
İzole edilmiş idari fonksiyonlar.	Entegre kaynak hizmetleri, açık ve şeffaf devlet.
Kâğıt işi ve dosyalama.	Elektronik hizmet teslimatı.
Zaman tüketen süreçler.	Hızlı seri iş süreçleri.
Elle düzenlenen finansal sözleşmeler.	Elektronik fon transferi.
Garip raporlama sistemleri.	Bilgiye esnek erişim.
Bağlantısız, kopuk bilgi teknolojileri	Bütünleşmiş ağ çözümü.
Her dönem idareci seçimi.	Gerçek, katılımcı ve sürekli demokrasi.

Kaynak: (Şahin ve Örselli, 2003)



Şekil 1: E-Devletin Ögeleri (Şahin ve Örselli, 2003)

E-devlet sadece devlet kurumlarından meydana gelen bir yapı değildir. E-devlet kendini oluşturan tüm unsurlarla bir bütün olarak değerlendirilmelidir. Şekil 1'de e-devlet yapısı ve bu yapıyı oluşturan unsurlar açıklanmaktadır. Açıklanan bu unsurlarla birlikte tüm bu hizmetleri sağlamak için izlenmesi gereken yolda, belirli çekirdek etkinlik ve teknoloji alanlarına yatırım yapılması özgün teknoloji ve ürün geliştirme çalışmalarının uzun dönemli bir yatırım stratejisi olarak görülmesi, teknik altyapının, bilgiye erişim ve bilgiyi saklama olanaklarının uluslar arası standartlarda olmasını gerektir (Tolunay ve Sarı, 2007). E-devlet uygulamalarının tamamında çok büyük miktarlardaki bilgi kümeleri vatandaşların, şirketlerin ve kurumların hizmetine girmektedir. İçinde bulunduğumuz çağa adını veren bilgi, önemi açısından tam bir koruma içinde bulunmalıdır. Bu kadar büyük öneme sahip bilgilerin istenmeyen kişi ve kurumların eline geçmesinin beraberinde birçok problem doğuracağı, hem ekonomik hem stratejik hem de hukuksal açıdan büyük sorunlara yol açacağı düşünülmektedir. Bu riskler, bilgisayar korsanı (hacker) saldırıları, elektrik kesintisi sonucunda oluşabilecek veri kayıpları, bilgisayar virüsleri ve bilgisayar üzerinden dolandırıcılık olarak belirlenmiştir (Grabosky, Smith ve Depsey, 2001; Akt: Clark, 2003). Ulusal bilgi paylaşım altyapısının korunması, yalnızca devletin değil bu altyapıyı kullanan kurumların, üniversitelerin ve özel kuruluşların ortak çabasını gerektirir. Bu amaçla bu kuruluşlar düzenli bir araya gelerek gerekli eşgüdüm sağlanmalıdır. Kuruluşların bu konudaki kaygılarını bir araya getiren, yorumlayıp çözüm üretecek örgütlenme gereklidir (Tolunay ve Sarı, 2007).

1.1 Avrupa'da ve Dünyada E-Devlet ve Güvenlik

Avrupa birliği ülkelerinin tamamında ve dünyanın çeşitli ülkelerinde yürütülen e-devlet uygulamalarına bakıldığında bu uygulamaların genel amacının, yürütülen işlemlerin hızlı, doğrudan ve güvenli bir ortamda gerçekleştirilmesi olduğu ve böylece hizmet kalitesini artırarak zaman ve maliyet tasarrufu sağladığı görülmektedir. Bu genel amaç doğrultusunda yapılan bütün e-devlet hizmetlerinin ortak problemi güvenlik sorunudur. Çünkü elektronik ağlar üzerinden gerçekleştirilen bu uygulamalar her an kötü niyetli saldırılara açık durumdadır. Bu durum e-devlet uygulamalarını yürüten tüm ülkelerin elektronik ortamda güvenlik önlemleri almaya mecbur bırakmaktadır. 2007 yılında yayınlanan bir araştırmanın sonuçlarına göre e-devlet uygulamalarına yönelik gerçekleşen güvenlik ihlalleri Tablo 2'de görülmektedir.

Tablo 2: E-devlet Uygulamalarındaki Güvenlik İhlalleri

Güvenlik İhlali	**Yüzde (%)**
Yetkisiz (İzinsiz) Erişim	5.2
Hizmetlerin (Servislerin) Engellenmesi	0.1
Kötü niyetli program kodları	4.6
Uygunsuz Kullanım	8.3
Tarama / İzinsiz Giriş Denemesi	73.1
Araştırma İnceleme	8.7
Toplam	100.0

Kaynak: (US-CERT, 2007)

1.1.1 Avrupa

E-Avrupa, Avrupa Birliği'ndeki tüm vatandaşların, şirketlerin, işletmelerin ve okulların internet kullanımını, internet üzerindeki günlük etkinliklerden, servis ve eğitim hizmetlerinden, sağlık, kültür ve e-devlet uygulamalarından yararlanmalarını sağlamayı amaçlamaktadır. Günümüz toplumlarında vatandaşların internet erişimine sahip olmaları temel bir haktır ve hükümetler bu hizmeti sağlamakla sorumludur (Europan Commission, 2002). E-devlet uygulamalarının yürütüldüğü bilgisayar sistemlerinin ve bu sistemler üzerinde yer alan kişisel ve özel bilgilerin korunması oldukça önemli bir konudur.

Tablo 3'de görüldüğü gibi Avrupa Birliği bünyesinde birçok e-devlet uygulaması vatandaşların hizmetine sunulmuştur. Bu e-devlet uygulamaları ile verilecek hizmetler için gerekli olan bilgiler veritabanlarında tutulmaktadır. Bu veritabanlarının ve bu veritabanlarının çalıştığı sistemlerin güvenliği çok önemlidir. Avrupa Birliği komisyonu bilgi ve ağ güvenliği konusunda gerçekleştirdiği geniş kapsamlı toplantıda, bilgi ve bilgisayar sistemlerine karşı yapılacak olan terörist saldırılara karşı nasıl bir karar verme mekanizması olması gerektiğini tartışmıştır. Aynı düzeyde öneme sahip bir başka durum da sistemden hizmet alanların bilgilerinin korunması ve mahremiyetlerinin güven altına alınmasıdır (Europan Commission, 2002). Bu doğrultuda hazırlanan bir güvenlik planı belirlenerek sisteme adapte edilmiştir.

Tablo 3: E-Avrupa'da Vatandaşlara ve Şirketlere Verilen Hizmetler

	Vatandaşlara Sunulan Servisler
1.	Vergi işlemleri (bildirim, bildirimin değerlendirilmesi)
2.	İş arama servisleri
3.	Sosyal güvenlik katkıları (primleri) İşsizlikten yararlanma. Aile ödemeleri Tıbbi maliyetlerin ödenmesi Öğrenci bursları
4.	Personel belgeleri (pasaport ve sürücü belgeleri)
5.	Araç kayıtları (yeni, kullanılmış ve ithal araçlar)
6.	Bina (inşaat) ruhsat başvuruları
7.	Polis bildirimleri (hırsızlık ve çalıntı gibi)
8.	Halk kütüphaneleri (kataloglara erişim ve arama araçları)
9.	Belgeler (doğum, evlilik vb.) : istek, gönderme
10.	Üniversite ya da yüksek eğitim kurumlarına kayıt
11.	Taşınma (adres değişikliği) bildirileri
12.	Sağlık problemlerini anlatma servisleri (interaktif tavsiye ve uyarı alma)
	İşyerlerine Sunulan (Ticari) Servisler
1.	İşçiler için sosyal yardımlar
2.	Anonim şirketlerinin vergilendirilmesi
3.	Katma değer vergisi (bildirim ve haber verme)
4.	Yeni şirketlerin kayıtları
5.	Şirket bilgilerinin istatistik ofislerine bildirilmesi
6.	Gümrük bildirimleri
7.	Çevre ile ilgili izinler
8.	Kamu ihaleleri

Kaynak: (Europan Commission, 2002)

1.1.2 ABD

ABD'de e-devlet uygulamaları temel olarak üç ana başlık altında toplanmaktadır. Bunlar;

- Devlet-Vatandaş (G2C)
- Devlet-İş Dünyası (G2B)
- Devlet-Devlet (G2G)

1.1.2.1 Devlet-Vatandaş (G2C)

Bu programın genel amacı, vatandaşların bilgi gereksinimlerini ve servislere erişimlerini çevrimiçi olarak gerçekleştirmelerini sağlamaktır. Vatandaşlar ihtiyaç duydukları bilgilere hızlı ve güvenli bir şekilde erişebilirler. Örneğin www.GovbBenefits.gov sitesi, devletin sağladığı hizmetlere erişimi sağlayan sitelerden biridir. Bu site üzerinden mahkeme kararları, çocuk yardımı, sakatlık, eğitim, devlet yardımları, burslar, sigorta hizmetleri, devlet sağlık sigortası, emekli aylığı işleri, sosyal güvenlik işlemleri ve felaket (deprem, sel, fırtına) yardımları gibi temel konularda bilgi almak mümkündür (E-Government Strategy, 2003).

1.1.2.2 Devlet-İş Dünyası (G2B)

Bu programın genel amacı, devlet ile iş dünyası arasındaki ağır iş yükünü azaltmak ve şirketler ile devlet arasındaki yazışmaları sayısal haberleşme dili kullanarak elektronik

ortamda gerçekleştirmektir. Bu bağlamda kullanılan ileri teknoloji, devlet ile iş dünyası arasındaki haberleşmeyi ve devlet-iş dünyası arasında istenilen raporların hazırlanmasını kolaylaştırabilecektir. Örneğin yeni kurulmak istenen bir işyeri için bir yardımcı aracı ya da avukat ihtiyacı ortadan kalkacak, şirket kurulması için gerekli olan en son kural ve açıklamalar www.Regulations.gov adresinden öğrenilebilecektir. Online vergilendirme işlemleri yine bu program altında gerçekleştirilecektir. İhracat formları ve yerleşke bilgileri bu program altında gerçekleştirilerek zaman tasarrufu sağlanmaktadır (E-Government Strategy, 2003).

1.1.2.3 Devlet-Devlet (G2G)

Bu programın genel amacı, vatandaşlara ve işletmelere daha iyi hizmet vermek amacıyla ulusal hükümet, eyalet yönetimleri ve yerel yönetimlerin birlikte daha uyumlu çalışmasını sağlamaktır. Giderek artan doğru ve hızlı bilgi ihtiyacı, bilgilerin yerel ve ulusal yönetimler arasında paylaşılması ihtiyacı kapsamında, bilgiler raporlaştırılarak paylaşılacaktır. Bu gelişme yerel ve eyalet yönetimleri ile ulusal hükümete birçok konuda yarar sağlayacaktır. Doğum ve ölüm kayıtları bu program altında saklanarak devlet kurumları arasındaki bağlantının sağlanması amaçlanmaktadır (E-Government Strategy, 2003). Örneğin, ölen bir vatandaşa emekli maaşı ödemesi gibi yanlış işlemlerin önüne geçilmiş olacaktır.

Yukarıdaki tüm programlar içindeki ortak olan en önemli konu elektronik doğrulama işlemidir. Elektronik doğrulama, ihtiyaçları ve kullanıcı yetkilerini belirlemeyi destekleyen bir çözüm olacaktır. Elektronik doğrulama sistemi kullanılarak kullanıcıların özel bilgilerinin ve güvenliklerinin korunması sağlanacaktır. Böylece elektronik doğrulama diğer e-devlet uygulamalarını da güven altına alacaktır (E-Government Strategy, 2003).

1.1.3 Çin

Bilindiği gibi Çin, oldukça fazla olan nüfusuyla büyük bir ülkedir ve doğal olarak e-devlet uygulamalarının hayata geçirilmesi oldukça kritik bir öneme sahiptir. Bunun için 1999 yılında Çin'de "Çevrimiçi Hükümet Projesi" adıyla bir proje başlatılmış ve şu anda birçok şehirde çevrimiçi bürolar bulunmaktadır. Bunun yanında "Aile Çevrimiçi Projesi" hayata geçirilerek bireylerin e-devlet ortamına teşvik edilmesi amaçlanmıştır (Chengyu, 2002). Çin Hükümeti'nin e-devlet uygulamalarını yürüttüğü site http://www.gov.cn adresindedir. Burada hazır bulunan çevrimiçi bürolar bireylerin ihtiyaçlarını karşılamaktadır.

Çin'de e-devlet uygulamaları için temelde yürütülen "Çevrimiçi Hükümet Projesi" sekiz ana başlıkta yürütülmektedir. Bunlar,

1) Çevrimiçi elektronik bilgi değişimi
2) Çevrimiçi hükümet ihale sistemi
3) Çevrimiçi yardım ödeme sistemi
4) Elektronik dağıtım
5) Danışma merkezi
6) Elektronik evrak yönetimi ve dağıtımı
7) Elektronik vergi
8) Dijital kimlik (Chengyu, 2002).

"Çevrimiçi Hükümet Projesi"nin hedefi, 2000 yılının sonuna kadar Çin eyalet organlarının %80'inin çevrimiçi hale gelmesiydi. Bunu başarmak için "Çevrimiçi Hükümet Projesi Servis Merkezi" kurulmuştur. Bu merkez öncelikle proje çalışanlarının örnek alması için oldukça önemli özelliklerden oluşan bir model geliştirmiştir. Bu özellikler şunlardır:

1) Yerel hükümetlere servislerin kurulmasını sağlayacak ve rehberlik edecek yönergeler oluşturmak.
2) Merkezi ve eyalet hükümetleri tarafından organize edilen projelerle ilgili olayları halka duyuracak bir propaganda merkezi oluşturmak.
3) Hükümetle ilgili reklamları yapacak bir bülten oluşturmak.
4) Sanal platformların kurulması, güvenlik ayarlamaları, personel eğitimi ve proje ile ilgili her türlü rehberlik etkinlikleri için bir servis merkezi kurulması.
5) Vatandaşla ve diğer veri bankalarıyla ilgili düzenlemeleri ve kanunları yapan bir danışma merkezi
6) Eyaletler arasında düzenli bilgi alışverişini sağlamak için 100 şehir arasında bir ağ kurmak (Holliday ve Yep, 2005).

1.1.4 Japonya

1990'ların ortasında pek çok Avrupa ve Kuzey Amerika ülkeleri ve bazı Asya ülkeleri (özellikle Singapur) e-devlet uygulamalarında oldukça ilerlemeler göstermesine rağmen, Japonya e-devlet uygulamalarına yavaş bir başlangıç yapmıştır. E-devlet uygulamalarında ilk ciddi atılımlar Başbakan Obuchi Keizo (1998-2000) zamanında 1990'ların sonlarında yapılmıştır. Nisan 1999'da acil eylem planı hazırlanmış, Temmuz 2000'de Bilişim Teknolojileri Strateji Konseyi toplanmıştır (Jain, 2002).

Haziran 2001'de Bilişim Teknolojileri Genel Merkezi tarafından "E-Japonya 2002 Programı" hazırlanmıştır. Bu programda, hükümetin bilişim teknolojileri politikasını yoğun bir biçimde ve stratejik olarak nasıl yürütmesi gerektiği ve bakanlıkların ve diğer hükümet kuruluşlarının hem "e-Japonya stratejisi"ni hem de "e-Japonya Öncelikli Politika Programı"nı yürütmesi etkinlikleri bulunmaktadır (e-Japonya 2002 Programı).

Japonya'da e-devlet uygulamalarında bir diğer önemli gelişme de, hükümet web sayfalarının bir portalda toplanmasıdır (E-Japonya) . Bu portal sayesinde pek çok tür farklı bilgiye hem vatandaşlar tarafından erişilebilmekte, hem de hükümet kuruluşları tarafından erişilebilmektedir.

2. Türkiye'de E-Devlet Uygulamaları, Bilgi Güvenliği ve Gizlilik

Dünyada birçok ülkede olduğu gibi Türkiye'de de e-devlet uygulamaları hızla gelişmiş ve sürekli olarak gelişmeye devam etmektedir. Türkiye'de e-devlet kapsamında kamu kurumlarının neredeyse tamamına yakını çeşitli hizmetler vermektedir. Ayrıca E-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı'na göre vatandaşlara, kolay erişilebilir, daha hızlı, daha ucuz, sürekli ve güvenli internet olanağının sağlanmasıyla ilgili çalışmalar da başlamıştır. Tablo 4'de e-devlet kapsamında hizmet veren kamu kurumlarının isimleri ve hizmet alanları görülmektedir. Tablo 4'de listelenen kamu hizmetleri vatandaşlar ile ulusal ve yerel yönetimler arasındaki iş yükü ve zaman miktarını azaltarak büyük kolaylıklar sağlamaktadır.

Tablo 4: E-Devlet Hizmetleri

E-Devlet Hizmetleri	
TC Kimlik Numarası Sorgulama	Gelir Vergisi Sorgulama
SSK Hizmet Sicil Sorgulama	Gelir Vergisi Gecikme Zammı Sorgulaması
SSK Emeklilik Günü Sorgulama	Bağkur Emeklilik Sorgulaması
Sağlık Karnesi Sorgulama	Emekli Sandığı Hizmet Süresi Sorgulama
Aracınızın Vergi Borcunu Sorgulama	Sigortalı Hizmet Dökümü Sorgulama
Ceza ve MTV Sorgulama	Türk Telekom Borç Sorma
Doğalgaz Fatura Sorgulama	SSK Hizmet Sicil Sorgula
A.Ö.F. Sınav Sonuçlarını Sorgulama	SSK Emeklilik Gün Hesabı
LES Sonuçlarını Sorgulama	Emekli Maaşınızı Sorgulama
ÖSYS Sonuçlarını Sorgulama	İgdaş Borç Sorma Servisi
KPDS Sonuçlarını Sorgulama	İSKİ Borç Sorma
PTT Posta Kodu Sorgulama	Vergi kimlik Kartı Sorgulama
Vergi Kimlik Numarası Sorgulama	Milli Eğitim Bakanlığı Portalı
Kayıp Şahıs Sorgulama	Y.Ö.K. - Tez Arama
Sürücü Ceza Puanı Sorgulama	Milli Kütüphane Veritabanı
OGS Bakiye Bilgi Sorgulama	Çalıntı Araç Sorgulama
Çalıntı Kayıp Cep Telefonu Sorgulama	Kazaya Karışan Araç Sorgulama
Emeklilik Yaşı Sorgulama	Kredi Yurtlar Kurumu Bilgi Sorgulama
Emeklilik Maaşı Sorgulama	Kurumsal/Kamu Web Sitelerindeki Diğer
Vakıfbank, Ziraat Bankası Internet Şubeleri	Sorgulamalar

Kaynak: (www.onlinesorgulama.com)

E-devlet uygulamalarının hayata geçirilmesi ve vatandaşların hizmetine sunulması sürecinde bazı düzenlemeler getirilmesi kaçınılmaz olacaktır. Bu düzenlemeler e-devlet hizmetlerinin yürütülmesi bakımından hayati öneme sahiptir. E-devlet uygulamalarının düzenlenmesine ilişkin olarak planlanan aşamalar;

- Hukuksal altyapı
- Teknolojik altyapı
- Kullanıcıların altyapıları
- E-devlet uygulamalarının finansmanı
- Hizmet altyapısını oluşturmak
- Hizmet (servis) mekanizmasını oluşturmak
- Güvenlik ve gizlilik
- Kritik başarı faktörlerinin belirlenmesi
- Bir koordinasyon merkezinin oluşturulması

şeklinde verilmektedir (Yıldız,2003 ;Erkul, 2004). Yapılması gereken düzenlemelerin önemli bir boyutunun bilgi güvenliği ve gizlilik olduğu düşünülmektedir. E-devlet uygulamalarındaki bilgi sistem güvenliği, dokümanların ve elektronik ortamdaki bilgilerin güvenliği üzerine kurulmuştur (Spinellis ve Diğerleri, 1999). E-devlet uygulamaları kapsamında hizmet sunan kamu kurumları arasındaki koordinasyonsuzluk bilgi açığı oluşmasına yol açabilmektedir. Kamu kurumları arasındaki bu koordinasyon eksikliğinin sonucu olarak kurumsal bilgilerin ya da vatandaşlara ait kişisel bilgilerin kötü niyetli insanların eline geçmesi kolaylaşmaktadır. Oysa günümüzde vatandaşların birçok resmi ve kurumsal işlemlerini bilgi temelli olarak yürüttüğü düşünüldüğünde bu güvenlik açığının öneminin çok büyük olduğu ortaya çıkmaktadır. Global piyasa araştırma şirketi Taylor Nelson Sofres, 2002 yılı içinde 31 ülkeden yaklaşık 29.000 kişi

ile görüşerek gerçekleştirdiği elektronik devlet araştırmasında, devlet hizmetlerinin elektronik ortamda kullanımını incelemiş ve dünya genelinde interneti devlet hizmetlerine erişim amacıyla kullananların oranında son bir yıl içinde %15'lik bir artış olduğunu gözlemlemiştir. Türkiye'de ise 2001 yılında %3 olan bu oranın 2002 yılında %13'e çıkmıştır. E-devlet uygulamaları, içerdiği bilgiler ve kullanıcı yoğunluğu nedeniyle çok çekici ve potansiyel bir hedeftir. E-devlet uygulamalarının kullanıldığı veritabanlarından, düşmanların devletin zayıf yönlerini algılayabilmeleri ve saldırı planlarını buna göre yapmaları mümkündür (Halchin, 2004).

2.1. Türkiye'de E-Devlet Uygulamalarında Bilgi Güvenliği, Gizlilik ve Açıklar

E-devlet uygulamalarının en önemli öğelerinden biri kişisel bilgilerin doğru olması ve yapılan işlemlerin güvenli bir ortamda gerçekleştirilmesidir. Güvenlik politikası özellikleri ise üç başlık altında toplanabilir;

- **Koruma:** Kullanıcıların topladıkları bilgiler, bunları kullanma şekilleri ve yaptıkları tüm işlemlerin gizli kalması ve dışarı sızdırılmaması.
- **Yeterlilik:** Kullanıcının yapmak istediği işlem ile ilgili olarak yalnızca gerekli bilgileri girmesi, o anki işlemle ilgili olmayan şahsi bilgileri girmek zorunda bırakılmaması.
- **Güvenlik:** E-devlet uygulamaları üzerinden yapılan tüm işlemlerin güvenliğinin sağlanması ve dışarıdan oluşabilecek tüm ataklara karşı güvenlik duvarlarının oluşturulması (Şener ve Paşayiğit, 2006).

Yukarıda verilen güvenlik politikasına ek olarak e-devlet uygulamalarında hizmet sağlayan (sunucu) bilgisayarların, kurumların kendi denetiminde bulunması ya da devlet bünyesinde kurulan (sunucu) bilgisayarlarda tutulması bilgi güvenliği açısından çok büyük öneme sahiptir. Örneğin, Ankara'nın Batıkent semtinde 45.000 mahalle sakininin kişisel bilgilerinin kayıtlı tutulduğu muhtarlık bilgisayarının çalınmış olması (www.kenthaber.com) ve aralarında İzmir'in de bulunduğu 15 ilin valiliğinin, daha ucuz ve hızlı olduğu gerekçesi ile barındırma hizmetini yurtdışından alması, bu valiliklerin internet üzerinden yaptıkları e-posta dâhil her türlü işlemin risk altına girmesi (www.devletim.com) bu durumun en açık göstergesidir. Basit gibi görünen bu tür olayların kişisel ve kurumsal bilgilerin korunması ve gizliliği ortadan kaldırması açısından çok önemli olduğu ortaya çıkmaktadır. Bu iki olay kurumsal ya da kişisel olarak gizli olması ve korunması gerekli olan bilgilerin doğrudan ticari bir kuruluşun ya da kötü niyetli insanların eline nasıl geçebileceğini anlatmakla birlikte e-devlet hizmetlerinde, hizmetleri sunan kamu kurumlarının koordinasyonsuzluklarından kaynaklanan açıkların da mevcut olduğunun bir göstergesidir. Artan elektronik saldırılardan birincisi, kişisel bilgilerin ele geçirilerek elektronik ortamda yapılan bankacılık, e-ticaret vb. alanlarda başkasının adına sahte işlemler yapılmasıdır. İkincisi ise, bu yasal olmayan işlemlerin yanı sıra kişilere ait özel bilgilerin kişilerin izni olmadan açığa çıkarılmasıdır (Ersoy, 2006). İnternet saldırganları bu bilgilere erişmek için çok çeşitli yöntemler kullanmakla birlikte, bu yöntemlerden birinin kamu kurum ve kuruluşlarının web sitelerinden yararlanmak olabileceği düşünülmektedir. Kamu kurumlarına ait e-devlet uygulamalarının bulundukları web siteleri üzerinden

gerçekleştirilen sorgular, bu sorguların çalıştırılması için gerekli kişisel bilgiler ve sorgu sonuçlarından elde edilen bilgiler Tablo 5'de görülmektedir.

Vatandaşlara hizmet verilen kamu web siteleri ve bu siteler üzerinden yapılan sorgulama işlemleri Tablo 5'den incelendiğinde iki önemli nokta ortaya çıkmaktadır;

- **Herhangi bir sorgulama işlemi için kullanıcıdan iki ya da üç farklı bilgi istenmekte, fakat sorgulama işlemi sonunda kullanıcıya işlemin amacından çok fazla ayrıntılı bilgi verilmektedir. Böylece kullanıcı istemediği bilgileri de almaktadır.**
- **Herhangi bir sorgulama işleminden elde edilen bilgiler başka bir web uygulamasında sorgu parametresi olarak kullanılabilmektedir. Böylece bir web sitesinden alınan bilgi ya da bilgiler farklı bir web sitesinde kullanılarak yeni bilgilere ulaşılabilmektedir.**

Tablo 5: Bazı E-Devlet Uygulamalarında Sorgulama İçin Gerekli Bilgiler ve Sorgu Sonucunda Elde Edilen Bilgiler

E-Devlet Uygulaması Erişim Adresleri *	**Erişim Tarihi**	**Sorgu Adı**	**Sorgu İçin Gerekli Bilgiler**	**Sorgu Sonucu Elde Edilen Bilgiler**
ÖSYM	19.07.2007	2007 ÖSS Sonuçları	T.C. Kimlik No	İsim, soyad, T.C. kimlik no ve bütün sınav puanları
Emekli Sandığı Genel Müdürlüğü	19.07.2007	Emekli sicil numarası öğrenme	İsim, soyad, doğum tarihi (yıl)	Emekli sicil no, doğum tarihi (gün.ay.yıl), baba adı, T.C. kimlik no ilk yedi hanesi, durum
Emekli Sandığı Genel Müdürlüğü	19.07.2007	Emekli Sandığı T.C. Kimlik Numarası Doğrulama ve Hak Sahipliği İşlemleri	T.C. Kimlik No	Emekli sicil no, doğum tarihi (gün.ay.yıl), baba adı, T.C. kimlik no ilk yedi hanesi, durum
Yüksek Öğrenim Kredi ve Yurtlar Kurumu Genel Müdürlüğü	19.07.2007	Kredi numarası sorgu ekranı	Ad, soyad, baba adı	Ad, soyad, baba adı, üniversite adı, kredi no, öğrenim kredi no, katkı kredi no, burs no
Yüksek Seçim Kurulu	20.07.2007	Seçmen sandık bilgileri sorgulama	T.C. kimlik no	İsim, soyad, seçmen numarası, T.C. kimlik numarası, Adres
Sosyal Sigortalar Kurumu	20.07.2007	Sigortalılık tescil kaydı tespiti uygulaması	T.C. kimlik, ad, soyad, baba adı, doğum yılı, ilk soyadı	Ad, soyad, Varsa ilk soyad, ssk sicil no, anne adı, doğum yeri, doğum tarihi (gün.ay.yıl), baba adı, T.C. kimlik no, durumu (aktif/pasif)
Sosyal Sigortalar Kurumu	20.07.2007	Sigortalı hizmet dökümü için SSK sicil numarasından sorgulama	SSK sicil no	SSK sicil no, ad, soyad, doğum yılı, ilk işe giriş tarihi
Gelir İdaresi Başkanlığı	20.07.2007	Vergi kimlik numarası sorgulama	İsim, soyad, baba adı, doğum yeri, doğum yılı	Vergi kimlik no, isim, soyad, vergi dairesi ili ve ilçesi
Milli Eğitim Bakanlığı	---	Öğretmen Atama Sonuçları	T.C. Kimlik no	İsim, soyad, atama yeri
Gelir İdaresi Başkanlığı	20.07.2007	Motorlu Taşıt Sorgulaması	Plaka, Vergi kimlik no, T.C. kimlik no, tescil tarihi (gün.ay.yıl)	Vergi kimlik no, T.C. kimlik no, isim, soyad, baba adı, ana adı, doğum tarihi (gün.ay.yıl),
Gelir İdaresi Başkanlığı	20.07.2007	Motorlu Taşıt Sorgulaması	Plaka, Vergi kimlik no, T.C. kimlik no, tescil tarihi (gün.ay.yıl)	doğum yeri, araç plakası,Tescil tarihi (gün.ay.yıl), araç tipi, silindir hacmi, adres bilgileri (mahalle, cadde, daire, posta kodu, il, ilçe) , trafik ceza bilgileri, motorlu taşıtlar vergisi bilgileri.
Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü	20.07.2007	T.C. Kimlik No Sorgulama Bilgileri	Nüfusa bağlı bulunduğu il, ilçe, baba adı, ana adı, doğum yılı, cinsiyeti	Nüfusa bağlı bulunduğu il, ilçe, baba adı, ana adı, doğum yılı, cinsiyeti, T.C. kimlik no, cilt no, aile sıra no, birey sıra no, mahalle/köy
Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü	20.07.2007	T.C. kimlik no doğrulama bilgileri	T.C. kimlik no	İsim, soyad, doğum yılı
Milli Eğitim Bakanlığı	31.07.2007	Devlet Parasız Yatılı Sınav Sonuçları	T.C. kimlik no	Sınav Sonuçları
İstanbul Su ve Kanalizasyon İdaresi	31.07.2007	İski borç sorgulama	Mukavele Numarası	Tam ev adresi, mukavele tarihi, hukuk durumu, geçmiş dönem borçları, son bir yıllık faturalar
Sağlık Bakanlığı	26.07.2007	Doktor Bilgileri Sorgulama	T.C. Kimlik No veya Adı Soyadı	Baba adı, doğum yeri, doğum tarihi (gün, ay, yıl), mezun olduğu üniversite, diploma no, branşı

* Erişim adresleri güvenlik gerekçesiyle burada belirtilmemiştir.

Bu iki durum dikkate alındığında, bir sorgulama işlemi sonucunda, istenmediği halde kullanıcıya sunulan fazladan bilgi ve bu bilgiler kullanılarak başka bir e-devlet uygulamasından elde edilen birçok kişisel ve kurumsal bilgi ortaya çıkmaktadır. Amerika'daki e-devlet uygulamalarında kullanılan bilgiler birçok yeni kategoriye ayrılmış, böylece vatandaşların sadece istenilen bilgilere ulaşımları sağlanmış, fazladan bilgiye erişimleri kısıtlanmıştır (Caidi ve Ross, 2005). Tablo 5'de verilen e-devlet uygulamaları incelendiğinde bu uygulamaların genel boyuttaki e-devlet uygulamaları oldukları, bu bakımdan e-devlet uygulamaları derinleştirilerek yerel boyuttaki e-devlet uygulamaları da incelenecek olursa, bilgi güvenliği ve gizlilik ihlallerinin çok daha derinleşebileceği göz ardı edilmemelidir. Bu güvenlik ve gizlilik ihlalleri nedeniyle en çok zarar görebilecek kesim, kamu kurum ve kuruluşlarında çalışan devlet memurları olacaktır. Kamu kurum ve kuruluşlarında çalışan devlet memurlarının kişisel ve kurumsal bilgileri daha düzenli tutulmakta ve bu durumun bir sonucu olarak kolay ve hızlı bir şekilde e-devlet platformlarına taşınabilmektedir. Genel ve yerel e-devlet uygulamaları incelenerek e-devlet sisteminde kayıtları bulunan bir devlet memurunun kişisel ve kurumsal bilgileri bir elde toplanabilir. Toplanan bilgiler kötü niyetli kullanılarak siber saldırılar gerçekleştirilebilir. Siber saldırganlar değerli hedeflere saldırırlar. Bu hedefler genelde ekonomik getirisi olan ya da değerli bilgi içeren hedeflerdir (Baykal, 2007). Çalınan bilgileri kullanan siber saldırganlar bu bilgileri;

- Sahte kimlik belgesi oluşturma,
- Sahtekârlık ve taklit,
- Casusluk faaliyetleri,
- Takip ve gözetleme,
- Ticari bilgi çalma,
- Banka bilgileri kullanılarak hesaplar üzerinde oynama,

gibi amaçlar için kullanabilir. E-devlet uygulamaları üzerinde gerçekleştirilebilecek suçların nitelikleri de bilinen suçlardan farklılık göstermektedir. E-devlet uygulamaları bir bütün olarak incelenirse, uygulamaların risk seviyeleri ve güvenlik ihtiyaçları da net olarak ortaya konabilir. Tablo 6'da e-devlet uygulamalarının risk seviyeleri ve güvenlik ihtiyaçları görülmektedir.

Tablo 6 incelendiğinde elektronik doğrulama işlemlerinin servis operatörleri açısından *orta düzeyde,* servis kullanıcıları (vatandaşlar) açısından *yüksek düzeyde* risk seviyesinde oldukları tespit edilmiştir. E-devlet uygulamalarını bu açıdan inceleyecek olursak, vatandaşların e-devlet servislerine yaptıkları girişlerin yüksek düzeyde risk taşıması, ayrıca servislerde vatandaşlara verilen bilgilerin çok olması bilgi güvenliği ve gizliliği açısından da yüksek düzeyde risk oluşmasına sebep olacaktır. Ayrıca, arama ve bilgi edinme işlemlerinin düşük düzeyde risk oluşturduğu fakat oluşan bu riskin e-devlet uygulamaları arasında *bütünlük* sağlanarak önlenebilineceği vurgulanmaktadır. Amerika'da, izinsiz olarak sisteme giriş yapmak ve buradan bazı bilgi ve belgelerin alınması işlemleri birinci kategoriye giren güvenlik ihlallerindendir (US-CERT, 2007).

Tablo 6: E-devlet Uygulamalarının Risk Seviyeleri ve Güvenlik İhtiyaçları

Servisler	Servis Aşaması	Erişim Tipi	Risk Seviyesi	Güvenlik İhtiyaçları
E-devlet İşlemleri	○ Sistem kurulumu (Düzenlenen servis biriminin donanım ve yazılım kurulumu)	○Sistem Yöneticisi	○ Orta	○ Sistem durumu ○ Performans ○ Özel hakların (imtiyazların) yönetimi
	○ Elektronik doğrulama	○ Servis operatörleri ○ Servis kullanıcıları	○ Orta ○ Yüksek	○ Elektronik doğrulama
	○ Servis kurulumu, web sunucularının güvenlik açıklarının kapatılması	○ Servis operatörleri	○ Orta	○ Güvenilirlik ○ Doğrulama
	○ Servis sunumu ○ Arama, bilgi edinme ○ Doğum belg. talepleri	○ Servis kullanıcıları	 ○ Düşük ○ Orta	 ○ Bütünlük ○ Güvenlik ○ Bütünlük
	○ Vergi bildirim formları		○ Orta	○ Güvenlik ○ Bütünlük ○ Kesinlik
	○ Elektronik ödeme		○ Yüksek	○ Güvenlik ○ Bütünlük ○ Doğrulama
	○ Servis görevlerinden sonra (Gönderilen vergi ödeme formlarının depolanması, elektronik ödeme ve gönderilerin gerçekleştirilmesi vb.)	○ Servis operatörleri	○ Orta	○ Güvenli depolama

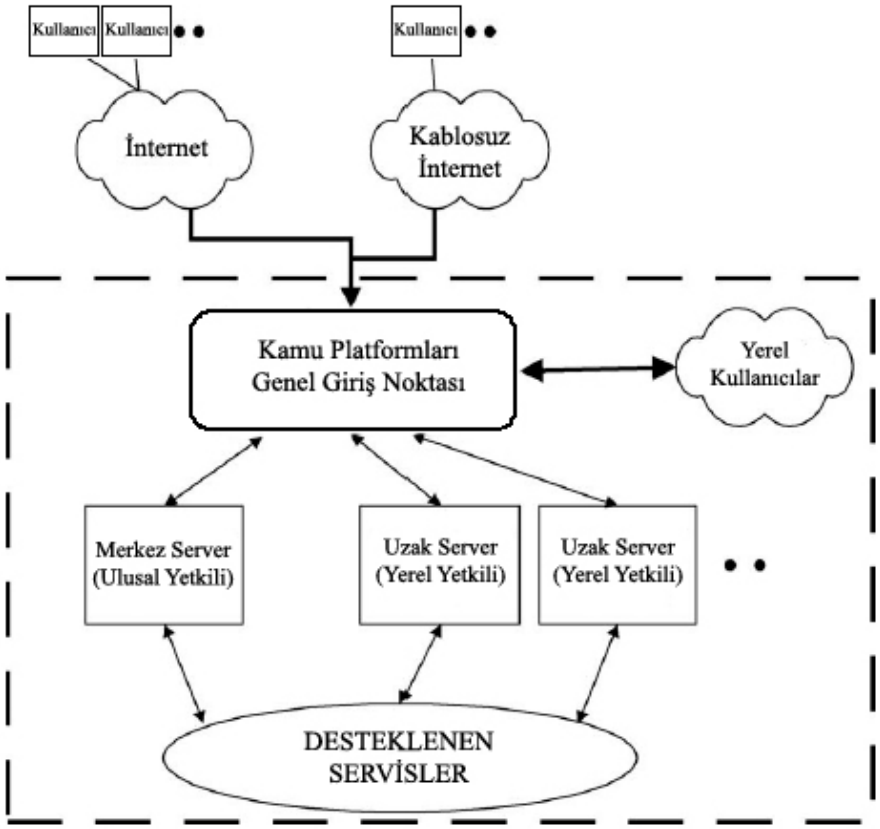
Servis operatörleri: Web sitesi yöneticileri, Servis kullanıcıları: Vatandaşlar
Kaynak: (Lambrinoudakis ve diğerleri, 2003)

3. Güvenlik ve Gizlilik İhlallerinin Önlenmesi

E-devlet uygulamalarında güvenliğin sağlanabilmesi için birçok etken vardır. Bu etkenlerden en önemlisi, yürürlükte olan e-devlet modelinin güncellenmesidir. Önerilen yeni model Şekil 2'de görülmektedir.

3.1. E-Devlet Modeli

Bu model öncelikli olarak e-devlet verilerinin tek bir adreste toplanmasını sağlamasını, kurumlar arasında bütünlük oluşturulmasını şart koşması ve e-devlet verilerini bir standarda kavuşturması açısından büyük avantajlara sahiptir. Sadece bu özellikleri dikkate alındığında bile birçok güvenlik açığını ortadan kaldırmış olacaktır. Örneğin, Ankara'nın Batıkent semtinde 45.000 mahalle sakininin kişisel bilgilerinin kayıtlı tutulduğu muhtarlık bilgisayarının çalınmış olması bilgisayarda depolanan bilgilerinde üçüncü kişilerin eline geçmesine sebep olmuştur. Şekil 2'de açıklanan model kullanıldığında, sadece bilgisayarın çalınmış olması nedeniyle maddi bir zarara sebep olacak, uzak bilgisayarlarda depolanan bilgiler hiçbir şekilde üçüncü kişilerin eline geçmeyecektir. Ayrıca kamu hizmetlerinin ortak bir platformdan sunulması için e-dönüşüm Türkiye projesi çerçevesinde sürdürülen bir çalışmadır. 25 Ocak 2005 tarihli bakanlar kurulu kararı ile T.C. E-devlet Kapısı'nın kurulması görevi Türk Telekom'a verilmiştir (Ersoy, 2006).



Şekil 2: E-Devlet Modeli (Lambrinoudakis ve Diğerleri, 2003).

Ayrıca E-Dönüşüm Türkiye Projesine göre, vatandaşlık numarası uygulamasındaki teknik altyapının hızla tamamlanması sağlanarak mevcut vergi, vatandaşlık, sosyal güvenlik vb. numaralarının bilgisayar ortamında vatandaşlık numarası esas alınarak eşleştirilmesinin sağlanması, uygulanmakta olan vergi numarasının gerçek kişiler bakımından vatandaşlık numarası ile birleştirilmesi ve bu numaranın her gerçek kişinin sosyal güvenlikle ilgili olanlar dâhil doğumundan ölümüne kadar kullanılması planlanmış ve hayata geçirilmiştir. Bu kadar büyük öneme sahip olan ve vatandaşların e-devlet üzerindeki uygulamalarının büyük bir bölümünde belirleyici bilgi olan TC kimlik numarasının uygulamalar ya da elektronik doğrulama işlemlerinde tek başına kullanılması güvenlik açısından büyük bir sistem açığı oluşmasına neden olacaktır. Kişi ya da kişilere ait TC kimlik numarası bilgisi çok farklı yollarla üçüncü şahısların ellerine kolaylıkla geçebilmektedir. Elektronik doğrulama işlemlerinde TC kimlik numarası ile birlikte bir de özel şifre kullanılması oturum güvenliği ve buna bağlı olarak bilgi güvenliğinin sağlanması ve oturum kaydının tutulması açısından daha güvenli olacaktır. Amerika'da elektronik doğrulama işlemi için, *isim-soy isim (tamamında kullanılmıyor), e-posta adresi, posta kodu, telefon numarası, ehliyet numarası, parmak*

izi ya da yüz ile ilgili fiziksel bir bilgi ve sosyal güvenlik numarası / ulusal kimlik numarası bilgileri kullanılmaktadır (US-CERT, 2006). Böylece gerçek kullanıcı olmayan kişilerin sistem üzerinde aktif olmaları engellenmiş ve başkalarına ait bilgileri görmeleri engellenmiş olacaktır.

Özellikle bilgi teknolojileri yönetiminde kullanılan uluslar arası standartlar (ISO / IEC: 17799) e-devlet uygulamalarına adapte edilmelidir. Bu standarda göre aşağıdaki düzenlemelerin gerçekleştirilmesi önem arz etmektedir;

3.2. Erişim güvenliği (e-authentication)

Her kullanıcıya ait bir kullanıcı numarası (T.C. Kimlik no) ve bir şifre verilmelidir. Şifrenin unutulması ya da kaybolması durumunda yapılması gereken yeni şifre alma işlemi sadece yetkili bir yerel kurum tarafından gerçekleştirilmelidir. Şifre değiştirme işlemi ise bireysel olarak web sitesi üzerinden gerçekleştirilmelidir. Kullanıcı girişlerinde, site içindeki hizmetlerle ilgili kurallar verilerek kullanıcının onayına sunulmalıdır. Böylece kullanıcıların site içindeki hak ve görevleri sunulmuş olacaktır. Kullanıcıların giriş bilgileri belirli seviyelere göre düzenlenmelidir. Örneğin standart kullanıcı hakları ile yönetici hakları farklı düzeylerde olmalıdır. Kullanıcı ve yöneticilerin site üzerinde gerçekleştirdiği işlemler bir kayıt dosyasında saklanarak istendiğinde geçmişte yapılan işlere ulaşabilme imkânı sağlanmalıdır. Elektronik doğrulama işlemlerinde kullanılacak giriş yapısı aşağıdaki özelliklere sahip olmalıdır;

- Her kullanıcı bir ID ve şifre ile giriş yapmalı,
- Kullanıcılara kendi şifrelerini oluşturabilmeleri, değiştirebilmeleri ve yanlış şifre girişi yapıldığında şifrelerini öğrenebilmeleri için doğrulama prosedürü sunulmalı,
- Kullanıcıların şifrelerini (güvenli, karmaşık) kaliteli seçmeleri sağlanmalı,
- Kullanıcıların servislere ilk giriş yaptıklarında geçici şifrelerini değiştirmeleri sağlanmalı,
- Kullanıcıların daha önce kullandıkları şifreleri yeniden kullanmaları engellenmeli,
- Ekranda şifre girilirken karakterlerin görünmesi engellenmeli,
- Şifreler ayrı ayrı dosyalarda saklanmalı,
- Depolanan ve taşınan şifreler güvenli bir ortamda tutulmalıdır (ISO/IEC:17799, 2005).

3.3. Bilgilerin Sınıflandırılması

E-devlet uygulamaları üzerinden verilen hizmetlerde sorgular sonuncunda elde edilen bilgiler sınıflandırılmalı ve fazladan hiçbir bilgi kullanıcılara verilmemelidir. Hizmetler sonucunda verilen bilgilerin, depolanan bilgilerle aynı ve geçerli olduğundan emin olunması şarttır. Bilgilerin geçerliliği;

- Bilgilerin doğruluğu test edilmelidir.
- İstenilen bilgilerin görüntüleme kayıtları saklanmalıdır (ISO/IEC:17799, 2005).

Böylece fazla bilginin izinsiz / yetkisiz kullanıcıların eline geçmesi engellenmiş, hizmetlerde yer alan kişisel bilgiler güvenlik ve gizlilik açısından korunmuş ve kullanıcılara doğru bilgiler verilmiş olacaktır.

3.4. Kurumlar Arasında Koordinasyon Sağlanması

E-devlet uygulamaları üzerinden yapılacak hizmetler sayesinde devlet kurumlarının yükleri oldukça hafiflemekte ve böylece büyük tasarruflar sağlanmaktadır. Bu hizmetlerin doğru ve verimli bir şekilde sürmesi için kamu kurumlarının bilgileri düzgün ve güvenli bir şekilde paylaşmaları büyük önem arz etmektedir (Liu ve Chetal, 2005). Kurumlar arasındaki bilgi paylaşımları bir elektronik doğrulama sertifikasına dayalı olarak yapılırsa, kurumlar arasında güvenli bilgi aktarımı sağlanarak hem bilgi paylaşım güvenliği hem de bilginin gizliliği korunmuş olacaktır. Ayrıca kurumların bilgileri arasındaki tutarsızlıklar da ortadan kaldırılmış olacaktır.

3.5. E- Okuryazarlık

Sadece bu hizmetin sunulduğu e-devlet uygulamalarında düzenlemelere gidilmesi bilgi ve güvenli açıklarını önlemeye yeterli olmayacaktır. Tüm bu önlemlere ek olarak vatandaşların da yeniçağa ayak uydurmaları ve e-okuryazar olmaları amaçlanmalıdır. Bilgi toplumunun oluşmasına katkıda bulunmak ve e-okuryazarlığın gelişmesine katkıda bulunmak amacıyla MEB bünyesindeki eğitim ve öğretim kurumlarına ait bilgi teknolojisi mekânlarının topluma açılması suretiyle bilgisayar okuryazarlığını arttırmaya yönelik ön çalıma ve gerekli düzenlemelere başlanmıştır (E-Dönüşüm Türkiye, 2003). E-okuryazar bir vatandaş, e-devlet uygulamaları ile sunulan hizmetlerden maksimum düzeyde yararlanabilecek, daha girişimci, daha bilinçli ve aktif bir vatandaş olacaktır. Böylece e-devlet uygulamalarının etkinliğinin de önemli oranda artabileceği düşünülmektedir.

4. Sonuç, Tartışma ve Öneriler

Türkiye'de e-devlet uygulamaları hızlı bir şekilde ilerlemektedir. Pek çok kurum bu işi kendi çabalarıyla yapmaktadır. Ancak bu özverili çaba beraberinde bazı sorunlar da getirmektedir. Kurumların yaptığı web sayfalarındaki sorgulamalar sonucunda elde edilen masum sorgu bilgileri, kurumların birlikte hareket etmemesinden dolayı kötü niyetli kişiler tarafından başka işlemlerde kullanılabilmektedir. OECD'nin raporunda Türkiye'nin e-kapı, yani tek bir portal üzerinden hizmet verir bir model oluşturmadığına, bunun da işleri aksattığına dikkat çekilmektedir (Tuncay, 2006). Bunun için e-devlet hizmetleri tek bir kapı (portal) üzerinden hizmet verecek şekilde düzenlenmelidir. E-devlet, içinde bulunduğumuz yüzyılda vatandaşların ihtiyaçlarından doğan bir yaşam biçimidir. Vatandaşlar bu yapının tamamlayıcı parçalarıdır. Bu yapıda en önemli görev devletle vatandaş arasındaki ilişkilerin elektronik ortamda kesintisiz ve *güvenli* olarak yürütülmesidir (Şahin ve Örselli, 2003). Bu güvenliğin sağlanması için sadece e-devlet uygulamalarında çeşitli tedbirler alınması yeterli olmayacaktır, çünkü e-devlet uygulamaları kurumlar arası bir uyum, bütünlük ve vatandaşın katılımını gerektirmektedir. Bu bağlamda e-devlet yapısının güvenliğini sağlamak için yasal bazı düzenlemelerin yapılması da kaçınılmaz olacaktır. AB mevzuatı çerçevesinde kişisel verilerin korunması ve mahremiyetin gizliliğinin sağlanması önemli bir yer işgal etmektedir. Günümüzün temel bileşenlerinden birisi olan kişisel verilerin korunmasına

yönelik olarak AB tarafından 2002/58/EC ve 95/46/EC sayılı iki adet direktif çıkarılmıştır. 95/46/EC sayılı AB direktifine ilişkin olarak adalet bakanlığı tarafından hazırlanan yasa taslağı halen yasalaşmamıştır (Ersoy, 2006). Tüm e-devlet uygulamalarında uluslararası ve AB standart kuruluşları tarafından yayınlanan standartların Türk Standardı olarak hazırlanması, bilgi, bilginin değişimi, bilgiye erişim, yazılım kalitesi vb. konularda uluslararası standartların takip edilmesi (E-Dönüşüm Türkiye, 2003) gerekliliği vurgulanmasına rağmen e-devlet hizmetlerinin yürütüldüğü web sitelerinde bu standartlara uyum sağlanamamıştır. Kamu kurumlarının web sayfalarında asgari ölçüde sunulması gereken bilginin ve sunum esaslarının tespit edilmesi, uygulamanın sağlanması, web sayfalarının WAI kılavuzu da dikkate alınarak içerik ve tasarım uyumunun sağlanması (E-Dönüşüm Türkiye, 2003) amaçlanmış fakat yerine getirilememiştir. Bunun için yukarıda da belirtildiği gibi Türkiye'de e-devlet uygulamalarının tek kapı üzerinden yürütülmesi e-devlet uygulamalarının gelişimi ve değerlendirilmesi açısından önem arz etmektedir. Ayrıca e-devlet uygulamalarının koordinasyonunu sağlayacak bir bakanlık biriminin de kurulması bu uygulamaların yönetimi, denetimi ve değerlendirilmesi için önemli görülmektedir.

KAYNAKÇA

Arifoğlu, A., Kömes, A., Yazıcı, A., Akgül, M.K., Ayvalı, A., (2002). **E-Devlet Yolunda Türkiye**, Türkiye Bilişim Derneği Yayınları, Ankara.

Baykal, N. Bilgi Teknolojisinin, Ulusal Güvenlik ve Ulusal Güvenlik Stratejisi ile İlgiliBoyutu.http://www.harpak.tsk.mil.tr/duyurular/sempozyum/11%20doc.dr.nazife%20baykal.doc, Erişim Tarihi: 29.06.2007

Caidi, N., Ross, A., (2005). Information Rights and National Security. *Government Information Quarterly 22 (s. 663–684)*.

Chengyu, X. (2002, Ocak). *E-Government in China, Present and Future*. "E-administration for the benefit of citizens" Uluslararası Semineri, Paris.

Clark, E., (2003). Managing The Transformation To E-Government: An Australian Perspective. *Thunderbird International Business Review, 45(4), (s. 377,397).*

E-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (2003–2004). Devlet Planlama Teşkilatı, Ankara.

E-Government Strategy (2003). Implementing The President's Management Agenda for E-Government. Nisan.

Erkul, E. R., (2004). Dünya Kamu Yönetimindeki Dönüşüm ve Türkiye'de Kamu Yönetimi Öğretimine Yansımaları, *II. Kamu Yönetimi Forumu (s. 212–225)*. Hacettepe Üniversitesi Yayınları.

Ersoy, E., (2006). Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması. http://ab.org.tr/ab06/bildiri/6.doc. Erişim Tarihi: 12.04.2007

European Commission (2002). Towards a Knowledge-Based Europe: The European Union and the Information Society. Ekim, 2002.

E-Japonya, www.e-gov.go.jp, Erişim Tarihi: 31.07.2007.

E-Japonya 2002 Programı, http://www.kantei.go.jp/foreign/it/network/0626_e.html, Erişim Tarihi: 31.07.2007.

Halchin, E., L., (2004). Electronic Government: Government Capability and Terrorist Resource. *Government Information Quarterly 21 (s. 406–419).*

Holliday, I., ve Yep, R. (2005). E-government in China. *Public Administration and Development*, 25, 239-249.

http://www.devletim.com/haberler/haber.asp?hbr=582, Erişim Tarihi: 17.07.2007

http://www.kenthaber.com/Arsiv/Haberler/2007/Subat/22/Haber_210340.aspx, Erişim Tarihi: 18.07.2007

http://www.onlinesorgulama.com, Erişim Tarihi: 16.07.2007

ISO/IEC:17799, (2005). **Information Technology-Security Techniques-Code Of Practise For Information Security Management (s. 71)**, International Standart, Second Edition.

Jain, P. (2002). The catch-up state: E-government in Japan. *Japanese Studies, 22(3)*.

Lambrinoudakis, C., Gritzalis, S., Dridi, F., Pernul, G., (2003). Security Requirements For E-Government Services: A Methodological Approach For Developing A Common PKI-Based Security Policy. *Computer Communications 26 (s. 1873–1883).*

Liu, P., Chetal, A., (2005). Trust-Based Secure Information Sharing Between Federal Government Agencies. *Journal Of The American Society For Information Science And Technology, 56, (s. 283–298).*

Spinellis, D., Kokolakis, S., Gritzalis, S., (1999). Security Requirements, Risk And Recommendation For Small Enterprise And Home Office Environments. *Information Management & Computer Security, 7, (s. 121-128).*

Şahin, A., Örselli, E., (2003). E-Devlet Anlayışı Sürecinde Türkiye. *Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi (9)*, 343–356

Şener, M., Paşayiğit, A., (2006). E-Devlette Kalite, Güvenlik ve Kişisel Gizlilik. *İstanbul Teknik Üniversitesi, EMOS Proje Yarışması, Şubat*, İstanbul.

Taylor Nelson Sofres, (2002). Government Online An International Perspective. Annual Global Report, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN007044.pdf. Erişim Tarihi: 30.05.2007

Tolunay, F., Sarı, F. Kamu Kurum ve Kuruluşları ile Özel Kurum ve Kuruluşların Bilgi Teknolojisi Alanında Ulusal Güvenlik Politikası Doğrultusunda Yönlendirilmeleri. http://www.harpak.tsk.mil.tr/duyurular/SEMPOZYUM/09%20prof%20dr%20ersin%20tolunay.doc, Erişim Tarihi: 30.05.2007

Tuncay, E. (2006). Kuyrukları bitirecek sihirli değnek e-devlet için Türkiye yolun başında.http://www.referansgazetesi.com/haber.aspx?HBR_KOD=54319&KTG_KOD=185&ForArsiv=1, Erişim Tarihi: 06.08.2007

US-CERT, (2006). Data Security and Privacy. *DHS Cyber Preparedness eNewsletter. Homeland Security, Eylül, Vol.2, s. 11.*

US-CERT, (2007). Quarterly Trends And Analysis Report.. *Homeland Security, Haziran, 2(2), s. 1–6.*

Yıldız, M., (2003). **Çağdaş Kamu Yönetimi I (s. 318)**, Nobel Yayınevi, Ankara.