Turkish Studies
Information Technologies & Applied Sciences
Volume 13/21, Summer 2018, p. 129-156
DOI Number: http://dx.doi.org/10.7827/TurkishStudies.13874
ISSN: 1308-2140, ANKARA-TURKEY

Research Article/ Araştırma Makalesi

Article Info/Makale Bilgisi
Received/Geliş: Temmuz 2018 **Accepted/Kabul:** Eylül 2018
Referees/Hakemler: Doç. Dr. Erhan ÖRSELLİ - Doç. Dr.Muhammet Fatih Bilal ALODALI

This article was checked by iThenticate.

TÜRKİYE'DE E-DEVLET UYGULAMALARINDA GÜVENLİK RİSKLERİNİN ANALİZİ*

*Önder KUTLU** - İsmail SEVİNÇ*** - Selçuk KAHRAMAN****

ÖZET

Küreselleşme, serbest piyasa dinamikleri ve uluslararası kuruluşların ülkelerin yönetsel yapıları ve işleyişleri üzerindeki etkileri ile teknolojinin ve internet ağlarının yaygınlaşması, e-devlet uygulamalarının neredeyse tüm kamu hizmet alanlarında yer bulmasına olanak sağlamıştır. Nitekim, günümüzde devletin kamu hizmetlerini dijital ortamda sunabilmesi ve devlet kurumlarında işlerin elektronik ortamda yürütülerek bürokrasinin en aza indirgenmesi modern devletin önemli göstergelerinden biri olarak gösterilmektedir. Böylece e-devlet uygulamaları geleneksel kamu yönetimi sorunlarına karşı geliştirilen çözüm sürecinin alternatif bir parçası olarak kabul görmeye başlamıştır.

Kamu yönetiminde güven artırıcı faktörler arasında e-devlet uygulamaları önemli bir yer edinmektedir. Buna karşın e-devlet ile ilgili gizlilik ve güvenlik tartışmaları daha fazla gündeme gelmeye başlamıştır. Bu noktada, vatandaşların yeterli güvenlik ve gizlilik önlemlerinin alınması hususuna daha fazla güven duyması ve bürokrasinin de gizlilik ile ilgili geleneksel direncini değiştirmesi oldukça önemlidir. Bu bağlamda devlet ile vatandaşlar ve özel sektör arasındaki güven ilişkisi ve veri mahremiyetine ilişkin güvenlik sorunsalı daha fazla tartışılmayı gerektirmiştir.

---

* 23-25 Mart 2018 tarihleri arasında Kudüs'te II. Uluslararası İktisat, Hukuk ve Siyaset Sempozyumu'nda sözlü olarak sunulan "*Türkiye'de E-Devlet Uygulamalarında Güven Sorunu ve Güvenlik Riskinin Analizi*" başlıklı bildirinin metinleştirilmiş halidir.

** Prof. Dr., Necmettin Erbakan Üniversitesi, Siyasal Bilgiler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, El-mek: okutlu@konya.edu.tr

*** Doç. Dr., Necmettin Erbakan Üniversitesi, Siyasal Bilgiler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, El-mek: isevinc@konya.edu.tr

**** Araş. Gör., Necmettin Erbakan Üniversitesi, Siyasal Bilgiler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, El-mek: skahraman@konya.edu.tr

E-devlet uygulamalarına yönelik olumsuz güvenlik algısı, esasında, internet ağları üzerinden her geçen gün çeşitli yöntemlerle kişisel ve kurumsal veri mahremiyetinin ihlal edilmesinden kaynaklanmaktadır. Bu açıdan e-devlet uygulamalarının yaygınlaşması ile güvenlik sorunlarının artması üst düzeyde veri güvenliği sorununu gündeme getirmektedir. Bu bağlamda e-devlet uygulamalarının güvenlik boyutunda öncelikli olarak Türkiye'nin temel kamusal ve kurumsal veri altyapısına yönelik eksikliklerini tamamlaması gerekmektedir. Nitekim e-devlet güvenliğinin, en az, ülkelerin coğrafi sınırlarının güvenliği kadar önemli olduğu ifade edilmektedir.

Bu çalışma ilk olarak Türkiye'de kamu yönetimindeki e-devlet hizmetlerine yönelik güven sorunlarını irdelemeyi hedeflemektedir. Ardından bu sorunların önemli bir boyutu olan güvenlik altyapısına yönelik çeşitli çalışmalar ve gelişmelere dikkat çekilecektir. Bu bağlamda, kurumsal ve yönetsel açıdan Türkiye'deki e-devlet uygulamalarının güvenlik altyapısına yönelik risk alanlarına ve politika önerilerine yer verilmeye çalışılacaktır.

Anahtar Kelimeler: e-devlet, güvenlik, siber güvenlik, Türkiye.

ANALYSIS OF SAFETY RISKS OF E-GOVERNMENT APPLICATIONS IN TURKEY

ABSTRACT

Globalization, dynamics of free market, and the impact of transnational corporations on the administrative structures and operations of countries and the spread of technology and internet networks have enabled e-government applications to be found in almost all public service areas. The fact that the state can present public services in digital environment and the work of state institutions is carried out in electronic environment followed by the reduction of bureaucracy is shown as one of the most important indicators of modern state in today's world. Thus, e-government applications have begun to be accepted as an alternative part of the solution process developed against traditional public administration problems.

E-government applications have an important place among the trust building factors in public administration. Discussions about secrecy and security about e-government have begun to come to the agenda more and more in recent times. At this point, it is important that the bureaucracy change its traditional resistance to secrecy and also citizens should also be confident that adequate security and secrecy measures are taken. In this context, the security relationships of the state and the citizens with the private sector and security concerns about data privacy have begun to be discussed more.

The negative security perception for e-government applications is caused by the infringement of personal and corporate data privacy with various methods every day through internet networks. In this respect, the widespread use of e-government applications followed by the increase in security problems raise the issue of data security at a high level. In

this context, in the dimension of security of e-government applications, Turkey needs to complete the shortcomings in the basic public infrastructure and corporate data. Thus, it is stated that e-government security is at least as important as the security of the geographical boundaries of the countries.

This study primarily aims to analyze the issues of trust for public administration on e-government services in Turkey. Then, it is going to draw attention to various studies and developments towards security infrastructure which is an important dimension of these problems. Thus, some suggestions for the security infrastructure of e-government applications will be given from the institutional and administrative points of view.

STRUCTURED ABSTRACT

Trust problems in a public service have two important dimensions as trust in the institution that provides the service and trust in the technical and technological mechanism that mediates the provision of the service. In this context, the acceptance of information and communication technologies by the society is important as a priority. However, when the development and diversity of today's technology is taken into account, it is clear that each technological structure has certain levels of security risks regardless of to what extent the elements of technology are accepted by the society.

Nowadays, the discussions about secrecy and security about e-government are beginning to come to the agenda more and more. At this point, it is very important for the bureaucracy to change the traditional resistance of secrecy and it is also important that the citizens to have trust that adequate security and secrecy measures are taken. Every risk involved in technological devices is being updated, so the confidence can be weakened. As a matter of fact, potential risks related to information and data security are increasing in direct proportion with developing technology tools. In the process of spreading electronic government applications, it is also important to provide secure technological infrastructure and to protect the privacy of personal data. In addition to this, an international cooperation on data security in the electronic environment is also proposed. Especially in the case of cyber crimes that exceed borders, it may be necessary to be taken joint measures by different states.

The first measure that necessary for e-government systems to be operated as a trust building factor in public administration is the development of secure softwares. As electronic businesses and transactions increase in public institutions and organizations in particular, current threats and dangers are more frequently encountered. In this context, the development of secure software techniques and the security of websites become very important. Undoubtedly, providingsecrecy and security for users by the implementation of the design of mandatory technological infrastructure is one of thes indispensable conditions for the success of e-government applications. From this point of view, it is necessary to protect the authenticity of every kind of document produced in the e-government environment from the

production stage to the archiving stage in compliance with the fundamental standards and in secure conditions.

In the security dimension of e-government applications, Turkey primarily needs to complete the gaps in the basic public infrastructure and corporate data. In addition, personal data stored in public institutions with various reasons, especially public security, has gained a new dimension along with improvements in information and communication technologies. In particular, the spread of cybercrime has led to the need to protect personal data and to take necessary security measures in e-government systems.

In Turkey, with regard to e-government services, a direct strategy document and action plan for e-government services at the national level was preparedfor the first time. Various strategic goals and action plans were documented for the first time under the title of "National E-Government Strategy and Action Plan 2016-2019", which were said to be prepared by using national resources. On September 9th of 2016, 2016-2019 National Cyber Safety Strategy and Action Plan was announced to the public in a publicity meeting in Ankara. In the National E-Government Strategy and Action Plan 2016-2019, cyber security has become one of the main emphases in strategic objectives for the technical and managerial infrastructure of e-government services. Thus, the security dimension in e-government services and applications was handled as related to cyber security risks. For this reason, the problem of security in government services carried out at the electronic level has begun to be considered together with the concept of cyber security.

When e-government policies determined in the National E-Government Strategy and Action Plan 2016-2019 at the national level; Turkey's own conditions, global developments, technological innovations and trends, and cyber security are all considered as main priorities for the development of e-government applications in public services. Moreover, one of the most important topics in e-government projects in Turkey was also the risk of information security. In this context, it is aimed to increase the competencies of related e-government institutions and to develop new softwares in common infrastructures in order to eliminate system security risks like cyber attacks in e-government projects.

The necessary attention on the cyber security issues in Turkey has started to be given recently, although it has been voiced by experts for long years. Ensuring the security of e-government systems developed by public institutions and organizations in Turkey, to be brought into line with international information security standards and controls must be based on the creation of a sustainable security structure. Work on information security and protection of personal data should be developed and institutional responsibilities should be reorganized, especially in the field of cyber security. It is also very important to educate the technocrats and technical personnel who are in charge of the cyber security in the state institutions.

In order the government and decision-makers to provide a high level of protection on e-government applications in Turkey, they need to be institutionalized to follow closely the technological developments and they need financial resources and human resources increasingly each

passing day. These needs are, of course, closely related to the diversity of risks that threaten e-government security. Even in the countries which are accepted as leaders in the area of information systems, many different examples have been experienced that can bring down e-government systems. Therefore, Turkey needs to follow a more serious way of handling its responsibilities in this area. In addition, the production of critical technologies in Turkey andtaking measures to ensure that the exported technologies can be used safely are necessary for Turkey.

It should be utilized in a variety of security models suggestions when designing e-government system in Turkey, and relevant technologies should be considered as multi-dimensional. However, for the cases arising from the secrity vulnerabilities in e-government services or technical problems, Turkey needs a risk management program. On the other hand, some e-government systems are experiencing delays and problems in e-government services due to the high demand from citizens. The importance of managing security risks in combating these problems should be taken into account more and more. In addition, when security risks are analyzed in e-government services, auditing functions that enter into the field of responsibility of public administrations in electronic environments should not be ignored.

Keywords: e-government, security, cyber security, Turkey.

Giriş

Mekâna bağlılığın sanal alana taşınması ile kamu yönetiminde hizmet sunma anlayışı önemli oranda değişime uğramıştır. Bu açıdan kamu yönetiminin ve unsurlarının artan bir şekilde bilgi ve iletişim teknolojilerine bağımlılığı oldukça önemlidir. Bununla birlikte geleneksel kamu yönetimi sorunlarına yeni çözümler üretmek adına devletin neredeyse her türlü kamu hizmet alanında yeniden yapılandırılmasına başlanmıştır. Bu bağlamda elektronik devlet (e-devlet) uygulamaları, bu sürecin alternatif bir parçası olarak ortaya çıkmıştır.

E-devlet uygulamalarının kamu yönetimi açısından olumlu yönleri, esasında kamu yönetiminin geleneksel sorunları ile yakından ilişkilidir. E-devlet uygulamalarını ortaya çıkaran çeşitli nedenler bulunmakla birlikte günümüzde e-devlet uygulamalarının yönetsel sorunları daha fazla gündeme gelmiştir. Bu noktada devlet ile vatandaşlar ve özel sektör arasındaki güven ilişkisi ve veri gizliliğine ilişkin güvenlik sorunsalı daha fazla tartışılmaktadır. Bu açıdan, bir tarafta küreselleşme ve serbest piyasa ortamının yaygınlaşması, bir taraftan da e-devlet uygulamalarının hem özel sektör hem de devlet kurumları açısından yaygın olarak kullanılmaya başlanması e-devlet ile ekonomik, yasal ve yönetsel gelişmeler arasındaki ilişkilerin yeniden düzenlenmesini gerektirmiştir. Bu süreçte ekonomik faaliyetlerin daha verimli gerçekleştirilebilmesi, yönetsel faaliyetlerin ise daha kaliteli ve verimli hizmet sunumlarına olanak verebilmesi adına e-devlet uygulamaları önemli bir araç olarak ele alınmaktadır.

Kamu yönetiminde güven sorununun yeni ve en önemli boyutlarından birisi elektronik ortamda sürdürülmeye çalışılan kamu hizmetlerinin güvenlik altyapısına yönelik ya da hizmet sunumunun taraflarına ait bir kısım gizli veri ve bilginin kötü amaçlarla dolaylı ya da doğrudan bir şekilde elde edilmesidir. Bu tür durumlar karşısında vatandaşların kamu yönetimine yönelik güven(siz)lik sorunu daha fazla artabilmektedir. Nitekim günümüzde küresel çapta görülen kişisel ve kurumsal her türlü bilgi, belge ve verilerin açığa çıkartılması, salt vatandaşlar açısından bir güven sorununa değil ulusal ve küresel güvenliği tehdit edebilecek sorunlara da yol açabilmektedir. Bu açıdan kamu yönetiminde güven olgusunun en önemli boyutlarından birisinin teknik ve teknolojik

altyapı sorunlarında yatmakta olduğu göz ardı edilmektedir. Bu nedenle kamu yönetiminde güven olgusunun oluşması her geçen gün değişime uğrayan ve elektronik ortamlara taşınan kamu hizmetlerinin güvenliği ile yakından ilişkili olduğu görülmektedir.

Tarihin çeşitli dönemlerinde insanlar güvenlik adına temel hak ve özgürlükleri sınırlandırıcı pek çok toplum sözleşmesine onay vermiştir. Bu açıdan güvenlik meselesi sıradan bir konu olarak ele alınamayacak kadar çok katmanlı bir olgudur. Güvenlik konularının önemli ilişkilerinin başında kamu yönetiminin olması ise ayrı bir önem kazanmaktadır. Özellikle kamu yönetiminde e-devlet hizmetlerinin yaygınlaşması ve küresel düzeyde risk alanlarının çeşitlenmesi dikkate alındığında önemi bir kat daha artmaktadır. Kuşkusuz e-devlet tanımlamalarının temel unsurları arasında güvenli hizmet sunumu yer almaktadır. Bu çalışmada ilk olarak e-devlet ve güvenlik ilişkisi esas alınarak dünyada ve Türkiye'de e-devlet uygulamalarına geçişin temel nedenlerine yer verilecek, ardından kamu hizmetlerinin güvenlik altyapısına yönelik farklı boyutlar irdelendikten sonra dünyadaki çeşitli örnekler, deneyimler ve çalışmalar ortaya konulmaya çalışılacaktır. Son olarak Türkiye'de e-devlet uygulamalarındaki güvenlik risklerine dikkat çekilerek çeşitli politika önerilerinin sunulmasına çalışılacaktır.

1. Kamu Yönetiminde Güven Sorunu ve Güvenlik Altyapısı

Kamu yönetiminde güven sorunu daha çok kamu kurum ve kuruluşlarının işleyişi ve vatandaşlarla olan ilişkileri üzerinden ele alınmaktadır. Bu noktada kurumsal gelenekler, uzmanlaşma standartları, yasal düzenlemeler, politik gelişmeler ve pozisyonlar ile teknik ve mali olanaklar kurumsal güvenle yakından ilişkilidir (Landau ve Krueger, 1998; Sinclair ve Irani, 2013: 59; Şahin, Örselli ve Taşpınar, 2016: 85-87). Bir yandan vatandaşlar açısından kamu kurum ve kuruluşlarından adil ve eşit hizmet beklentileri önemli iken diğer yandan hükümetlerin de kamu kurumları üzerindeki denetim yollarının etkinlik derecesi yönetimde güven olgusunun geleceğini belirlemektedir. Böylece devlet kurumlarının performansı ve devlet kurumları hakkındaki şeffaf bilgiye erişim olanaklarının artması vatandaşların kamu kurumlarına olan güvenini etkileyebilecektir. Bütün bunlar kadar teknolojinin ulaştığı boyutların kontrol altına alınabilmesi ve teknolojiden en iyi ölçüde yarar sağlanabilmesi için devletlere ve hükümetlere önemli görevler düşmektedir.

Bir kamu hizmetine yönelik güven sorununun, hizmeti sunan yapıya güven ve ilgili hizmetin sunumuna aracılık eden teknik ve teknolojik mekanizmaya olan güven olmak üzere iki önemli boyutu bulunmaktadır (Tolbert ve Mossberger, 2006: 354; Carter ve Weerakkody, 2008: 475; Tarhan, 2011: 230). Bu nedenle bilgi ve iletişim teknolojilerinin toplum tarafından öncelikli olarak kabul görmesi önemlidir. Ancak teknolojik unsurlar, toplum tarafından ne ölçüde kabul görürse görsün günümüzdeki teknolojinin gelişimi ve çeşitlenen boyutu dikkate alındığında her bir teknolojik yapının belirli düzeylerde güvenlik risklerini barındırdığı açık bir durumdur. Bu bağlamda etkin güvenlik politikalarının kamu yönetiminde öncelikli olarak benimsenmesi gerekmektedir.

Özellikle elektronik ortama taşınan bilgilerin korunabilmesi ve kurumların karşılaşabileceği olası risklerin önüne geçilebilmesi için bilgi güvenliği yönetim sistemlerinin kamu kurum ve kuruluşlarında üst düzey yöneticilerin de yardımıyla uygulanabilmesi oldukça önemlidir. Vatandaşların ve kurumların bilgi güvenliğinin basit yazılımlarla ve çeşitli elektronik saldırı yöntemleri ile sürekli risk altında bulunduğu dikkate alındığında, güvenlik zincirinin personel ya da insan kaynağı en zayıf halkası olarak ifade edilmektedir (Vural ve Sağıroğlu, 2008a: 507-508). Bu nedenle e-devlet hizmetlerinin uygulanması sürecinde güven ve güvenlik sorunlarının giderilebilmesinde uzman ve güvenilir insan kaynaklarına çok fazla ihtiyaç bulunmaktadır.

Kamu kurum ve kuruluşlarında elektronik iş ve işlemler arttıkça güncel tehdit ve tehlikelerle daha fazla karşılaşılmaktadır. Bu bağlamda güvenli yazılım tekniklerinin geliştirilmesi ve web sitelerinin güvenliği ile ilgili çeşitli çalışmalar yapılmaktadır. Bu alanda ciddi çalışmalar yapan pek

çok kuruluş bulunmaktadır. Örneğin bunlardan birisi 2001 yılında kurulan, web uygulama güvenliğinin artırılmasına yönelik ücretsiz araçlar ve standartlar üreten, güvenlik forumları düzenleyen ve ilgili yayınlar hazırlayan "The Open Web Application Security Project (OWASP)" adlı kuruluştur. Bir diğeri ise 2004 yılında kurulan, kurumların web siteleri ile ilgili açık standartların geliştirilmesi ve yaygınlaştırılmasını hedefleyen "The Web Application Security Consortium (WASC)" adlı kuruluştur (Demchenko vd., 2005; Gordeychik, Grossman ve Khera, 2010: 4). Bu kuruluşların e-devlet uygulamalarını da yakından ilgilendiren beş temel konu üzerinde yoğunlaştıkları görülmektedir. Bu konular arasında; kimlik doğrulama sistemleri, web sitelerinde yetkilendirme açıkları, kod yazılımlarındaki sorunlar, yapısal programlama dili ve komut çalıştırma sorunları yer almaktadır (Sindre ve Opdahl, 2005; Vural ve Sağıroğlu, 2008a: 517-519; Subashini ve Kavitha, 2011).

Bilgi teknolojileri alanında yaşanan hızlı gelişmeler, bir yandan önemli fırsatlar sunarken diğer yandan da öngörülen ya da öngörülemeyen birçok tehdit unsurunu da beraberinde getirmektedir (Örselli ve Taşpınar, 2016: 19). Muhtemel tehditlerin önlenebilmesine yönelik güçlü bir kurumsal risk yönetimine ihtiyaç bulunduğu belirtilmektedir (Zhou ve Hu, 2008: 208). Devletler, hükümetler, kamu kurum ve kuruluşları, elektronik ortamda sunulan tüm kamu hizmetlerindeki risk unsurlarının yönetiminde yerel ve ulusal hususlar ile uluslararası standartları, yasal ve mali ihtiyaçları ve denetim işlevlerini yerine getirebilmelidir. Ayrıca riskin kontrol edilebilmesine yönelik koordineli faaliyetlere ihtiyaç duyulması, ilgili kurumların mevzuatları ile uyumlu olması, doğru uygulama yazılımlarının tercih edilmesi ve risklerin analiz aşamasında nicel ya da nitel risk analiz ölçümlemelerinden yararlanılması gerekmektedir. Bu açıdan bilgi teknolojilerine ait risklerin yönetilmesinde yeni arayışların, yöntemlerin ve çözüm önerilerinin geliştirilmesi bir zorunluluk olarak ifade edilmektedir (Şahinaslan, 2013: 573-574).

2. E-Devlet Uygulamalarına Geçiş Nedenleri

Günümüzde modern devletin önemli göstergelerinden biri olarak devletin kamu hizmetlerini dijital ortamda sunabilmesi (Örselli vd., 2018: 701) ve kamu kurumlarında işlerin elektronik ortamda yürütülerek bürokrasinin en aza indirgenmesi gösterilmektedir (Eren ve Durna, 2005: 139; Doğan, 2015: 390). Bu nedenle geleneksel bürokratik işlem aşamaları yerine e-devlet sistemleri üzerinden sanal bürokrasinin daha yararlı olacağı savunulmuştur (Baştan ve Gökbunar, 2004: 72). Bilişim teknolojilerinin kamu hizmetlerinde kullanılması elektronik devlet (e-devlet) kavramının ortaya çıkmasının temel nedenleri arasında yerini alarak kamu yönetiminde yeni bir paradigmanın oluşumunu sağlamıştır. Nitekim, bir yandan bilgiyi üreten, diğer yandan da teknolojiyi etkin bir biçimde kullanan ülkeler küresel rekabet ortamında önemli kazanımlar elde etmeye başlamıştır. Bununla birlikte e-devlet uygulamalarının geliştirilmesinde ve yaygınlaştırılmasında özellikle gelişmiş ülkeler açısından öncelikli amaçlar arasında bürokratik işlemlerin azaltılması, kaynak tasarrufunun sağlanması ve vatandaşlara daha hızlı hizmet sunulabilmesi yer almıştır (Naralan, 2008: 2).

Kamu yönetiminde güven artırıcı faktörler arasında e-devlet uygulamaları önemli bir yer edinmektedir (Tolbert ve Mossberger, 2006: 354; Delibaş ve Akgül, 2010: 112-113). Buna karşın, vatandaşların e-devlet memnuniyeti ile yönetime güven arasında doğrudan bir ilişki söz konusudur. Daha açık bir ifadeyle e-devlet uygulamalarına duyulan güven, devlete duyulan güvene de bağlıdır (Kıvanç vd, 2006: 106; Şahin, 2007: 173). Bu bağlamda e-devlet, vatandaşlar ile kamu kurumları arasında çevrimiçi bilgi alışverişine ve çeşitli elektronik ağlara olanak sağlayarak aracılık eden ve vatandaşların güvenine ihtiyaç duyan bir yapıdır. Bu nedenle e-devlet uygulamalarında bilgi ve verinin yüklendiği elektronik sisteme, sistemin bağlı olduğu kuruma ve sistemin devamlılığını sağlayan personele güven oldukça önem arz etmektedir (Şahin, Örselli ve Taşpınar, 2016: 109).

Devlet ile vatandaşlar arasındaki güvenin güçlendirilmesinde e-devlet uygulamalarının nasıl işlediği oldukça önemlidir (Şişman, Alkış ve Maraş, 2011: 29; Karkın ve Özgür, 2012: 97;

Ghernaouti, 2013: 19). Özellikle olumsuz örnekler ve tecrübelerin artması e-devlet uygulamalarına çeşitli açılardan bakılmasını ve yeni çözüm önerilerinin geliştirilmesini gerektirmektedir. Örneğin kişisel verilerin korunmasına yönelik doğrudan bir yasal düzenlemenin uzun bir süre gecikmiş olması Türkiye'de e-devlet hizmetlerinin kullanımında çeşitli endişelerin sürekli dile getirilmesinde etkili olmuştur. Bu nedenle e-devletin temel hedefleri arasında yer alan yönetimde güven ortamının geliştirilmesi gerekmektedir (Şahin ve Örselli, 2003: 349-350). Böylece vatandaşların e-devlet hizmetlerinde ve uygulamalarında sorun alanlarının asgari düzeylere çekilerek güven duygusunun oluşturulması e-devletin başarılı bir şekilde işleyebilmesini de etkileyecektir.

Akıllı devlet, dijital devlet vb. terimlerle de ifade edilen e-devlet olgusu hakkında literatürde çeşitli tanımlara rastlamak mümkündür. Ancak e-devlet tanımlarından önemli bir bölümü kamu kurumları ile vatandaşlar arasındaki pek çok kamu hizmetinin sürekli ve güvenli bir şekilde yürütülmesine odaklanmıştır (Kıvanç vd., 2006: 104; Durna ve Özel, 2008: 4). Bu açıdan e-devlet uygulamalarının en önemli unsurlarının başında, yapılan işlemlerin güvenli bir ortamda sürdürülmesi gelmektedir (Yılmaz, Ulus ve Gönen, 2015: 136). E-devlet tanımlarının temel vurguları arasında ise bilişim stratejilerinin stratejik kullanımı, katılımcı, şeffaf ve hesap verebilir bir yönetim yapısı ile güvenilir hizmet erişimi ve sunumu yer almaktadır (Metin, 2012: 98).

Tablo-1: Geleneksel Devlet ile E-Devlet Arasındaki Temel Farklılıklar

Geleneksel Devlet	E-Devlet
Pasif Yurttaş	Aktif Müşteri Yurttaş
Kâğıt temelli iletişim	Elektronik iletişim
Dikey/Hiyerarşik yapılanma	Yatay/koordineli ağ yapılanması
Yönetimin veri yüklemesi	Vatandaşın veri yüklemesi
Garip raporlama sistemleri	Bilgiye esnek erişim
Personel yanıtı	Otomatik sesli posta, çağrı merkezi vb.
Personel yardımı	Kendi kendine yardım/uzman yardımı
Personel temelli denetim mekanizması	Otomatik veri güncellemesiyle denetim
Nakit akışı/çek	Elektronik fon transferi (EFT)
Tek tip hizmet	Kişiselleştirilmiş/farklılaştırılmış hizmet
Bölümlenmiş kesintili hizmet	Bütünsel/sürekli/tek-duraklı hizmet
Zaman tüketen süreçler	Hızlı seri iş süreçleri
Yüksek işlem maliyetleri	Düşük işlem maliyetleri
Verimsiz büyüme	Verimlilik yönetimi
Tek yönlü iletişim	Etkileşim
Uyruk ilişkisi	Katılım ilişkisi
Kapalı devlet	Açık devlet
İzole edilmiş yönetsel işlevler	Açık ve şeffaf yönetim
Birbirinden kopuk bilgi teknolojileri	Bütünleşik ağ yapısı

Kaynak: Şahin ve Örselli, 2003: 347; Çelen, Çelik ve Seferoğlu, 2011: 64.

Kuşkusuz geleneksel kamu yönetiminde kırtasiyecilik, katı hiyerarşik yönetsel işleyiş, uzun süreli prosedürler, kaynak israfı, şeffaf olmayan devlet anlayışı vb. sorunlar e-devlet uygulamalarına geçiş ile birlikte büyük ölçüde değişime uğramıştır. Bununla birlikte kamu hizmetlerinin teknoloji ile bütünleşmesi ile kamu yönetiminin yapısı, işleyişi ve performans süreçleri de reforma uğramıştır. Bu açıdan e-devlet anlayışının gelişimi kamu yönetiminin yeniden yapılandırılması süreci ile de yakından ilişkili olmuştur. Böylece yönetsel reform pratiklerinin bilişim teknolojilerinin de etkisiyle daha hızlı bir şekilde kamu kurum ve kuruluşlarında yerleşmeye başladığı ifade edilmektedir (Ma, Chung ve Thorson, 2005; Kraemer ve King, 2006).

E-devlet uygulamalarına geçiş nedenlerinden birisi de bilgi ve belge güvenliğinin bir parçası olan depolama işlemidir. Bu noktada fiziksel depolamanın elektronik depolamaya oranla daha fazla

güvenlik riskine sahip olduğu öne sürülmektedir. Böylece elektronik belge yönetimi sistemlerinin geleneksel sistemlere göre daha güvenli olduğu ifade edilmektedir (Odabaş, 2009: 415). Her ne kadar bu tür görüşler savunulsa da, günümüzde teknolojik gelişmelerin hızlı ve öngörülemeyen değişimi, küresel düzeyde çeşitli siber saldırılar, çökertilen yazılımlar ve programlar, e-devlet kurumları üzerindeki güvenlik kaygılarını her geçen gün artırmaktadır.

E-devlet uygulamalarının önemli bir yönü de kamu yönetimlerinin işletme yönetiminin temel ilkeleri çerçevesinde ele alınması düşüncesine dayanmaktadır (Zengin, 2017: 615). Bununla birlikte küreselleşme, serbest piyasa dinamikleri ve ulus-ötesi kuruluşların ülkelerin yönetsel yapıları ve işleyişleri üzerindeki etkileri ile teknolojinin ve internet ağlarının yaygınlaşması e-devlet uygulamalarının neredeyse tüm kamu hizmet alanlarında yer bulmasına olanak sağlamıştır. Bu noktada elektronik yönetişim (e-yönetişim) kavramı da gündeme gelmiştir. E-yönetişim ise vatandaş ya da müşteri odaklı beklentileri esas alan bir yönetim anlayışını yaşama geçirmeyi hedeflemektedir. Böylece vatandaşların her türlü kamusal hizmete ilişkin bilgiye ulaşması ve hizmet alım süreçlerini daha da kısaltarak hizmetlerden hızlı ve verimli bir biçimde yararlanması ve kamusal işlem maliyetlerinin önemli ölçüde azaltılması sağlanmaktadır. Kuşkusuz e-yönetişim faaliyetlerinin başarısında ulusal strateji, politik liderlik, yönetici personelin tutumu vb. etmenler oldukça belirleyicidir (Demirel, 2000: 73). Bu bağlamda e-devlet uygulamaları yönetimin çeşitli boyutları ile eşzamanlı bir biçimde genişlemektedir.

3. E-Devlet Uygulamalarında Güvenlik Riskleri ve Çeşitli Önlemler

Günümüzde e-devlet ile ilgili gizlilik ve güvenlik tartışmaları daha fazla gündeme gelmeye başlamıştır. Bu noktada bürokrasinin gizlilik ile ilgili geleneksel direncini değiştirmesi ve yeterli güvenlik ve gizlilik önlemlerinin alındığına vatandaşların da güven duyması oldukça önemlidir (Durna ve Özel, 2008: 20). Nitekim cep telefonları, akıllı televizyonlar vb. gündelik yaşamın birer parçası haline dönüşen cihazların özellikleri, yazılımları ve internet ağlarına bağlılıkları teknolojinin yararları kadar olumsuzluklarının da kullanıcılar tarafından önemsenmesine neden olmuştur. Bu bağlamda teknolojik aygıtların içerdiği her bir risk olasılığı güncellenmekte ve güven duygusunu zayıflatabilmektedir. Yapılan bazı araştırmalar, akıllı televizyonlar üzerinde zararlı yazılımların düşük maliyetle bulaştırılabildiğini ortaya koymaktadır. Yine WikiLeaks belgelerinde "Weeping Angel" adlı televizyon markasına sahip yüz binlerce kişinin kendi rızaları olmaksızın izlendiği belirtilmektedir (www.theguardian.com/, 2017).

E-devlet uygulamalarında her bir yazılım ve şifreleme sistemi birtakım riskleri içerisinde barındırmaktadır. Bununla birlikte bilgisayar destekli şifreleme teknikleri çok düzeyli bilgiye ihtiyaç duyan çeşitli güvenlik önlemlerine dayalı tekniklere sahiptir. Ancak her bir yeni tekniğin süreç içerisinde başka güvenlik açıkları ile karşı karşıya kaldığı ve herhangi bir şifreleme yönteminin sonlu bir süre sonrasında çözülebileceği ifade edilmektedir (Milani, Pehlivan ve Pour, 2013: 519). Bu nedenle hükümetlerin kamu kurum ve kuruluşlarında uygulanan e-devlet hizmetlerine yüksek koruma sağlayabilmesi için teknolojik gelişmeleri yakından takip edebilmesi, gerekli mali kaynakları ve uzman personeli temin edebilmesi gerekmektedir.

2000'li yıllardan itibaren e-devlet güvenliğini tehdit eden zararlı virüsler ve programlar çeşitli yöntemlerle kamu kurum ve kuruluşlarından özel sektöre kadar çeşitli bilgi sistemlerini olumsuz yönde etkilemiştir. Bu saldırı yöntemlerinden birisi ise kurumsal bilgi ve veri kaynaklarına yönelik casus programların 'sazan avlama' (phishing) adı verilen saldırı yöntemi ile karşılaşması olmuştur (Bahtiyar, 2003). Bu saldırı yönteminde elektronik hizmetlerde kişiler hedef olarak seçilmekte ve soygunlar gerçekleştirilmektedir. Dünyaca ünlü bir firma tarafından geliştirilen ve web tarayıcılarıyla uyumlu bir şekilde çalışan güvenlik yazılımı aracılığıyla bu tür yöntemle yapılan saldırılar 2005 yılında 41.000 adet olarak tespit edilirken, 2006 yılında ise bu sayı 609.000 olarak tespit edilmiştir. Bu nedenle kamu kurum ve kuruluşlarının güvenlik teknolojilerine yeterince yatırım yapmadıklarından yakınılmaktadır (Vural ve Sağıroğlu, 2008a: 508).

Türkiye'de de e-devlet kurumlarının güvenliğini tehdit eden zararlı saldırılara yönelik Ulaştırma, Haberleşme ve Denizcilik Bakanlığı resmi internet sayfasından zaman zaman çeşitli bilgiler ve uyarılar paylaşılmaktadır. Örneğin 18 Şubat 2015 tarihinde paylaşılan "CryptoLocker Virüsü Hakkında Bilgilendirme" başlıklı duyuruda bilgilendirme notu ve tanıtıcı bir yazılım paylaşılmıştır. Bahsedilen virüsün fidye isteyen virüs kategorisinde (ransomware) zararlı bir yazılım olduğu, Türkiye'de o tarihler itibariyle genellikle elektronik fatura (e-fatura) içeren sahte postalar ile yayıldığı ve özellikle kurumsal bilgisayarlardaki çalışmalara zarar verdikleri belirtilmiştir. Bununla birlikte Crypto Locker virüsüne ilişkin teknik ayrıntıları ve alınabilecek önlemleri içeren bir bilgilendirme broşürü hazırlanmış ve Jandarma Genel Komutanlığı tarafından hazırlanan ve virüsle ilgili süreçlerin uygulamalı olarak görülebildiği eğitici tanıtım yazılımı paylaşılmıştır (www.udhb.gov.tr/, 2015).

E-devlet hizmetlerinde kullanıcıların bilgilerinin güvenli bir ortamda saklanması ve kullanıcıların gizlilik ilkelerinin uygulandığından emin olması gerekmektedir (Carter ve Belanger, 2005: 5; Welch, Hinnant ve Moon, 2005: 371; West, 2004: 15; Sevinç ve Şahin, 2013: 201). Bu açıdan e-devlet uygulamalarının bilgiye erişim konusunda internet vb. güvensizlik duygusu oluşturan ortamlarda yapılması nedeniyle bu elektronik ortamlar ve uygulamalarda bilgi ya da veri güvenliğinin sağlanması oldukça önemlidir (Kaşıkçı vd., 2014: 238). Bu bağlamda yüksek düzeyde yönetsel ve kurumsal veri güvenliğinin oluşturulması gerekmektedir (Panagopoulos, 2004). Bu noktada e-devlet güvenliğinin en az ülkelerin coğrafi sınırlarının güvenliği kadar önemli olduğu ifade edilmekte ve e-devlet hizmetlerinde güvenlik unsurları aşağıdaki şekilde sıralanmaktadır (Lambrinoudakis, vd., 2003; Stibbe, 2005: 8-10; Sağıroğlu ve Vural, 2010; Çelen, Çelik ve Seferoğlu, 2011: 68):

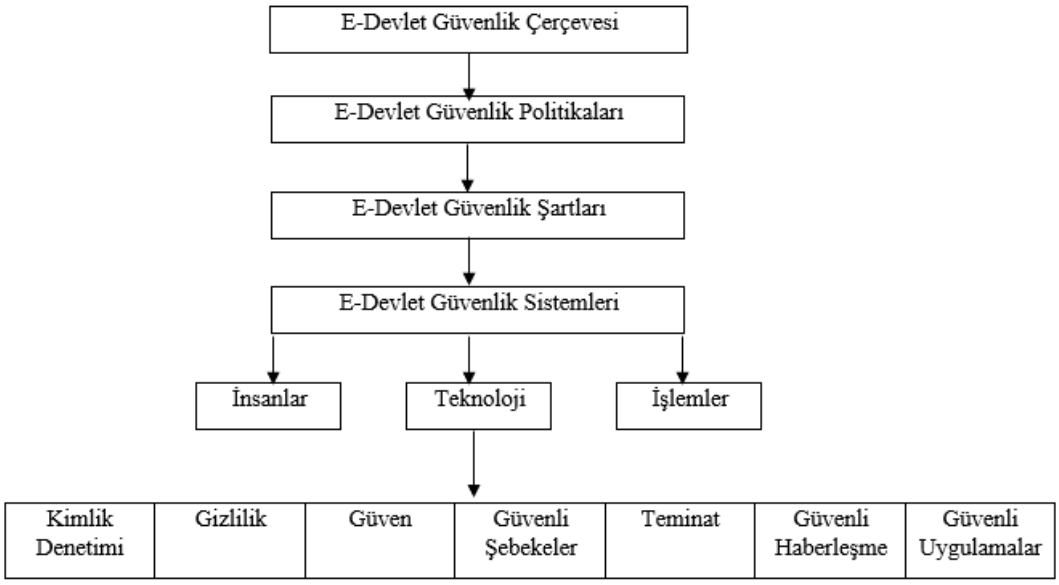
- Gizlilik
- Veri bütünlüğü
- İzlenebilirlik veya kayıt tutma
- Süreklilik
- Kimlik sınaması
- Güvenirlik
- İnkar edememe

Kuşkusuz e-devlet uygulamalarının başarıya ulaşmasında olmazsa olmaz şartlar arasında zorunlu teknolojik altyapı tasarımının gerçekleştirilmesi ve uygulanması ile kullanıcılar açısından gizlilik ve güvenliğin sağlanması gelmektedir (Belanger ve Hiller, 2008; Keskin, 2011: 1718). Bununla birlikte e-devlet ortamında üretilen her türlü belgenin, üretim aşamasından arşivleme aşamasına kadar temel standartlara uygun ve güvenli koşullarda özgün niteliğinin korunması gerekmektedir (Odabaş ve Polat, 2008: 6). Örneğin Avrupa ülkelerinde elektronik posta (e-posta) ve elektronik tebligat (e-tebligat) güvenliği oldukça tartışılan konuların başında gelmiştir. Nitekim elektronik ortamda tebligat hizmetlerine olanak sağlayan çeşitli yasal düzenlemelerle bu hizmetlerin güvenli bir şekilde yürütülmesi hedeflenmiştir (Tanrıkulu, 2009: 319-320). Bu bağlamda e-devlet uygulamalarında güvenlik altyapısının çerçevesi daha açık ve net bir şekilde ortaya konabilmelidir.

Türkiye'de, belgelerin fiziksel ve elektronik ortamda oluşturulmasında kullanılan üst verilerde ortak bir terminoloji ve standardın bulunmaması, özellikle elektronik belge yönetim sistemlerinin (EBYS) devlet kurumlarında yaygınlaşması ile daha önemli bir hale gelmiştir. Bu bağlamda üst veri modellerinin oluşturulması ve geliştirilmesi gerekmektedir. Bir doktora tezi araştırmasında Türkiye'de 2009-2010 yılları arasında kamu kurum ve kuruluşlarında belgeler için kurulan üst veriler derlenerek bir sınıflandırmaya tabi tutulmuş ve E-Devlet Üstveri Modeli (EDuS)

ortaya atılmıştır (Yalçınkaya, 2014). Çeşitli üst veri türleri olmakla birlikte kimlik ve güvenlik ile şifreleme anahtarı gibi unsurlar teknik üst veri olarak adlandırılmaktadır. Teknik üst veriler EBYS'ye olan güvensizlik nedenleri arasında genelde sıralanmamakla birlikte oldukça önemlidir. Çünkü üst verilerin kamu yönetimlerinin kullanım amaçları arasında belgelere erişim haklarını ve ilgili kısıtlılıkları belirleme ve yetkilendirme rolü bulunmaktadır.

Tablo-2: E-Devlet Güvenlik Kapsamının Temel Bileşenleri



Kaynak: İnalöz, Ünver ve Alkan, 2008: 11.

Tablo-2'de yer alan bilgiler de dikkate alındığında e-devlet güvenliği e-devletin ileri aşamalara ulaşmasını sağlayan en önemli faktörlerden birisidir. E-devlet sistemlerinin başarılı bir şekilde işletilebilmesi için ilgili hizmetlerin tüm tarafları arasında güvenlik düzeyinin korunması gerekmektedir. Bu açıdan e-devlet sistemlerinde çeşitli güvenlik modeli önerileri geliştirilmiştir. Bu modeller içerisinde güvenliği artırmak üzere kullanılacak teknolojinin çok boyutlu olarak dizayn edilmesi gerektiği temel vurguların başında gelmiştir. Bununla birlikte e-devletin karşılaştığı belli başlı güvenlik risklerini şu şekilde sıralamak mümkündür (İnalöz, Ünver ve Alkan, 2008: 11-12):

- Bilgi yollarının kesintiye uğraması ya da kötü maksatlı ele geçirilmesi
- Orijinal bilgilerin tahrif edilmesi
- Hizmetlerin ortadan kaldırılması (hacker saldırıları, virüs vb.)
- Sistem kaynaklarının çalınması
- Elektronik sistemdeki sertifikaların ve sistem işleyişi hakkındaki bilgilerin taklit edilmesi

Kuşkusuz tüm bu güvenlik risklerinin yönetimi esasında risk tanımlaması, risk analizi ve risk kontrolü olmak üzere üç temel aşamayı kapsamakta ve bu aşamaların denetim boyutu ise oldukça önemlidir. Bu süreçte yönetim ilkelerinden olan denetim bazen kısmen bazen de tümüyle elektronikleşen bir yapı haline gelebilmektedir. Elektronik ortam üzerinde denetim yapacak olan kimseler, bilgi sistemlerine bağımlılığın getirdiği riskleri, elektronik işlem ve verilerin kaybolma riskini, internet hizmeti sağlayıcılarının riski vb. hususlarını dikkate almak zorundadır. Bununla

birlikte bazı kamu hizmet alanlarındaki denetim sürecinin bir parçası olarak elektronik denetim kanıtları üzerindeki güvenlik riski çok boyutlu bir şekilde değerlendirilmelidir (Şirin, 2006: 32).

E-devlet sistemlerinin kamu yönetiminde güven artırıcı bir faktör olarak işletilebilmesi için gerekli önlemlerin başında güvenli yazılımların geliştirilmesi gerekmektedir. Yazılım ve sistem güvenliği konusunda dünyada ilk önemli çalışmaların başında 1983 yılında Amerika Birleşik Devletleri Savunma Bakanlığı tarafından TCSEC Standartı'nın (Trusted Computer System Evaluation Criteria) yayınlanması gelmiştir. Bununla birlikte 1980'li yıllar boyunca Almanya, Fransa, Hollanda ve İngiltere kendi güvenlik test standartlarını oluşturmaya başlamıştır (Beydağlı vd., 2009: 11). Türkiye'de de bu tür çalışmalar ve standartların yerli dizaynlar ile oluşturulmasına olan ihtiyacın her geçen gün arttığı düşünülmektedir.

E-devlet sistemlerinde güvenlik sorununun önemli bileşenlerinden birisi de şifreleme işlemlerine ilişkindir. Kuşkusuz şifreleme kendi içerisinde kriptoloji, kriptografi, kripto-analiz vb. çeşitli boyutlara sahiptir (Diffie ve Hellman, 1976: 644). Kriptoloji, iki ya da daha fazla tarafın bilgi alışverişini güvenli bir şekilde yapabilmesini sağlayan matematiksel teknikleri de içeren uygulamalar bütünüdür. Kriptografi ise bilginin şifrelenmesi ya da çözümü için kullanılan çeşitli yöntemleri ifade etmektedir. Örneğin kurumlar arası bilgi paylaşımlarının elektronik bir doğrulama sertifikasına bağlı olarak yapılması durumunda kurumlar arası güvenli bilgi aktarımının sağlanarak bilgi paylaşım güvenliliğinin ve gizliliğinin korunması hedeflenmektedir (Efendioğlu ve Sezgin, 2007: 234). Kuşkusuz kriptografi sistemleri tarafından ortaya konulan uygulamaların çok boyutlu analiz edilmesi ise kripto-analiz olarak tanımlanmaktadır. Tüm bunlarla birlikte kriptoloji ile e-devlet uygulamaları arasındaki ortak çalışma konularının başında elektronik imza (e-imza) gelmektedir. Ayrıca bir e-imza sisteminin işletilebilmesinde kriptografik donanımlara, e-imza algoritmalarına ve çeşitli bilgilere ihtiyaç duyulmaktadır (Akleylek, Yıldırım ve Tok, 2011: 715). Bu açıdan e-imza uygulamalarının güvenlik boyutunun çok yönlü bir şekilde ele alınması gerektiği vurgulanmaktadır (Güler ve Ömürgönülşen, 2011: 202-203).

Gelişen teknoloji araçları ve dijitalleşme ile bilgi ve veri güvenliğine ilişkin olası riskler doğru orantılı olarak artmaktadır (Öcal ve Altıntaş, 2018: 2080). Elektronik devlet uygulamalarının yaygınlaşması sürecinde güvenli teknolojik altyapıların sağlanması ve kişisel verilerin gizliliğinin korunması da bir o kadar önemlidir. Bununla birlikte elektronik ortamda yer alan verilerin güvenliği konusunda uluslararası işbirliği de önerilmektedir. Özellikle bilişim suçlarının sınırları aşan bir boyut kazanması devletler arası ortak önlemler almayı gerektirebilmektedir. Örneğin 2000 yılında "Love Letter" isimli virüs dünya genelinde yedi milyar ABD Doları zarara yol açarken 2001 yılında "Code Red Worm" isimli virüs ise ortaya çıktığı andan itibaren ilk on dört saat içerisinde 359.000 elektronik sisteme zarar vermiştir (Özenç, 2007: 183). Bu örnekler göstermiştir ki bilişim güvenliğinin sağlanması için dünya ölçeğinde kararlı bir konsensüs oluşturulmalıdır.

Kamu güvenliği başta olmak üzere çeşitli etkilerle kamu kurumlarında depolanan kişisel veriler, bilgi ve iletişim teknolojilerinde yaşanan gelişmelerle birlikte yeni bir boyut kazanmıştır (Schaar, 2017: 22). Özellikle siber suçların yaygınlaşması ile kişisel verilerin korunmasını ve e-devlet sistemlerinde gerekli güvenlik önlemlerinin alınmasını gerektirmiştir (Babahanoğlu ve Örselli, 2016: 550). Nitekim e-devletin temel özelliklerinden birisi teknik bir devlet anlayışını ifade etmesidir. Bu açıdan bir ülkede e-devletin etkinliğini belirleyen en önemli faktörlerin başında ülkenin telekomünikasyon altyapısı gelmektedir. Bu bağlamda bir ülkede yaygın anlamda dijital ağlar olmadıkça e-devlet sistemlerinin işleyişi başarılı olamamaktadır (Demirel, 2006: 95). Ayrıca e-devlet uygulamalarının en önemli sorun alanlarından birisi olarak sistemi oluşturan teknik unsurların, veri yapılarının ve üretilen bilgi kaynaklarının birbirleri ile uyumlu hale getirilebilmesi gelmektedir (Odabaş ve Polat, 2008: 9).

Birleşmiş Milletler'in 2010 yılında yayınladığı e-devlet gelişim indeksinde e-devlet uygulamalarının bazı özel sektör girişimcileri tarafından kullanmama yönündeki gerekçeler arasında güvenliğe ilişkin kaygılar %32,7 ile üçüncü sırada yerini almıştır (UN, 2010: 114; Metin, 2012: 100). Birleşmiş Milletler'in sonraki pek çok raporunda da e-devlet açısından önemli bir konu olarak güvenlik kaygıları ele alınmaya devam etmiş ve güvenlik kaygıları çeşitlenmiştir. Örneğin 2016 yılında yayınlanan Birleşmiş Milletler E-Devlet Raporu'nda kişisel verilerin korunması ve güvenliği ile siber güvenlik konularına özel bir vurgu yapılmıştır (UN, 2016: 2-3). Kuşkusuz siber güvenlik konusu siber uzay tartışmalarının önemli bir boyutu olarak ele alınmıştır. Bununla birlikte e-devlet üzerinden gerçekleştirilen her türlü iş ve işlemlerin de siber uzay tanımlaması içerisinde olduğu ifade edilmektedir (Yılmaz, 2017: 28).

Kişisel ve kurumsal düzeyde her türlü stratejik bilgileri içeren sistemlerin güvenlik tehditlerine karşı korunması bir zorunluluktur. Bu açıdan güvenlik ihlallerinin en aza indirgenmesi, ülkelerin bilgi güvenliğinin yüksek düzeyde sağlanması ve korunması gerekmektedir. Elektronik ortamda ulusal bilgi güvenliğini olumsuz yönde etkileyen unsurlar yalnızca siber saldırılarla sınırlı olmayıp yangın, sel, deprem, terör, sabotaj vb. olaylar sonrasında da bilgi sistemleri kısmen ya da tamamen zarar görmesi şeklinde ortaya çıkabilmektedir. Kuşkusuz tüm bunlar içerisinde günümüzde en önemli güvenlik konularının başında elektronik ortamlardaki siber saldırılar gelmektedir. Örneğin devletlerarası ilk siber savaş olarak da nitelendirilen Rusya kaynaklı uzun süreli saldırılar sonrası 2007 yılında Estonya'da kamu kurum ve kuruluşlarının internet sayfaları çökertilmiş ve ülkede kamusal hizmetler açısından yaşamın durma noktasına geldiği ifade edilmiştir (Vural ve Sağıroğlu, 2008b: 3; Bıçakcı, 2014: 120-122).

Siber saldırılar sonrası bireylerin ve ülkelerin karşılaştıkları zararların büyüklüğü, siber güvenlik konusunun ülkelerin ve uluslararası kuruluşların önemli gündem maddeleri arasında yer almasına yol açmıştır. Örneğin 1996 yılında başlayan, 1998 yılında ABD tarafından tespit edilen ve siber saldırı tarihine "Moonlight Moze" ismiyle geçen bir saldırılar dizisi gerçekleştirilmiştir. NASA, Enerji Bakanlığı, Pentagon vb. kurumlara yönelik Ruslar tarafından gerçekleştirildiği iddia edilen siber saldırılarda askeri haritalar, askeri tesislere ait bilgiler, araştırma projeleri vb. oldukça önemli veriler çalınmıştır (Raiu vd., 2017). E-devlet sistemleri açısından da oldukça büyük bir tehdit olarak ifade edilebilecek olan siber saldırıların tarafları ve türleri ise genel olarak şu şekilde sıralanabilir (Ünver ve Canbay, 2010: 96; Ünver, Canbay ve Mirzaoğlu, 2011: 8-10; Abolhassan, 2017: 3-7):

- Virüsler, kurtçuk (worm), Truva atı (trojan)
- Zombi ve botnetler
- Sazan avlama (phishing)
- İstenmeyen elektronik postalar (spam)
- Hizmetin engellenmesi saldırıları (DoS, DDoS)
- Klavye izleme yazılımları (key logger)
- Casus/köstebek yazılımlar (spyware)
- Şebeke trafiğinin takip edilmesi (sniffing ve monitoring)

Siber saldırı türlerinin önlenmesine yönelik yasal düzenleme ve ceza tanımlamalarının güncellenerek yaşama geçirilmesi oldukça önemlidir. Bununla birlikte yazılım vb. teknik araçların geliştirilmesi ve ulusal politika ve stratejilerden sorumlu bir kuruluş aracılığıyla siber güvenlik alanında ilgili hizmetleri sunan kurum sistemlerinin korunması gerekmektedir. Bu süreç içerisinde de tüm paydaşlar arasında işbirliği ve koordinasyon kurulabilmelidir. Buna karşın e-devlet hizmetlerine olan güven duygusunun korunabilmesi ve güvenlik açıklarını gideren önlemlerin alınabilmesi kurumsal, mali ve teknik kapasitenin geliştirilmesi ile yakından ilişkilidir. Bu bağlamda

her bir yeni elektronik güvenlik riski karşısında politika yapıcıların çok yönlü çözümler üretebilmeleri bir zorunluluk olarak görülmelidir (Ünver ve Canbay, 2010: 100).

4. Türkiye'de E-Devlet Uygulamaları

Türkiye'de e-devlet uygulamaları ilk olarak kurumsal bilişim sistemi oluşturma çabaları ile ortaya çıkmıştır. Kuşkusuz elektronik hizmetler, niteliği ve genişliği açısından farklı özelliklere sahiptir. Örneğin Merkezi Nüfus Sistemi (MERNİS), kamu kurum ve kuruluşlarında tüm hizmetlerin her vatandaşa ait bir kimlik numarası ile yapılmasını hedefleyen bir projenin yaşama geçirilmesidir (Eroğlu, 2006: 105). Hatta MERNİS, dünyadaki ilk e-devlet projelerinden birisi olarak ifade edilmektedir (Arslan, Kılıç-Akıncı ve Bayhan-Karapınar, 2007: 45). Buna karşın belirli bir hizmet kolunda ya da bir kurumsal yapının özel bir hizmet alanında oluşturulan e-devlet hizmetleri de bulunmaktadır (Odabaş ve Polat, 2008: 8). Bunlar arasında Gümrük Bakanlığı Gümrük Sistemleri Otomasyonu (GİMOP), Maliye Bakanlığı Gelirler Genel Müdürlüğü Bilgisayar Otomasyonu (VEDOP), Adalet Bakanlığı Ulusal Yargı Ağı (UYAP) ve Tapu Kadastro Genel Müdürlüğü Bilgi Sistemi (TAKBİS) sayılabilir. Ayrıca Türkiye'de teknik ve yasal altyapısı oluşturulmuş tek bir portal üzerinden e-devlet faaliyetlerinin sürdürülmesi 18 Aralık 2008 tarihinde hizmete açılan E-Devlet Kapısı uygulaması ile yaşama geçirilmiştir (Keskin, 2011: 1720; Söylemez, 2016: 152-153).

Türkiye'de e-devlet çalışmaları 1997 yılında Ulusal Enformasyon Altyapısı Planı'nın (TUENA) hazırlanması ile ivme kazanmıştır. Bu bağlamda Türkiye'de e-devlet uygulamalarına yönelik ilk önemli projelerin başında Saymanlı Otomasyon Projesi (Say-2000i) gelmektedir. Say 2000i Projesi, tüm kamu çalışanlarının personel ve maaş bilgilerini merkezi bir veri tabanında toplayan ve devletin gelir-gider hesaplarını yapan saymanlıkların otomasyona geçirildiği bir e-devlet projesidir. Ayrıca Say 2000i Projesi, Dünya Bankası (WB) ve Uluslararası Para Fonu (IMF) tarafından da desteklenmiştir (Örselli ve Kahraman, 2016: 180-181). Diğer yandan Türkiye'de 1990'lı yıllardan itibaren birçok kamu kurum ve kuruluşu, bilgi işlem birimleri ile kurumsal internet sayfaları kurmaya başlamıştır. Bununla birlikte Türkiye'de 2003 yılında E-Dönüşüm Türkiye Projesi başlatılarak çeşitli kamu hizmetlerinin elektronik ortamda sunulması hedeflenmiştir. 27 Şubat 2003 tarihinde yayımlanan 2003/12 sayılı Başbakanlık Genelgesi ile E-Dönüşüm Türkiye Projesi'nin amaçları, kurumsal yapısı ve uygulama esasları belirlenmiştir (Çetiner, 2008: 41).

Türkiye'de e-devlet hizmetlerine yönelik hedefler beş yıllık kalkınma planlarında da yer almıştır. İlk olarak VIII. Beş Yıllık Kalkınma Planı'nın hazırlanma aşamasında 2000 yılında Devlet Planlama Teşkilatı'na Bilişim Teknolojileri ve Politikaları Özel İhtisas Komisyonu tarafından Bilgi Hizmetleri ve İçerik Alt Komisyonu Raporu sunulmuştur. İlgili raporda bilgi hizmetleri altyapısına ve elektronik sistemlerin boyutlarına dikkat çekilmiştir. Ancak VIII. Beş Yıllık Kalkınma Planı'nda yalnızca elektronik ticaret uygulamalarına ve hizmetlerine yer verilmiştir (DPT, 2000). Bununla birlikte beş yıllık kalkınma planlarında e-devlet hizmetlerine yönelik hedeflere IX. Kalkınma Planı'nda yer verilmezken doğrudan ilk olarak X. Beş Yıllık Kalkınma Planı'nda yer verilmiştir. X. Beş Yıllık Kalkınma Planı'nda Kamu Hizmetlerinde E-Devlet Uygulamaları başlığı altında tasarlanan, altyapısı oluşturulan ve uygulamaya konulan birçok e-devlet hizmeti vurgulanmıştır. Tüm bu e-devlet hizmetlerinde ise bilgi güvenliği ve kişisel bilgilerin korunmasına yönelik yasal mevzuat ihtiyacına vurgu yapılmıştır (DPT, 2013: 54).

Türkiye'de 23 Ocak 2004 tarihinde yürürlüğe konulan 5070 sayılı Elektronik İmza Kanunu ile elektronik imzanın kullanıcılar tarafından benimsenmesi ve açık ağ sistemine güven duyulması hedeflenmiştir. Bu güvenin kurulabilmesi için taraflar arası iletilen bilgilerin bütünlüğünün ve gizliliğinin korunması ve yasal güvencelerin sağlanması öncelenmiştir. Nitekim 5070 sayılı Kanun'un 4. maddesinde "güvenli elektronik imza" başlığı altında e-imzanın tanımsal özellikleri sıralanmış ve 5. maddesinde ise güvenli e-imzanın uygulama alanı ve hukuksal sorumluluğu anlatılmıştır (Aktaş, 2009: 138-139). Diğer taraftan Türkiye'de kamu kurum ve kuruluşlarının

bilişim sistemlerine artan bağımlılığı e-devlet sistemlerinin güvenli ve güvenilir bir ortamda veriler üretip üretmediğine yönelik denetimlerin yapılması oldukça önem arz etmeye başlamıştır. Nitekim Türkiye'de Sayıştay elektronik denetime yönelik ilk önemli kararı 2003 yılında kabul edilen Hazine Bilişim Sistemleri Denetimi Raporu'dur. Raporun hazırlanmasında Uluslararası Sayıştaylar Birliği (INTOSAI), Bilgi Güvenliği Standartları (ISO), Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) vb. kuruluşların standartlarından yararlanılmıştır. Ayrıca temel denetim hedefinin ilgili devlet kurumlarında kullanılan sistemlerin güvenirliğini ve güvenliğini sağlayan iç kontrollerin incelenmesi olduğu belirtilmiştir (Yıldız, 2007: 182-183).

Türkiye'de e-devlet örneklerini çoğaltmak mümkün olmakla birlikte en başarılı e-devlet uygulamalarından birisi olarak Ulusal Yargı Ağı Bilişim Sistemi (UYAP) gösterilmektedir. Bu sistem, adalet hizmetlerinin elektronik ortamda yürütülmesini hedefleyen bir bilişim projesidir. UYAP üzerinden hangi adalet hizmetlerinin ne şekilde yürütüleceği Hukuk Muhakemesi Kanunu'nda ayrıntılı olarak düzenlenmiştir. Her türlü yargısal iş ve işlemlerin UYAP üzerinde saklanması hedeflenmiştir. Güvenli elektronik imza ile dava açılabilmesi, harç ve avansların ödenmesi ve tüm dava dosyalarının incelenmesi sağlanmıştır (Çam ve Tanrıkulu, 2012: 208). Bununla birlikte UYAP vb. sistemlerin ilgili hizmetlerin özelliği dikkate alındığında güvenlik açısından oldukça korunaklı olması gerekmektedir.

Günümüzde neredeyse herkesin kullandığı ve taşıdığı cep telefonları üzerinden kamu hizmetlerine erişimin sağlanması mobil devlet (m-devlet) terimini de ortaya çıkarmıştır. 2000'li yıllarda hem Türkiye'de hem de Avrupa ülkelerinde çeşitli kamusal hizmetlerde m-devlet uygulanmasına başlanmıştır. Örneğin 2005 yılı itibariyle Avusturya'da vatandaşların cep telefonları yoluyla güvenli bir şekilde e-devlet uygulamalarını kullanabilmeleri ve elektronik imza atabilmeleri sağlanırken, Almanya'da otoyol geçiş ücretlerinin coğrafi yer belirleme sistemi aracılığıyla otomatik olarak cep telefonları ile ödenebilmesi sağlanmıştır. Türkiye'de ise m-devletin ilk örnekleri 2005 yılında Mobil Elektronik Sistem Entegrasyonu Projesi (MOBESE) ve Milli Eğitim Bakanlığı'nın Mobil Bilgi Projesi olmuştur (Yıldız, 2006: 259). Bunlarla birlikte süreç içerisinde Türkiye'de m-devlet uygulamaları tüm kamu kurum ve kuruluşlarına taşınmıştır.

4.1. Türkiye'de E-Devlet Uygulamalarında Güvenlik Sorunları

E-devlet uygulamalarının güvenlik boyutunda öncelikli olarak Türkiye'nin temel kamusal ve kurumsal veri altyapısına yönelik eksiklikleri tamamlaması gerekmektedir. Türkiye'de 2000'li yıllardan itibaren önemi oldukça artmaya başlayan e-devlet projelerinden birisi de 2003 yılında Devlet Planlama Teşkilatı (DPT) Müsteşarlığı bünyesinde kurulan ve Bilgi Toplumu Dairesi Başkanlığı aracılığıyla yürütülen E-Dönüşüm Türkiye Projesi'dir (Çelen, Çelik ve Seferoğlu, 2011: 60). Bu projenin en önemli bileşenlerinden birisini ise Ulusal Konumsal Veri Altyapısı (UKVA) oluşturmaktadır. UKVA çalışmaları, Amerika Birleşik Devletleri'nde resmi olarak 1994 yılında Başkan Clinton'un 12906 sayılı Genelgesi ile başlatılmıştır. Türkiye'de ise 2000'li yıllarda bu altyapıya yönelik yeterli ilerlemeler sağlanamamıştır. UKVA, konumsal veri erişimi ve kullanımı sağlayan ve veri ve servis sağlayıcılarının oluşturduğu bir ağdır. Bu ağ özellikle oto-kontrol mekanizmalarını işler hale getirmesi açısından afet yönetimi ve kriz yönetimi için de oldukça önemlidir. Bu bağlamda UKVA, e-devlet uygulamalarının önemli bir bileşeni olarak değerlendirilmiş ve geliştirilmesine yönelik çeşitli öneriler getirilmiştir (Cömert ve Akıncı, 2005: 3-6).

Türkiye'de 2000'li yıllarda e-devlet uygulamalarında oluşturulan bilişim sistemlerinin önemli bir kısmı teknik altyapı bağlamında güvenlik risklerine açık bir biçimde varlığını sürdürmüştür. Bu risklerde önemli bir unsur olan elektronik veri yapılarından yeterince yararlanılamamış ve kurumsal bilgi kaynaklarının paylaşıma sunulduğu bir bilgi yönetimi modülünden yoksun kalınmıştır (Odabaş ve Polat, 2008: 8). Nitekim Avrupa Birliği üyesi ülkelerdeki e-devlet uygulamalarındaki güvenlik ihlalleri üzerine yapılan bir çalışmada yetkisiz ve izinsiz erişim,

kötü niyetli program kodları ile izinsiz giriş denemeleri %83 oranında yer almıştır (Efendioğlu ve Sezgin, 2007: 222). Bu bağlamda elektronik ortamda sunulan hizmetlerin daha başarılı bir şekilde işleyebilmesi için gerekli altyapı önlemlerinin alınmasının gerektiği düşünülmektedir.

Türkiye'de e-devlet uygulamalarında veri güvenliği ve gizliliğini ilgilendiren önemli bir çalışma yapılmıştır. 2006 yılında Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ile Marmara Araştırma Merkezi (MAM) işbirliği ile hazırlanıp yayınlanan "Kamu Kurumları İnternet Sitesi Kılavuzu" başlıklı bu çalışmada sekiz temel başlık altında otuz konu incelenmiştir. Örneğin "gizlilik ve güvenlik" üst başlığı altında "ziyaretçi bilgilerinin korunması" ile "gizlilik ve güvenlik sözleşmesi" konuları ele alınmıştır (Alır ve Soydal, 2007: 162-163). Bu bağlamda e-devlet hizmetlerini yerine getiren kurumların web tabanlı sayfalarında bulunması gerekli olan standartlar ortaya konulmaya çalışılmıştır. Kuşkusuz e-devlet kurumları günümüzde önemli ilerlemeler kaydetmiş olsa da uzun bir süre web sayfalarında gizlilik ve güvenlik sözleşmesi ya da bir bilgilendirme metnine yer verilmemiş ve vatandaşlar ile ilgili kurumlar arasındaki güven ilişkisi de olumsuz yönde etkilenebilmektedir.

E-devlet uygulamalarına yönelik olumsuz güvenlik algısı esasında internet ağları üzerinden her geçen gün çeşitli yöntemlerle kişisel ve kurumsal veri mahremiyetinin ihlal edilmesinden kaynaklanmaktadır (Warkentin vd., 2002: 158; Aydın, 2012: 529). Bu nedenle e-devlet uygulamalarının yaygınlaşması ile güvenlik sorunlarının artması üst düzeyde veri güvenliği sorununu gündeme getirmektedir. Türkiye açısından vatandaşların kişisel verilerinin önemli bir bölümü Merkezi Nüfus İdare Sistemi (MERNİS), Adrese Dayalı Nüfus Kayıt Sistemi (ADNKS) ve Tapu ve Kadastro Bilgi Sistemi (TAKBİS) üzerinde kayıtlı olarak yer almaktadır. Bununla birlikte dijital ortamlarda kayıtlı ve depolanan verilerin korunmasına yönelik önlemler diğer teknolojik gelişmelerin tehlikesi altında kalmakta ve elektronik veri tabanları çeşitli saldırılarla karşı karşıya kalabilmektedir. Buna karşın e-devlet uygulamaları üzerinde karmaşık teknolojilerin artması ile uzman teknokratlar ve teknik birimler üzerindeki denetim de azalabilmektedir (DDK, 2013: 787-788). Ayrıca bazı teknokratların ya da ilgili birim personelinin kendi değerleri ve anlayışları çerçevesinde kişisel verilerin korunmasını ihlal eden birtakım özellikleri ilgili sisteme uygulayabilmeleri ve niyetlerini saklamaları mümkün görülmektedir (Tataroğlu, 2013: 286). Bu açıdan e-devlet uygulamalarında sadece sistemin teknik boyutunun korunması değil aynı zamanda personel kaynakları, kurum kültürü ve olası diğer etmenlerin de kişisel ve kurumsal verilerin korunmasında dikkate alınması gerekmektedir.

Kişisel verilerin korunmasına yönelik politikalar, e-devlet uygulamaları açısından da oldukça dikkate alınması gerekmektedir. Nitekim kişisel verilerin korunamamasına yönelik her türlü durum vatandaş ile devlet kurumları arasındaki güven ilişkisini de etkilemektedir. Bu noktada özellikle e-devlet uygulamalarında kişisel verilerin korunması sorunu önem arz etmektedir. Yapılan çeşitli araştırmalarda e-devlet hizmetlerini kullanmama gerekçelerinin başında kişisel bilgilerin güvenliğinden kişilerin emin olamaması gelmektedir (Şataf, Çiçek ve Dikmen, 2013: 11). Türkiye açısından kişisel verilerin korunmasına yönelik doğrudan bir yasal düzenleme oldukça uzun bir süre ertelenmiştir (Kutlu ve Kahraman, 2017: 57). Nitekim Türkiye'de 6698 sayılı Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde Resmi Gazete'de yayınlanarak hayata geçirilebilmiştir. Bu kanunda veri mahremiyeti ile elektronik hizmetler arasındaki ilişkiler konusundaki hükümlere ise yer verilmediği görülmektedir.

Vatandaşlar ile devlet arasındaki ilişkilerde kamu düzeni ve güvenliği başta olmak üzere çeşitli gerekçelerle kamu hizmetlerinin muhatabı her bir kimse ile ilgili bilgilerin toplanması, derlenmesi, işlenmesi ve kullanılması yaygın bir uygulama olarak yerini almaktadır. Ancak bu uygulamalar, bilişim ve bilgisayar teknolojilerinin çeşitlenerek gelişimi ile yeni boyutlar kazanmaya başlamıştır. Türkiye açısından kişisel verilerin elektronik ortamda korunması sorunu uzun bir süre kamu kurum ve kuruluşlarının ve özel sektörün kendi çabalarına bağlı kalmış ve güncellenebilir bir

standartlaşma süreci içerisine girilememiştir. Örneğin 2007 yılında bazı kamu kurum ve kuruluşlarına hangi tür kimlik doğrulama ile erişim sağlanıp hangi verilere ulaşıldığı Tablo-3'de gösterilmektedir (Ketizmen ve Ülküderner, 2007: 191-192; Karaarslan, Koç ve Akın, 2010: 3-4):

Tablo-3: Türkiye'de 2007 Yılı İtibariyle Bazı E-Devlet Uygulamalarında Bilgi ve Belge Güvenliğini İhlal Eden Kimlik Doğrulama Örnekleri

İlgili Kurum	Erişim için Gerekli Bilgiler	Edinilen Bilgiler
Sosyal Güvenlik Kurumu	Ad, Soyad, Baba Adı, Doğum Yılı	Sicil No, TC Kimlik No, Anne Adı, Hizmet Dökümü
İçişleri Bakanlığı, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü	Ortak zorunlu alan: İl, İlçe, Ad, Soyad	T.C. Kimlik No, Mahalle / Köy, Baba Adı, Anne Adı, Cilt No, Aile Sıra No, Doğum Yılı, Birey Sıra No, Cinsiyeti
Yüksek Seçim Kurulu	T.C. Kimlik No	Seçmen No, Ad, Soyad, Adres (Kısa), Oy vereceği yer, Sandık no
Sağlık Bakanlığı	T.C. Kimlik No, Ad, Soyad, Baba Adı, Doğum Yılı, Doğum Yeri	Anne Adı, Cinsiyet, Medeni Hali, Cilt No, Birey Sıra No, Aile Sıra No, Mahalle / Köy, Unvan, Branş, Sabit Telefon, Cep Telefonu, E-Posta, Adres, İl, İlçe, Çalışma Durumu, Çalıştığı Kurum, Kurumdaki Unvan ve Şifre.

Özellikle kamu kurumlarının web sitelerinde yapılan sorgulamalar sonucunda birçok kişisel ve kurumsal bilgi ve veri ortaya çıkmaktadır. Veri mahremiyetini ihlal eden bu sorunların önlenebilmesi için etkili bir denetime ihtiyaç bulunmaktadır (Çelen, Çelik ve Seferoğlu, 2011: 68). Kurumların birbirinden farklı sistemlere, veri yapılarına, ara yüzlere, denetim mekanizmalarına ve belge biçimlerine sahip olması e-devlet uygulamalarının başarısını da etkilemektedir. Bununla birlikte kurumlar tarafından geliştirilen e-devlet uygulamalarında ortak bir standart geliştirilemediği gibi veri gizliliği, güvenliği ve kimlik doğrulama sistemleri açısından çok fazla eksiklik bulunmaktadır (Naralan, 2008: 9-10). Bu nedenle elektronik ortamda bilgiye erişimin belirli kurallara bağlanması, bilginin güvenliği ve gizliliği açısından bir zorunluluk olarak ele alınmalıdır. Örneğin ABD'deki e-devlet uygulamalarında vatandaşların fazladan bilgiye erişimleri kısıtlanmıştır (Efendioğlu ve Sezgin, 2007: 230).

Türkiye'de çeşitli e-devlet hizmetlerinde kişisel verilere yönelik güvenlik sorunları örneklerini çoğaltmak mümkündür. 2004 yılında MERNİS'ten 77.756 kişiye aynı vatandaşlık numarasının verilmesi ve 2009 yılında Milli Eğitim Bakanlığı Bilişim Sistemleri (MEBBİS) üzerinden 648.000 öğretmenin kimlik bilgilerinin kopyalanıp internet ortamında sergilenmesi birer güvenlik açığı olarak ortaya çıkmaktadır (Tataroğlu, 2009: 103). Bu noktada yasal eksikliklerin de tamamlanması ve güncellenmesi oldukça önemlidir. ABD'de 1999 yılında çıkartılan Tekbiçim Elektronik İşlem Yasası'nda (Uniform Electronic Transaction Act – UETA) elektronik belge güvenliğine ilişkin çeşitli düzenlemeler yer almıştır (Odabaş, 2008: 8). Türkiye açısından da doğrudan ve müstakil bir elektronik bilgi ve belge güvenliğini koruma altına alacak düzenlemelere olan ihtiyaç devam etmektedir.

27 Ekim 2010 tarihli Milli Güvenlik Kurulu toplantısında siber tehditler ele alınarak kavramın Milli Güvenlik Siyaset Belgesi'ne girmesine karar verilmiştir. 25-28 Ocak 2011 tarihlerinde ise Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumu (TÜBİTAK) ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) işbirliği ile I. Ulusal Siber Güvenlik Tatbikatı yürütülmüştür. Bu tatbikat sonrasında yayınlanan raporda Türkiye'nin siber saldırılara karşı oldukça

güvensiz olduğu ve kamu kurum ve kuruluşlarının gerekli önlemleri almadığı belirtilmiştir. Bununla birlikte 2012 yılında "Redhack" adlı siber saldırı grubunun pek çok e-devlet kurumuna yönelik saldırıları Türkiye'de e-devlet hizmetleri üzerindeki tehdit algısını artırmıştır. Nitekim 20 Ekim 2012 tarihli Bakanlar Kurulu toplantısında "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" onaylanmış ve 28447 sayılı Resmi Gazete'de yayınlanmıştır. İlgili Bakanlar Kurulu Kararı ve 5809 sayılı Elektronik Haberleşme Kanunu çerçevesinde siber güvenlik strateji belgesi ve eylem planının hazırlanmasında yetkili kurum olarak Ulaştırma, Denizcilik ve Haberleşme Bakanlığı belirlenmiştir (Ünver, 2017: 113-114).

Türkiye özelinde e-devlet sistemlerinin güvenliğini yakından ilgilendiren siber güvenlik alanında üst düzey bir koordinasyon kurumunun oluşturulması sürecinde 2012 yılında önemli bir adım atılmıştır. Bakanlar Kurulu tarafından 11.06.2012 tarihli ve 3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonu'na İlişkin Karar, 20.10.2012 tarihli ve 28447 sayılı Resmi Gazete'de yayımlanarak yürürlüğe konulmuştur. Bu karar doğrultusunda Siber Güvenlik Kurulu ihdas edilmiştir. Kurul'un temel görevi ise siber güvenlik ile ilgili alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, yöntem ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak olarak belirlenmiştir. Siber Güvenlik Kurulu ilk toplantısını 21 Aralık 2012 tarihinde Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında gerçekleştirmiştir. Toplantıya Dışişleri, İçişleri ve Milli Savunma Bakanları, Kamu Düzeni ve Güvenliği ile Milli İstihbarat Teşkilatı (MİT) müsteşarları, Genelkurmay Başkanlığı Muharebe Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, TÜBİTAK Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı yetkilileri katılmıştır.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, siber saldırıları önleme ve siber saldırılara müdahale etme konusunda Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı yayınlamıştır. Türkiye'nin bu ilk siber güvenlik strateji belgesi ve planında büyük ölçekteki kamusal ve kritik hizmetlerin internet ortamında sunulmasına dikkat çekilerek siber güvenliğe yönelik çalışmaların yetersiz olduğu ve siber tehditlere karşı yeterli önlemlerin alınması gerektiği belirtilmiştir (Ceyhan, Demiryürek ve Kandemir, 2015: 7). Nitekim Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması" başlıklı 4. eylem maddesi gereğince Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde USOM kurulmuştur. USOM, 2016 yılında TİB'in lağvedilmesinden sonra 2008 yılında kurulmuş olan Bilgi Teknolojileri ve İletişim Kurumu'na bağlanmıştır (Akses, 2016: 9). USOM ise siber güvenlik olaylarına yönelik alarm, uyarı, duyuru faaliyetleri yapmakta ve kritik sektörlere yönelik siber saldırıların önlenmesinde ulusal ve uluslararası koordinasyonu sağlamaktadır (www.btk.gov.tr/, 2015).

2013-2014 Eylem Planı'ndan sonra 2016-2019 dönemini kapsayan yeni eylem planı için bir önceki eylem planından sorumlu ve ilgili kurumlarla 10 Mart - 7 Nisan 2015 tarihleri arasında yedi adet değerlendirme toplantısı yapılmıştır. Toplantıların ardından kamu kurumları, kritik altyapı işletmecileri, bilişim sektörü, üniversiteler ve sivil toplum kuruluşlarını temsil eden 73 kurum ve kuruluştan toplam 126 uzmanın katılımı ile Ortak Akıl Platformu oluşturulmuştur. İki gün süren platform çalışmaları çerçevesinde Türkiye'nin siber güvenlik alanında güçlü ve zayıf yönlerinden hareketle stratejik hedefleri ve gerçekleştirilmesi gereken faaliyetler ortaya konulmaya çalışılmıştır. Bununla birlikte 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanırken ABD başta olmak üzere Avrupa ve Uzak Doğu'dan çok sayıda ülkenin siber güvenlik stratejileri gözden geçirilmiştir. Tüm bu çalışmalar sırasında üretilen bilgilerin toplanması, incelenmesi ve değerlendirilmesi ile "2016-2019 Ulusal Siber Güvenlik Stratejisi" ve "2016-2019 Ulusal Siber Güvenlik Eylem Planı" hazırlanmıştır (UDHB, 2016a: 6).

Türkiye'de 2016-2019 yılları arasında uygulanmak üzere hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çerçevesinde mevcut güvenlik risklerini asgari düzeye indirmeyi hedefleyen stratejiler şu şekilde sıralanmıştır (UDHB, 2016a: 13-14):

- Ulusal kritik altyapı envanterinin oluşturulması ve bu altyapıların bağlı oldukları düzenleyici kurumlar tarafından denetlenmesi,
- Tüm kamu kurumlarının kendi bilgi güvenliği yönetim sürecini çalıştırabilecek yetkinliğe ulaşması,
- Siber güvenlik konusunda kurum yöneticilerinin farkındalığının artırılması,
- Siber güvenlik alanında uzmanlaşmak isteyen araştırmacıların ve öğrencilerin teşvik edilmesi,
- Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesinin oluşturulması,
- Güvenli yazılım geliştirme ve tedarik yönetimi kültürünün oluşturulması,
- Siber güvenlikte dışa bağımlılığı azaltmak üzere araştırma ve geliştirme faaliyetlerine önem verilerek yerli ürünlerin geliştirilmesi,
- Tehdit unsurlarının saldırılarını önleyebilmek için ulusal proaktif siber savunma yeteneğinin geliştirilmesi,
- Tehdit unsurlarının siber uzaydaki en büyük avantajı olan anonimliğini ortadan kaldırmak üzere etkin kayıt yönetimi ve IPv6 (İnternet Protokolü Sürüm 6) teknolojilerinin yaygınlaştırılması,
- Kurumsal ve sektörel SOME'lerin etkinliğinin artırılması için yasal ve mali düzenlemelerin yapılması, bilişim altyapısının sağlanması, nitelikli personel ihtiyacının karşılanması ve ulusal siber olaylara müdahale kapsamında bilgi paylaşımının geliştirilmesi.

Bu strateji belgesinde kritik kamu hizmetleri ve su yönetimi alanlarındaki sektörel SOME'ler arasında İçişleri Bakanlığı, Adalet Bakanlığı, Maliye Bakanlığı, Sağlık Bakanlığı, Çevre ve Şehircilik Bakanlığı, Çalışma ve Sosyal Güvenlik Bakanlığı, Gıda, Tarım ve Hayvancılık Bakanlığı ile Orman ve Su İşleri Bakanlığı olmak üzere toplam sekiz bakanlık sıralanmıştır. Bununla birlikte yukarıda sıralanan stratejiler içerisinde özellikle kamu kurum ve kuruluşlarındaki e-devlet uygulamalarına yönelik her türlü riske karşı yerli kaynaklarla güvenli yazılım tekniklerinin ve yöntemlerinin geliştirilmesi oldukça önemlidir. Ayrıca risk yönetimi sürecinde ilgili tüm paydaşları denetleyebilecek ve koordinatör rol üstlenebilecek merkezi bir otoritenin Türkiye'de kurulması 2016-2019 dönemi Strateji Belgesi'nin temel vurguları arasında yerini almıştır.

Devletler siber istihbarat faaliyetlerine kuşkusuz artan oranda mali bütçe ayırmaya başlamıştır. Nitekim siber saldırı türleri üzerinden hedef e-devlet altyapılarının ve web sitelerinin çökertilmesi ya da hacklenmesi durumları ile her geçen gün karşı karşıya gelmek mümkündür. Bununla birlikte Türkiye'de ulusal düzeyde bir bilgi güvenliği teşkilatının kurulması için çeşitli fikirler, raporlar ve kanun tasarıları hazırlanmaktadır. Bu süreçte çeşitli sivil toplum kuruluşları da öneriler geliştirmektedir. Örneğin Türkiye'de 1971 yılında kurulan ve bilişim teknolojisi alanında ilk sivil toplum kuruluşlarından birisi olan Türkiye Bilişim Derneği tarafından Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı hazırlamıştır. Bu tasarı önerisinde e-devlet hizmetlerinin güvenliğine ilişkin ayrıntılı düzenleme taleplerine yer verilmiştir (www.tbd.org.tr/, 2018).

Türkiye'de e-devlet hizmetlerine ilişkin ulusal düzeyde ilk defa e-devlet hizmetlerine yönelik doğrudan bir strateji belgesi ve eylem planı hazırlanmıştır. 2016-2019 Ulusal E-Devlet

Stratejisi ve Eylem Planı başlığı altında ilk defa milli kaynaklar kullanılarak hazırlandığı ifade edilen belgede çeşitli stratejik hedefler ve eylem planları yer almıştır. 9 Eylül 2016 tarihinde Ankara'da 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ile birlikte bir tanıtım toplantısı ile kamuoyuna duyurulmuştur. 2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı'nda e-devlet hizmetlerinin teknik ve yönetsel altyapısına yönelik stratejik amaçlar arasında siber güvenlik temel vurguların arasında yerini almıştır. Böylece e-devlet hizmetleri ve uygulamalarında güvenlik boyutu önemli ölçüde siber güvenlik riskleri ile yakından ilişkili olarak ele alınmıştır. Bu nedenle elektronik düzeyde yürütülen devlet hizmetlerinde güvenlik sorunu siber güvenlik kavramı ile birlikte değerlendirilmeye başlamıştır. Nitekim eğitim, sağlık, kamu mali yönetimi, sosyal hizmetler, çalışma ve sosyal güvenlik, ulaşım ve iletişim, tarım ve hayvancılık başta olmak üzere çeşitli kamu hizmetlerinde e-devlet eylem planları siber güvenlik ile birlikte ele alınmıştır (UDHB, 2016b: 91-107). Ayrıca E-Devlet Strateji Belgesi'nde siber güvenlik kanununun çıkartılması da hedeflenmiştir.

2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı'nda ulusal düzeyde e-devlet politikaları belirlenirken Türkiye'nin kendine özgü şartları, küresel gelişmeler, teknolojik yenilikler ve eğilimler ile siber güvenlik dikkate alınarak kamu hizmetlerinde e-devlet uygulamalarının geliştirilmesi temel öncelikleri arasında yerini almıştır. Bununla birlikte Türkiye'de e-devlet projelerinde en önemli konu başlıklarında birisi olarak bilgi güvenliği riski yer almıştır. Bu bağlamda e-devlet projelerinde siber saldırılar gibi sistem güvenliği risklerinin giderilebilmesi için ilgili e-devlet kurumlarının yetkinliklerinin artırılması ve ortak altyapılarda yeni yazılımların geliştirilebilmesi hedeflenmiştir.

E-devlet uygulamalarında yer alan her türlü bilgi, belge, doküman ve arşivin korunması, bilgi teknoloji aracılığıyla yapılan her türlü riskin yönetilmesi açısından ayrı bir önem kazanmaktadır. Nitekim Türkiye'de kamu kurum ve kuruluşlarında elektronik belge yönetimi, 2000'li yıllardan itibaren önem verilen konular arasında yerini almaya başlamıştır. Bu bağlamda e-devlet projelerinin temel yapı taşları arasında yer alan e-belge yönetim sistemlerinin gelişen ve değişen teknolojik şartlarla eşzamanlı olarak reform ve revize edilmesi gerekmektedir. Buna karşın geleneksel kamu yönetimi sorunlarının bu tür güncel sorunlarla mücadeleyi etkilemeye devam ettiği görülmektedir.

Kişi mahremiyetinin üçüncü kişiler tarafından ihlalinde önemli bir sorun alanı vatandaş-devlet ilişkilerinde ortaya çıkmaktadır (Tataroğlu, 2009: 95). Bu süreçte e-devletin ayrı bir önemi bulunmaktadır. E-devlet sürecinde kişisel verilerin ağlarla birbirine bağlı çok büyük sistemler üzerinde saklanması ve paylaşılması çeşitli güvenlik önlemleri alınsa dahi teknolojinin doğası ile uyum sorunu yaşayabilmektedir. Bütün bunlarla birlikte altyapı çalışmalarına yeterince yatırım yapılmaması ve mevcut verilerin olası riskler karşısında ikinci ve üçüncü alternatif yollar üzerinden önceden çalışılmaması ayrı bir güvenlik sorunu olarak ortaya çıkabilmektedir. Nitekim Türkiye'de Şubat 2018 tarihinde uygulamaya konulan E-Devlet Kapısı'nda Alt-Üst Soy Bilgisi Sorgulama başlığı altında 18. yüzyılın ikinci yarısına kadar geriye götürülebilen verilerin paylaşıma açılması ile vatandaşlar kısa bir zaman dilimi içerisinde sisteme yoğunlaşmışlardır. Bunun üzerine E-Devlet Kapısı'na erişim sorunu yaşanmış ve ilgili hizmetin bir süre sistemden kaldırılması söz konusu olmuştur. Üstelik aynı ay içerisinde bu sefer Milli Savunma Bakanlığı'nın "Şehit Listesi" ve "Personel Sefer Görev Emri Sorgulama" başlıklı iki e-devlet hizmeti erişim yoğunluğu nedeniyle sistemsel sorunlara yol açmıştır.

Birleşmiş Milletler 2016 yılında yayınladığı E-Devlet Gelişmişlik Endeksi'nde 189 ülke arasında sırasıyla Birleşik Krallık, Avustralya ve Güney Kore ilk üç içerisinde yerlerini almışlardır. Örneğin Güney Kore'nin e-devlet uygulamaları açısından öncü ülkeler arasında yer almasının temel nedeni olarak güvenlik öncelikli teknolojik ve bilişsel altyapının bir devlet politikası olarak kabul görmesi olduğu belirtilmektedir (Sadioğlu ve Erdinçler, 2017: 3). Türkiye ise aynı Endeks'te yüksek seviyede derecelendirilmiş ancak 68. sırada yerini alabilmiştir. Bununla birlikte E-Katılımcılık Endeksi'nde ise 60. sırada yer bulmuştur (UN, 2016). Bu açıdan Türkiye'nin uluslararası endekslerde daha iyi sıralarda yer alması için e-devlet hizmetlerinin güvenlik altyapısını ve yasal güvencelerini

geliştirmesi gereklidir. Bu bağlamda Türkiye'de güncellenen teknik altyapıya ve yerel teknolojik araçların geliştirilmesine ayrı bir ihtiyaç bulunmaktadır.

Türkiye'de özellikle siber güvenlik konusu uzun yıllar uzmanlar tarafından dile getirilmesine karşın gerekli ilgiyi yeni yeni görmeye başlamıştır. Türkiye'de kamu kurum ve kuruluşları tarafından geliştirilen e-devlet sistemlerinin güvenliğinin sağlanması, uluslararası bilgi güvenliği standartlarına uygun hale getirilmesi ve denetime dayalı sürdürülebilir bir güvenlik yapısının oluşturulması gerekmektedir. Bilgi güvenliği ve kişisel verilerin korunmasına yönelik çalışmalar geliştirilmeli ve özellikle siber güvenlik alanında kurumsal sorumluluklar yeniden düzenlenmelidir (Temür, 2012: 524-525; Güngör, 2015: 52-55). Ayrıca devlet kurumlarında siber güvenlik alanında görevli teknokrat ve teknik personelin eğitilmesi de oldukça önemlidir (Keleştemur, 2017: 6).

Genel Değerlendirme ve Öneriler

Kamu kurum ve kuruluşlarında e-devlet uygulamalarının istenilen düzeylere ulaşamamasında kurumsal yapı, yöneticiler ve geleneksel çalışma şekline uyum sağlamış bazı personelin direnci yadsınamaz bir gerçek olarak ortaya çıkmaktadır. Bununla birlikte kamu bürokrasisinde e-devlet uygulamaları veri mahremiyetine ilişkin önemli riskleri de içerisinde barındırmaktadır. Bu açıdan e-devlet uygulamalarının en önemli boyutlarının başında güvenlik gelmektedir. Nitekim pek çok ülkede daha az risk içeren kamu hizmet alanlarında e-devlet uygulamalarının yaşama geçirilmesi kolay olmaktadır. Buna karşın e-devlet uygulamalarının teknik ve fiziksel altyapı olanakları ciddi bir incelemeye tabi tutulmalıdır. Özellikle ilgili e-devlet uygulamasının yazılımı ya da birtakım teknolojik açıkları, bazı hizmet alanları açısından önemli güvenlik sorunlarına kapı aralamaktadır. Bu güvenlik sorunları ise vatandaşlar ile devlet kurumları arasındaki güven sorununu da derinleştirmektedir.

E-devlet uygulamaları ile etkin ve güvenilir hizmet sunumunun gerçekleşebilmesi için bilgi ve belge yönetiminin kurumsallaşması gerekmektedir. Daha açık bir ifadeyle yasalara uygun, teknoloji ile uyumlu, uzman personele sahip ve reforma açık bir yönetsel ve kurumsal anlayış, e-devlet uygulamalarının başarısı için oldukça önemlidir. Bu açıdan geleneksel yönetim sorunlarını da azaltması beklenen e-devlet uygulamalarının vatandaşlar, özel sektör vb. kesimler ile olan güven ilişkisinin de sürdürülebilir olması gerekmektedir.

Türkiye'de 2000'li yıllar boyunca e-devlet uygulamalarındaki bilişim sistemlerinde ve teknik altyapısında önemli güvenlik riskleri oluşmuştur. Bu risklerin yönetilebilmesi için e-devlet hizmetlerinde risk analizlerinin sürekli olarak yapılması ve ilgili denetimlerin artırılması gerekmiştir. Bununla birlikte MERNİS ve MEBBİS örneklerindeki güvenlik sorunları dikkate alındığında Türkiye'de elektronik bilgi ve belge güvenliğini koruma altına alacak teknik, mali ve beşeri kaynaklar ile yasal düzenlemelere olan ihtiyaç teknolojinin çeşitlenen boyutları ile birlikte sürekli olarak artmaya devam etmektedir. Bu açıdan yeni teknolojik süreçlerin takip edilmesi, güncellenen tehditlere karşı proaktif önlemlerin alınması, yeni yerli ve milli nitelikli yazılım araçlarının geliştirilmesi, elektronik ortamlardaki her türlü risk unsuruna karşı kapsamlı bir mevzuatın oluşturulması ve güçlü bir kurumsal ağın kurulması gerekmektedir.

ABD, Estonya, Güney Kore vb. ülkelerde e-devlet hizmetlerinin ve uygulamalarının bilişim teknolojilerinin gelişimi ile eşzamanlı olarak yaşama geçirildiği görülmüştür. Buna karşın 2007 yılında Estonya'da siber saldırılar sonrasında tüm e-devlet hizmetlerinin aksaması tecrübe edilse de Türkiye'de devlet düzeyinde siber tehdit algısı ilk olarak 27 Ekim 2010 tarihli Milli Güvenlik Kurulu toplantısında gündeme alınabilmiştir. Kuşkusuz Türkiye bu tür adımlar konusunda biraz gecikme yaşamış olsa da son yıllarda teknoloji ve yasal alanlarda önemli ilerlemeler kaydetmiştir.

Türkiye'de e-devlet hizmetlerinde veri güvenliği ve gizliliğine yönelik ilk önemli çalışma 2006 yılında TÜBİTAK ve MAM işbirliği ile hazırlanabilmiştir. Bu çalışmada özellikle kamu kurum ve kuruluşlarının internet sitelerindeki gizlilik ve güvenlik sorunlarının tüm boyutları ele alınmaya

çalışılmıştır. İkinci önemli adım ise Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından hazırlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 yıllarını kapsayan Eylem Planı ile atılmıştır. Türkiye'de bu tür süreçler hükümetler tarafından birincil politikalar arasında değerlendirilmeli ve politika yapıcılar daha fazla önlemlerin geliştirilmesi konusunda her türlü aktörü sürece dahil ederek ve altyapı kaynaklarına yatırım yaparak e-devlet hizmetlerindeki güvenlik sorunlarının asgari düzeylere çekilebilmesine olanak sağlamalıdır. Bu bağlamda e-devlet sistemlerini ve hizmetlerini hedef alan siber saldırıların asimetrik karakteri çeşitli risk tehditleri ile mücadeleyi zorlaştırabilmektedir. Bu açıdan siber güvenlik risklerinin yönetilebilir düzeylere çekilmesi öncelikli hedefler arasında yerini almalıdır.

Türkiye bazı kritik düzeydeki e-devlet sistemlerine yönelik siber güvenlik alanında uluslararası rekabet gücüne sahip bir sistem kurabilmelidir. Bu bağlamda Türkiye'de e-devlet sistemlerinin güvenliğine ilişkin ulusal düzeyde ve kurumlar üstü bir proaktif siber savunma kurumunun oluşturulması gerekmektedir. Nitekim 2016-2019 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda e-devlet uygulamalarındaki her türlü iş, hizmet ve verinin sunumunda sistem güvenliğinin ve gizliliğinin sağlanması, siber güvenlik olaylarının etkilerinin en düşük düzeyde tutulması ve kritik teknolojilerin Türkiye'de üretilmesi ve dışarıdan alınan teknolojilerin de güvenle kullanılabilmesi temel hedefleri arasında yerini almıştır. Bu açıdan Türkiye'de ulusal düzeyde siber güvenlik sağlanmasında risk yönetimi etkin ve devamlı bir niteliğe sahip olmalı, muhtemel risklerin asgari düzeylerde tutulması için proaktif planlar hazırlanmalı, yerli teknolojik araçların üretimi konusunda araştırma ve geliştirme projelerine beşeri, mali, teknik ve yasal destek sağlanmalıdır.

2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı'nda elektronik düzeyde yürütülen devlet hizmetlerinde güvenlik sorunu siber güvenlik kavramı ile birlikte değerlendirilmiş ve müstakil bir siber güvenlik kanununun çıkartılması hedeflenmiştir. Aynı dönemde hazırlanan 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın temel hedefleri arasında ise bilgi teknolojileri üzerinden sağlanan her türlü iş, hizmet ve verinin sunumunda sistem güvenliğinin ve gizliliğinin sağlanması ve siber güvenlik olaylarının etkilerinin en düşük düzeyde tutulması yer almıştır. Bu bağlamda Türkiye'de e-devlet güvenliği ve siber güvenlik alanında ulusal düzeyde etkin bir risk yönetimine ihtiyaç bulunmaktadır.

Türkiye'de hükümetlerin ve karar alıcıların e-devlet uygulamalarında yüksek düzeyli koruma sağlayabilmesi için teknolojik gelişmeleri yakından takip edebilecek bir kurumsallaşmaya ve mali ve beşeri kaynaklara olan ihtiyacı her geçen gün artmaktadır. Kuşkusuz bu ihtiyaç, e-devlet güvenliğini tehdit eden risklerin çeşitlenmesi ile oldukça yakından ilişkilidir. Küresel düzeyde bilişim sistemleri alanında öncü olarak ifade edilen ülkelerde dahi e-devlet sistemlerini çökertebilecek çeşitli örneklerin tecrübe edilmiş olması Türkiye'nin bu alandaki sorumluluklarını daha ciddi bir şekilde ele almasını zorunlu kılmaktadır. Ayrıca kritik önemi haiz teknolojilerin Türkiye'de üretilmesi ya da dışarıdan alınan teknolojilerin güvenle kullanılabilmesini sağlayacak önlemlerin alınması ve geliştirilmesi gerekmektedir.

Türkiye'de e-devlet sistemleri tasarlanırken çeşitli güvenlik modeli önerilerinden yararlanılmalı ve ilgili teknolojinin çok boyutlu olarak düşünülmesi gerekmektedir. Bununla birlikte Türkiye'deki e-devlet hizmetlerinde güvenlik açıklarından ya da teknik sorunlardan kaynaklı durumlarda bir risk yönetimine ihtiyaç bulunmaktadır. Buna karşın bazı e-devlet sistemlerine vatandaşların hizmet talepleri üzerine erişim yoğunluğunun yaşanması ile ilgili e-devlet hizmetlerinde aksaklıklar ve gecikmeler yaşanmış ve yaşanmaya devam edebilmektedir. Bu sorunlarla mücadelede güvenlik risklerinin yönetiminin önemi daha fazla dikkate alınmalıdır. Ayrıca e-devlet hizmetlerinde güvenlik riskleri analiz edilirken elektronik ortamlarda kamu yönetimlerinin sorumluluk alanlarına giren denetim işlevleri de göz ardı edilmemelidir.

KAYNAKÇA

Abolhassan, F. (2017). Security: The real challenge for digitalization. *Cyber Security*. Ed. Ferri Abolhassan, Cham: Springer, 1-11.

Akleylek, S.; Yıldırım, H. M. ve Tok, Z. (2011). Kriptoloji ve uygulama alanları: Açık anahtar altyapısı ve kayıtlı elektronik posta. *XIII. Akademik Bilişim Konferansı Bildiriler Kitabı*. Ed. M. Akgül, vd., 2-4 Şubat 2011, Malatya, 713-718.

Akses, A. (2016). Bilgi güvenliği ve Türkiye. *Herkese Bilim Teknoloji*, (28), 9-9.

Aktaş, K. (2009). Türkiye Büyük Millet Meclisi dilekçe komisyonu örneğinde elektronik devlet uygulamaları. *Yasama Dergisi*, (11), 130-156.

Alır, G. ve Soydal, İ. (2007). Türkiye'de e-devlet uygulamaları kapsamında kamu kurumlarına ait web sayfalarının değerlendirilmesi. Ed. Kurbanoğlu, S., vd., *Değişen Dünyada Bilgi Yönetimi Sempozyumu Bildiriler Kitabı*. 24-26 Ekim 2017, Ankara, 158-166.

Arslan, M.; Kılıç-Akıncı, S. ve Bayhan-Karapınar, P. (2007). E-iş, e-devlet, etik. Ankara: Siyasal Kitabevi.

Aydın, M. D. (2012). Veri güvenliği, mahremiyet, gözetim uygulamaları ve e-devlet. Ed. M. Z. Sobacı ve M. Yıldız, *E-devlet: Kamu yönetimi ve teknoloji ilişkisinde güncel gelişmeler*. Ankara: Nobel Akademik Yayıncılık, 529-547.

Babahanoğlu, V. ve Örselli, E. (2016). Türk kamu yönetiminde kişisel verilerin korunması ve güvenliğine ilişkin kurumsal yapılanma: Kişisel verilerin korunması kurumu. *ASOS Kongre Bildiri Kitabı*. Elazığ, 550-556.

Bahtiyar, Z. (2003). *Virüsler ve Güvenlik*. İstanbul: Pusula Yayınları.

Baştan, S. ve Gökbunar, R. (2004). Kamu hizmetlerinin sunumunda e-devletle ilgili yeni gelişmeler: Tümleşik e-devlet sistemlerine Doğru. *D.E.Ü. İ.İ.B.F. Dergisi,* 19 (1), 71-89.

Belanger, F. and Hiller, J. S. (2006). A framework for e-government: Privacy implications. *Business Process Management Journal*, 12 (1), 48-60.

Beydağlı, E., Kara, M., Bahşi, H. ve Alparslan, E. (2009). Güvenli yazılım geliştirme modelleri ve ortak kriterler standardı. *4. Ulusal Yazılım Mühendisliği Sempozyumu Bildiriler Kitabı*. İstanbul, 11-17.

Bıçakcı, S. (2014). NATO'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. *Uluslararası İlişkiler,* 10 (40), 101-130.

Carter, L. and Belanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal*, 15 (1), 5-25.

Carter, L. and Weerakkody, V. (2008). E-government adoption: A cultural comparison. *Information Systems Frontiers*, 10 (4), 473-482.

Ceyhan, E. B., Demiryürek, E. ve Kandemir, B. (2015). Sosyal ağlarda güncel güvenlik riskleri ve korunma yöntemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* 1 (1), 1-10.

Cömert, Ç. ve Akıncı, H. (2005). Ulusal konumsal veri altyapısı ve e-Türkiye için önemi. *10. Türkiye Harita Bilimsel ve Teknik Kurultayı*. 28 Mart-1 Nisan 2005, Ankara: TMMOB, 1-9.

Çam, A. R. ve Tanrıkulu, C. (2012). Yargı ve e-devlet: UYAP örneği. Ed. M. Z. Sobacı ve M. Yıldız, *E-devlet: Kamu yönetimi ve teknoloji ilişkisinde güncel gelişmeler*. Ankara: Nobel Akademik Yayıncılık, 205-231.

Çelen, F. K., Çelik, A. ve Seferoğlu, S. S. (2013). Türkiye'deki e-devlet uygulamalarının değerlendirilmesi. XIII. Akademik Bilişim Konferansı Bildiriler Kitabı. Ed. M. Akgül, vd., 2-4 Şubat 2011, Malatya, 63-71.

Çetiner, Y. T. (2008). E-dönüşümde Türkiye nerede?.*Uluslararası Ekonomik Sorunlar Dergisi*, (31), 40-48.

Delibaş, K. ve Akgül, A. E. (2010). Dünyada ve Türkiye'de e-devlet uygulamaları: Türkiye'de e-demokrasi ve e-katılım potansiyellerinin harekete geçirilmesi. *Sosyoloji Araştırmaları Dergisi,* 13 (1), 101-144.

Demchenko, Y., vd. (2005). Web services and grid security vulnerabilities and threats analysis and model. *6th IEEE/ACM International Workshop on Grid Computing*. Proceedings Book, 13-14 Nowember 2005, Washington, DC., 262-267.

Demirel, D. (2006). E-devlet ve dünya örnekleri. *Sayıştay Dergisi*, (61), 83-118.

Demirel, D. (2010). Yönetişimde yeni bir boyut: e-yönetişim. *Türk İdare Dergisi*, (466), 65-94.

Devlet Denetleme Kurumu (DDK). (2013). *Kişisel verilerin korunmasına ilişkin ulusal ve uluslararası durum değerlendirmesi ile bilgi güvenliği ve kişisel verilerin korunması kapsamında gerçekleştirilen denetim çalışmaları raporu*. https://www.tccb.gov.tr/assets/dosya/ddk56.pdf, 12.11.2017.

Diffie, W. ve Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22 (6), 644-654.

Doğan, K. C. (2015). Yeni kamu yönetimi ve etik anlayışının Türk kamu yönetiminde kurumsallaşması: kamu görevlileri etik kurulu örneği. *Turkish Studies*, 10 (10), 381-402.

DPT (Devlet Planlama Teşkilatı). (2000). *Sekizinci beş yıllık kalkınma planı (2001-2005)*. http://www.kalkinma.gov.tr/Lists/Kalknma%20Planlar/Attachments/2/plan8.pdf, 19.02.2018.

DPT (Kalkınma Bakanlığı). (2013). *Onuncu beş yıllık kalkınma planı (2014-2018)*.http://www.kalkinma.gov.tr/Lists/Kalknma%20Planlar/Attachments/12/Onuncu%20Kalk%C4%B1nma%20Plan%C4%B1.pdf, 19.02.2018.

Durna, U. ve Özel, M. (2008). Bilgi çağında bir yönetsel dönüşüm yaklaşımı: e-(yerel) yönetim. *Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 5 (10), 1-32.

Efendioğlu, A. ve Sezgin, E. (2007). E-devlet uygulamalarında bilgi ve paylaşım güvenliği. *Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi,* 16 (2), 219-236.

Eroğlu, H. T. (2006). E-devlet uygulamaları çerçevesinde MERNİS projesi ve beklentiler. *Sayıştay Dergisi*, (62), 83-106.

Ghernaouti, S. (2013). *Cyber power: Crime, conflict and security in cyberspace*. Lausanne: EPFL Press.

Gordeychik, S., Grossman, J. ve Khera, M. (2010). *Web application security statistics 2008*. http://www.webappsec.org/projects/statistics/, 09.02.2018.

Güler, M. ve Ömürgönülşen, U. (2011). Türkiye'de e-imza alanındaki hukuki düzenlemeler ve bazı kamu kurumlarındaki e-imza uygulamaları. *Sosyoekonomi*, (1), 197-230.

Güngör, M. (2015). *Ulusal bilgi güvenliği: Strateji ve kurumsal yapılanma*. Ankara: Kalkınma Bakanlığı Yayınları.

İnalöz, A., Ünver, M. ve Alkan, M. (2008). E-devlet güvenliği. *3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*. 25-27 Aralık 2008, Ankara, 9-13.

Karaarslan, E., Koç, S. ve Akın, G. (2010). Vatandaşlık numarası bazlı e-devlet sistemlerinde kişisel veri mahremiyeti durum saptaması. *İzmir Bilişim Hukuku Kurultayı*. 9-11 Haziran 2010, 1-8.

Karkın, N. ve Özgür, H. (2012). Türkiye'nin Yönetsel Düzeninde E-Devletten E-Yönetişime Geçiş. *E-Devlet: Kamu Yönetimi ve Teknoloji İlişkisinde Güncel Gelişmeler*. Ed. Mehmet Zahid Sobacı ve Mete Yıldız, Ankara: Nobel Akademik Yayıncılık, 85-102.

Kaşıkçı, D. N., vd. (2014). Türkiye ve Avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim ve Bilim,* 39 (171), 230-243.

Keleştemur, A. (2017). Türkiye siber güvenlik alanında yükseliyor. *Siber Güvenlik*, (1), 6-6.

Keskin, İ. (2011). E-devlet uygulamalarının kamu yönetiminde şeffaflaşmaya etkisi. *9. Bilgi, Ekonomi ve Yönetim Kongresi Bildirileri*. 23-25 Haziran 2011, Saraybosna, 1715-1728.

Ketizmen, M. ve Ülküderner, Ç. (2007). E-devlet uygulamalarında kişisel verilerin korun(ma)ması. *XII. Türkiye İnternet Konferansı, Bildiriler Kitabı*. 8-10 Kasım 2007, Ankara, 189-193.

Kıvanç, E., vd. (2006). E-devlet dönüşümünde kritik faktörler ve işletmecilik açısından değerlendirmeler. *XI. "Türkiye'de İnternet" Konferansı Bildirileri*. 21-23 Aralık 2006, Ankara, 103-112.

Kraemer, K. ve King, J. L. (2006). Information technology and administrative reform: Will e-government be different?.*International Journal of Electronic Government Research (IJEGR),* 2 (1), 1-20.

Kutlu, Ö. ve Kahraman, S. (2017). Türkiye'de kişisel verilerin korunması politikasının analizi. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi,* 5 (4), 45-62.

Lambrinoudakis, C., vd. (2003). Security requirements for e-government services: methodological approach for developing a common PKI-based security policy. *Computer Communications,* 26 (16), 1873-1883.

Landau, R. I. ve Krueger, J. E. (1998). *Corporate trust administration and management*. New York: Columbia University Press.

Ma, L., Chung, J. and Thorson, S. (2005). E-government in China: Bringing economic development through administrative reform. *Government Information Quarterly,* 22 (1), 20-37.

Metin, A. (2012). Türkiye'de e-devlet uygulaması ve e-devletin bürokrasiye etkisi. Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, (7), 97-108.

Milani, M. M. R. A.; Pehlivan, H. ve Pour, S. H. (2013). Kaos tabanlı bir şifreleme yöntemi ve analizi. *XIII. Akademik Bilişim Konferansı Bildiriler Kitabı*. Ed. M. Akgül, vd., 2-4 Şubat 2011, Malatya, 519-525.

Naralan, A. (2008). Türkiye'de e-devlet güçlükleri, *EKEV Akademi Dergisi*, (37), 1-20.

Odabaş, H. (2008). Elektronik belge düzenleme yaklaşımları ve Türkiye'de e-devlet uygulamalarında elektronik belge yönetimi. *Atatürk Üniversitesi SBE Dergisi,* 12 (2), 121-142.

Odabaş, H. ve Polat, C. (2008). E-devlet bilişim sistemlerinde kurumsal bilgi ve belge yönetimi. *Balkan Ülkeleri Kütüphaneler Arası Bilgi-Belge Yönetimi ve İşbirliği Sempozyumu, Bildiriler Kitabı*. Ed.: E. Bilar ve Y. Ekinci, Edirne: Trakya Üniversitesi Yayınları, 236-246.

Odabaş, H. (2009). Bilgi kaynaklarının işletiminde elektronik doküman yönetimi ve elektronik belge yönetimi sistemlerinin rolü. *XI. Akademik Bilişim Konferansı Bildiriler Kitabı*. 11-13 Şubat 2009, Şanlıurfa, 411-421.

Öcal, F. M. ve Altıntaş, K. (2018). Dördüncü sanayi devriminin emek piyasaları üzerindeki olası etkilerinin incelenmesi ve çözüm önerileri. *Uluslararası Toplum Araştırmaları Dergisi*, 8 (15), ss. 2066-2092.

Örselli, E. ve Kahraman, S. (2016). E-devlet projeleri bağlamında say-2000i projesi. Ed. A. Şahin ve E. Örselli, *Teoriden uygulamaya e-devlet*. 2. Baskı, Konya: Atlas Akademi, 175-192.

Örselli, E. ve Taşpınar, Y. (2016). E-devlet: fırsatlar ve tehditler bağlamında bir analiz. Ed. A. Şahin ve E. Örselli, *Teoriden uygulamaya e-devlet*. 2. Baskı, Konya: Atlas Akademi, 1-34.

Örselli, E., Sevinç, İ., Karabulut, N. ve Dinçer, S. (2018). Web 2.0 Uygulamalarının Seçim Çalışmalarındaki Yeri: Anayasa Referandumu ve Twitter Kullanımı. *Uluslararası Sosyal Araştırmalar Dergisi*, 11 (57), 696-713.

Özenç, K. (2007). Bilgi ve iletişim teknolojilerinde kişisel ve kurumsal bilgi güvenliğinin sağlanması. *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*. 13-14 Aralık 2007, Ankara, 183-190.

Panagopoulos, C. (2004). Consequences of the cyberstate: The political ımlications of digital government in ınternational context. Ed. A. Pavlichev and G. D. Garson, *Digital government: principles and best practices*. Hershey: Idea Group Publishing, 116-132.

Raiu, C.; Moore, D.; Guerrero-Saade, J. A. ve Rid, T. (2017). Penquin's moonlit maze. https://securelist.com/penquins-moonlit-maze/77883/, 15.02.2018.

Sadioğlu, U. ve Erdinçler, R. E. (2017). Bilgi teknolojileri konusunda devlet deneyimleri: Güney Kore'de e-devlet ve geleceği. *I. Kamu Yönetimi ve Teknoloji Çalıştayı*. 12-14 Mayıs 2017, Alanya, 1-9.

Sağıroğlu, Ş. ve Vural, Y. (2010). E-devlette bilgi güvenliği ve çözüm önerileri-2. *Telekom Dünyası*, Nisan, 72-80.

Schaar, P. (2017). Data protection empowerment. *Cyber security*. Ed. Ferri Abolhassan, Cham: Springer, 21-26.

Sevinç, İ. ve Şahin, A. (2013). Kamu çalışanlarının e-devlet uygulamalarında karşılaştıkları sorunların belirlenmesine yönelik Karaman ilinde bir araştırma. *Süleyman Demirel Üniversitesi İ.İ.B.F. Dergisi,* 18 (2), 197-212.

Sinclair, J. and Irani, T. (2013). Advocacy advertising for biotechnology: The effect of public accountability on corporate trust and attitude toward the ad. *Journal of Advertising*, 34 (3), 59-73.

Sindre, G. and Opdahl, A. L. (2005). Eliciting Security Requirements with Misuse Cases. *Requirements Engineering, Vol. 10*, No. 1, pp. 34-44.

Stibbe, M. (2005). E-government security. *Infosecurity Today*, 2 (3), 8-10.

Söylemez, A. (2016). Geçmişten günümüze Türkiye'de uygulanan önemli e-devlet projeleri. Ed. A. Şahin ve E. Örselli, *Teoriden Uygulamaya E-Devlet*. 2. Baskı, Konya: Atlas Akademi, 149-174.

Subashini, S. ve Kavitha, V. (2011). A survey on security ıssues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 33 (1), 1-11.

Şahin, A. ve Örselli, E. (2003). E-devlet anlayışı sürecinde Türkiye. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (9), 343-356.

Şahin, A. (2007). Türkiye'de e-belediye uygulamaları ve Konya örneği. *Erciyes Üniversitesi İ.İ.B.F. Dergisi*, (29), 161-189.

Şahin, A., Örselli, E. ve Taşpınar, Y. (2016). *Etik ve güven*. 1. Basım, Konya: Atlas Akademi.

Şahinaslan, E. (2013). Bilgi ve bilgi teknolojilerine ait risklerin yönetilmesinde arayış, yöntem ve çözüm önerileri. *XIII. Akademik Bilişim Konferansı Bildiriler Kitabı*. Ed. M. Akgül, vd., 2-4 Şubat 2011, Malatya, 573-577.

Şataf, C., Çiçek, H. G. ve Dikmen, S. (2013). Kamu hizmetlerinin sunulmasında e-devlet uygulamalarının toplumsal algı düzeyi üzerine ampirik bir çalışma. *11. Uluslararası Bilgi, Ekonomi ve Yönetim Kongresi Bildirileri*. 27-30 Kasım 2013, Valletta/Malta, 1-15.

Şirin, M. (2006). Denetimde kanıt teorisi ve gelişimi. *Sayıştay Dergisi*, (61), 23-36.

Şişman, A., Alkış, Z. ve Maraş, E. E. (2011). E-devlet ve m-devlet'in geliştirilmesinin önündeki engel: sayısal uçurum. *Harita Teknolojileri Elektronik Dergisi*, 3 (1), 27-37.

Tanrıkulu, C. (2009). Türk ve Avusturya hukukunda elektronik tebligat. *TBB Dergisi*, (85), 315-331.

Tarhan, A. (2011). *Kamu yönetiminde halkla ilişkiler ve e-devlet*. 1. Baskı, Konya: Palet Yayınları.

Tataroğlu, M. (2009). E-devlet'te kullanılan gözetim ve kayıt teknolojilerinin mahremiyet üzerinde etkileri. *Abant İzzet Baysal Üniversitesi SBE Dergisi*, 1 (18), 95-120.

Tataroğlu, M. (2013). Mahremiyet sorunlarının önlenmesinde mahremiyet etki değerlendirmesi (MED). *Yönetim ve Ekonomi*, 20 (1), 263-289.

Temür, N. (2012). İç güvenlik politikaları ve e-devlet. Ed. M. Z. Sobacı ve M. Yıldız, *E-devlet: kamu yönetimi ve teknoloji ilişkisinde güncel gelişmeler*. Ankara: Nobel Akademik Yayıncılık, 501-526.

Tolbert, C. J. and Mossberger, K. (2006). The effects of e-government on trust and confidence in government. *Public Administration Review*, 66 (3), 354-369.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB) (2016a). 2016-2019 ulusal siber güvenlik stratejisi. www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf, 17.02.2018.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB) (2016b). 2016-2019 ulusal e-devlet stratejisi ve eylem planı. www.edevlet.gov.tr/wp.../2016-2019-Ulusal-e-Devlet-Stratejisi-ve-Eylem-Plani.pdf, 17.02.2018.

United Nations (UN) (2010). E-government survey 2010, https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2010-Survey/Complete-survey.pdf, (Erişim Tarihi: 27.01.2018).

United Nations (UN) (2016). E-government survey 2016, https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2016-Survey/Executive%20Summary.pdf, (Erişim Tarihi: 27.01.2018).

Ünver, M. ve Canbay, C. (2010). Ulusal ve uluslararası boyutlarıyla siber güvenlik. *Elektrik Mühendisliği*, (438), 94-103.

Ünver, M., Canbay, C. ve Mirzaoğlu, A. G. (2011). *Siber güvenliğin sağlanması: Türkiye'deki mevcut durum ve alınması gereken tedbirler*. 1. Basım, Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Ünver, G. N. (2017). Ulusal siber güvenlik strateji belgelerinde insan hakları. *Siber Politikalar Dergisi,* 2 (4), 104-129.

Vural, Y. ve Sağıroğlu, Ş. (2008a). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniversitesi MMF Dergisi,* 23 (2), 507-522.

Vural, Y. ve Sağıroğlu, Ş. (2008b). Ülke bilgi güvenliği. *3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*. 25-27 Aralık 2008, Ankara, 3-8.

Yalçınkaya, B. (2014). *E-devlet üstveri standardının oluşturulması ve Türkiye için modellenmesi*. Marmara Üniversitesi Türkiyat Araştırmaları Enstitüsü Doktora Tezi, İstanbul.

Yıldız, M. (2006). Kamu siyasaları açısından cep telefonu teknolojisi ve mobil devlet. *H. Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi,* 24 (1), 241-263.

Yıldız, Ö. R. (2007). Bilişim sistemleri denetimi ve Sayıştay. *Sayıştay Dergisi*, (65), 173-185.

Yılmaz, E. N., Ulus, H. İ. ve Gönen, S. (2015). Bilgi toplumuna geçiş ve siber güvenlik. *Bilişim Teknolojileri Dergisi,* 8 (3), 133-146.

Yılmaz, O. (2017). Küreselleşme sürecinde dönüşen güvenlik algısı ve siber güvenlik. *Siber Politikalar Dergisi,* 2 (4), ss. 22-43.

Warkentin, M., vd. (2002). Encouraging citizen adoption of e-government building trust, *Electronic Markets,* 12 (3), 157-162.

Welch, E. W., Hinnant, C. C. ve Moon, M. J. (2005). Linking citizen satisfaction with e-government and trust in government. *Journal of Public Administration Research and Theory, Vol. 15*, No. 3, pp. 371-391.

West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes. *Public Administration Review,* 64 (1), 15-27.

Zengin, S. (2017). Yanılsamadan gerçekliğe: kamu yönetiminde e-devlet etkisi. *VIII. Ulusal Sosyoloji Kongresi Bildiriler Kitabı*. Ed. F. Artar ve A. Bakioğlu, Ankara: Sosyoloji Derneği Yayınları, No. 24, 614-620.

Zhou, Z. ve Hu, C. (2008). Study on the e-government security risk management. *IJCSNS International Journal of Computer Science and Network Security,* 8 (5), 208-213.

https://www.btk.gov.tr/tr-TR/Sayfalar/SG-USOM-ve-Kurumsal-SOME, 18.02.2018.

http://www.tbd.org.tr/ulusal-bilgi-guvenligi-teskilati-ve-gorevleri-hakkinda-kanun-tasarisi/, 08.02.2018.

https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance, 15.02.2018.

http://www.udhb.gov.tr/duyuru-56-cryptolocker-virusu-hakkinda-bilgilendirme-.html, 18.02.2018.