

T.C.
FIRAT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TEKNOLOJİ VE BİLGİ YÖNETİMİ
ANABİLİM DALI



BİLGİ GÜVENLİĞİ AÇISINDAN BİR DEĞERLENDİRME:
e-DEVLET UYGULAMALARI

YÜKSEK LİSANS TEZİ

DANIŞMAN
Dr. Öğr. Üyesi İlke Bezen TOZKOPARAN

HAZIRLAYAN
İlknur TUNCER

ELAZIĞ-2019

T.C.
FIRAT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TEKNOLOJİ VE BİLGİ YÖNETİMİ ANABİLİM DALI

BİLGİ GÜVENLİĞİ AÇISINDAN BİR DEĞERLENDİRME:
e-DEVLET UYGULAMALARI

YÜKSEK LİSANS TEZİ

DANIŞMAN
Dr. Öğr. Üyesi İlke Bezen TOZKOPARAN

HAZIRLAYAN
İlknur TUNCER

Jürimiz, 19.09.2019 tarihinde yapılan tez savunma sınavı sonunda bu yüksek lisans tezini oy birliği /oy çokluğu ile başarılı saymıştır.

Jüri Üyeleri:

1. Dr. Öğr. Üyesi İlke Bezen TOZKOPARAN
2. Doç. Dr. Erkan Turan DEMİREL
3. Dr. Öğr. Üyesi Emrah AYDEMİR



F. Ü. Sosyal Bilimler Enstitüsü Yönetim Kurulunun 16.07.2019 tarih ve 2019-41 sayılı kararıyla bu tezin kabulü onaylanmıştır.

Prof. Dr. Osman Ömer UMAR
Sosyal Bilimler Enstitüsü Müdürü

ÖZET**Yüksek Lisans Tezi****Bilgi Güvenliği Açısından Bir Değerlendirme: e-Devlet Uygulamaları****İlknur TUNCER****Fırat Üniversitesi****Sosyal Bilimleri Enstitüsü****Teknoloji ve Bilgi Yönetimi Anabilim Dalı****Elazığ – 2019, Sayfa: XII+95**

e-Devlet günümüzde en sık kullanılan ve birey-devlet etkileşiminin verimli bir şekilde yürütülmesi için sıklıkla başvurulmuş bir sistemdir. Teknolojinin hızla gelişmesi, e-Devlet kullanımını yaygınlaştırmıştır. e-Devlet sistemleri yaşayan organizmalardır ve birçok modülden oluşurlar. Bu organizmayı sağlıklı bir şekilde yaşatabilmek ve maksimum seviyede verim sağlayabilmek sosyal bilimler ve fen bilimlerinin çalışma alanı haline gelmiştir. Sosyal bilimler açısından e-Devlet birey-birey, birey-kurum ve kurum-kurum ilişkilerinin efektif hale getirirken, toplumsal yaşamda bir çağın kapılarını aralamaktır ve bu çağ sayısal çağ olarak adlandırılmaktadır. Sağladığı toplumsal katkılarının yanı sıra teknik bir alt yapıya sahip olan e-Devletin bilgisayar bilimleri ve bilgi güvenliği açısından da ele alınması gerekmektedir. Çünkü mahrem veriler herkese açık bir ağda depolanmaktadır. Bu verilerin mahremiyetinin sağlanması günümüzün en önemli problemleri arasında yer almaktadır. Bu problemi çözebilmek için kriptoloji kullanılmaktadır. Kriptoloji temel olarak 3 ana dalda incelenmektedir. Bunlar gizli anahtarlı, açık anahtarlı ve anahtarsız şifreleme algoritmalarıdır. Temel olarak internet üzerinde güvenilir haberleşmenin ve bilgi alışverişinin sağlanması için üç ana dalda bulunan en güçlü algoritmaların bir araya gelmesiyle oluşturulan kriptolojik protokollerin kullanılması gerekmektedir. Bu nedenle e-Devlet sistemleri kriptolojik protokoller kullanarak fiziksel güvenliklerini sağlamaktadır. Ancak bireylerinde e-Devlet uygulamalarına güvenmeleri de gerekmektedir. Güven unsuru sağlandığında e-Devletin efektif kullanımı tam olarak sağlanabilmektedir. Bu nedenle bu tez

alışmasında hem Ortadoęu lkelerinin e-Devlet kullanımı hem de gelişmiş lkelerin e-Devlet kullanımı incelenmiştir. Gelişmiş lkelerde sistemlere olan güven sağlandığı için e-Devlet uygulamaları her alanda kullanılmaktadır. Ancak gelişmekte olan veya siyasi istikrarın sağlanmadığı bölgelerde e-Devlet kullanımı yaygın değildir. Bu sebepten dolayı bu tez alışmasında e-Devlet yapısı bilgi güvenliği açısından ele alınmıştır. Öncelikle e-Devlet tanımı ve e-Devlet bileşenleri tanımlanmıştır. Ardından e-Devlet bilgi güvenliği açısından ele alınmış ve bilgi güvenliğine bağlı bileşenlerden (kriptoloji, bilişim hukuku) bahsedilmiştir. Özetle, bu tez alışmasıyla e-Devlet kavramı teknoloji ve bilgi yönetimi açısından kapsamlı olarak ele alınmıştır ve bilgi güvenliği hususları tartışılmıştır.

Anahtar Kelimeler: e-Devlet, e-Devlet Uygulamaları, Bilgi Güvenliği, Teknoloji, Bilgi Yönetimi

ABSTRACT**Master Thesis****An Evaluation in terms of Information Security: e-Government Applications****İlknur TUNCER****The University of Firat****The Institute of Social Science****The Department of Technology and Information Management****Elazığ – 2019, Page: XII+95**

The e-Government is the most frequently used system today and is frequently used for efficient individual-state interaction. The rapid development of technology has spread the use of e-Government. e-Government systems are living organisms and consist of several modules. To maintain this organism in a healthy way and to provide maximum yield has become the field of study of social sciences and science. In terms of social sciences, e-Government is to open the gates of an age in social life while making individual-individual, individual-institution and institution-institution relations effective. In addition to its social contributions, e-Government, which has a technical infrastructure, needs to be addressed in terms of computer science and information security. Because confidential data is stored in a public network. Ensuring the privacy of these data is one of the most important problems of today. Cryptology is used to solve this problem. Cryptology is mainly studied in 3 main branches. These are secret key, public key and keyless encryption algorithms. In order to ensure reliable communication and exchange of information on the internet, it is necessary to use cryptological protocols which are formed by combining the most powerful algorithms in three main branches. For this reason, e-Government systems provide physical security by using cryptological protocols. However, they should also rely on e-Government practices in their individuals. Effective use of the e-Government can be fully achieved when the trust element is provided. Therefore, in this thesis, both the e-Government usage of the Middle East countries and the e-Government usage of the developed

countries were examined. In developed countries, e-Government applications are used in every field since trust is provided to the systems. However, the use of e-Government is not widespread in developing or political stability areas. For this reason, e-Government structure is discussed in terms of information security in this thesis. Firstly, the definition of e-Government and its components are defined. Then, e-Government information security is discussed and components related to information security (cryptology, information law) are mentioned. In summary, with this thesis, the concept of e-Government has been comprehensively discussed in terms of technology and information management and information security issues have been discussed.

Key Words: e-Government, e-Government Applications, Information Security, Technology, Information Management



İÇİNDEKİLER

ÖZET	I
ABSTRACT.....	IV
İÇİNDEKİLER.....	VI
TABLOLAR LİSTESİ	IX
ŞEKİLLER LİSTESİ	X
ÖNSÖZ	XI
KISALTMALAR	XII
GİRİŞ.....	1
1. Çalışmanın Amacı ve Önemi	2
2. Çalışmanın Hipotezleri.....	3
3. Çalışmanın Yöntemi	3
4. Çalışmanın Sınırlılıkları.....	3

BİRİNCİ BÖLÜM

1. BİLGİ GÜVENLİĞİ	4
1.1. Bilgi Güvenliğini Etkileyen Temel Kavramlar	4
1.1.1. Teknoloji Kavramı.....	6
1.1.2. Bilgi Kavramı	8
1.1.3. Bilgi Yönetimi Kavramı	10
1.1.4. Bilgi Güvenliği Kavramı	14
1.1.5. Bilgi Toplumu	16

İKİNCİ BÖLÜM

2. e-DEVLET GELİŞİMİ.....	19
2.1. e-Devlet	19
2.2. e-Devletin Tarihsel Perspektifi	29
2.3. e- Devletin Yaşam Döngüsü	30
2.4. e-Devlet Uygulamalarında Bilgi Güvenliği	32
2.4.1. e-Devlet Güvenliği	35
2.4.2. e-Devlet Güvenliğini Etkileyen Teorilerin Sentezi	37
2.4.3. e-Devlete Politik Bağlılık ve Halkın Güveni.....	39
2.4.4. Teknoloji ve e-Devlet Güvenliği İlişkisini Etkileyen Faktörler	41
2.4.5. Kullanıcıların Gizliliği.....	41

2.4.6. Web Tasarım Kalitesi	42
2.4.7. e-Devlet Güvenliği ve Kullanıcı Merkezliliği	43
2.4.8. e-Devlet Güvenlik Problemleri.....	44
ÜÇÜNCÜ BÖLÜM	
3. DÜNYADA VE TÜRKİYE’DE e-DEVLET	46
3.1. Dünyada e-Devlet Gelişmişlik Analizi	46
3.2. Dünyada e-Devlet Kullanımı	51
3.2.1. Amerika Birleşik Devletleri	52
3.2.2. İngiltere.....	52
3.2.3. Finlandiya	53
3.2.4. Irak.....	53
3.2.5. Libya.....	56
3.2.6. Gürcistan.....	57
3.2.7. Bahreyn.....	59
3.2.8. Libya.....	59
3.3. Türkiye’de e-Devlet Uygulamaları Tarihsel Perspektifi.....	60
3.4. Türkiye’de Yaygın Olarak Kullanılan e-Hizmetler	60
3.4.1. e-Nabız	61
3.4.2. UYAP	62
3.4.3. MERNİS	62
3.4.4. e-Eğitim	63
3.4.5. e-Vergi	63
3.5. Taşrada Kullanılan e-Devlet Uygulamaları	64
3.6. Türkiye’de 2016-2019 Ulusal e-Devlet Strateji ve Eylem Planı	65
3.7. e-Devlet Uygulamalarının Güvenlik Alt Yapıları ve Analizi	67
3.8. Bilişim Suçları ve İlgili Mevzuatlar	69
3.8.1. Bilişim Alanındaki Suçlar	71
3.8.2. Bilgisayar Korsanlığı.....	71
3.8.3. Dolandırıcılığın Nitelikli Hali: Bilişim Sistemlerini Yetkisiz Kullanma	72
3.9. e-Devlet Uygulamalarının Bilgi Güvenliği Alt Yapısını Güçlendirmek için Yapılması Gereken Süreçler	74
SONUÇ VE TARTIŞMALAR.....	76
KAYNAKÇA.....	80

EKLER	94
Ek 1. Orjinallik Raporu	94
ÖZGEÇMİŞ	95



TABLÖLAR LİSTESİ

Tablo 1. e-Devlet Alanında Gelişmiş İlk 10 Ülke İndeksi.....	47
Tablo 2. Çevrimiçi Hizmetler İndeksi Şehirlerin 2018 Yılı Sıralaması.....	50
Tablo 3. Elazığ Valiliğinin Kullandığı e-Uygulamalar.....	64
Tablo 4. Elazığ Belediyesinin Kullandığı e-Uygulamalar	65



ŞEKİLLER LİSTESİ

Şekil 1. Verinin Bilgiye Dönüştürülme Süreci	9
Şekil 2. Bilginin Genel Özellikleri	9
Şekil 3. BM Önerdiği Model	24
Şekil 4. e-Devletin yaşam döngüsü	31
Şekil 5. Bilgi Güvenlik Yönetim Sistemi Süreci	32
Şekil 6. Enigma Makinesi.....	33
Şekil 7. Bilgi Güvenlik Sisteminde Risk Faktörleri	34
Şekil 8. Erişim Kontrolü Blok Diyagramı	34
Şekil 9. Günümüz Ağları ve Güvenlik Önlemleri	36
Şekil 10. 2008-2018 Yılları Arasında Türkiye e-Devlet İndeks Sonuçları	49
Şekil 11. Türkiye’de Resmi Kurumların Sunduğu e-Hizmetler	61
Şekil 12. Etkin e-Devlet Ekosistemi.....	67
Şekil 13. e-İmza Altyapısının Blok Diyagramı	68

ÖNSÖZ

Çalışmam esnasında her türlü hoşgörü, destek ve bilgisiyle bana katkıda bulunan değerli danışmanım Dr. Öğr. Üyesi İlke Bezen TOZKOPARAN'a, uygulama geliştirme esnasında yardımını esirgemeyen Doç. Dr. Şengül DOĞAN'a, Erhan ÖZMEN'e her daim bana destek veren ve yanımda olan çok kıymetli canım eşim Türker TUNCER'e, onlara ayıracağım zamandan feragat eden Durum ve Ömer'ime, arkadaşlarıma ve özellikle anneme,

Teşekkür ederim...

ELAZIĞ-2019

İlknur TUNCER



KISALTMALAR

ABD	: Amerika Birleşik Devletleri
TDK	: Türk Dil Kurumu
BİT	: Bilgi ve İletişim Teknolojileri
MERNİS	: Merkezi Nüfus İdare Sistemi
BM	: Birleşmiş Milletler
CBS	: Coğrafi Bilgi Sistemi
BT	: Bilgi Teknolojileri
GSK	: Güvenilir Soket Katmanı
EGI	: e-Devlet Gelişim İndeksi
YÇHİ	: Yerel Çevrimiçi Hizmetler İndeksi
SKG	: Sürdürülebilir Kalkınma Gündemi
DOI	: Roger'ın İnovasyon Yayılımı
TKM	: Teknoloji Kabul Modeli
UTM	: Uygulama-Teknoloji Modeli
İBE	: İnsan Bilgisayar Etkileşimi
UYAP	: Ulusal Yargı Ağı
TCK	: Türkiye Cumhuriyeti Kanunu
ESHS	: Elektronik Sertifika Hizmet Sağlayıcısı

GİRİŞ

e-Devlet uygulamaları verimliliği ve şeffaflığı arttırdığı için dünya genelinde kullanımı, hızla artmaktadır. Zaman içerisinde devlet teorisi için birçok modeller geliştirilirken, e-Devlet ortamının geliştirilmesi için yapılandırılmış bir teori mevcut değildir. e-Devlet, gün geçtikçe herkes tarafından kabul gören bir uygulamadır. Dünyanın birçok ülkesinde e-Devlet uygulamaları kullanılmaktadır (Demirel, 2006). e-Devlet uygulamaları saydamlığı ve verimliliği arttırdığı için kullanımı hızla yaygınlaşmaktadır. e-Devlet aynı zamanda kamu sektöründeki geliri, rekabeti ve pazarlamayı artırmak için de gereklidir. Türkiye’ de e-Devlet, işgücünden ve zamandan tasarruf sağlayan çok etkili kullanılan bir uygulamadır. e-Devlet kullanılarak, iş gücü, zaman, mekân gibi durumlardan tasarruf sağlanmaktadır. Örneğin; e-Devlet etkili bir şekilde kullanılırsa, bir hükümet konağının olduğu caddenin trafiği ve insan popülasyonu azalacağı, binaların güvenliğinin sağlanmasının daha kolay bir hale geleceği düşünülmektedir.

e-Devlet ortamında bankacılık hizmetleri, belediyeler, üniversiteler, bakanlıklar ve diğer özel kurumlar hizmet vermektedir. Örneğin bir öğrenci üniversiteye kayıt olacağı zaman, kazandığı üniversiteye ders döneminden önce gidip kayıt yaptırmak yerine, e-Devlet üzerinden kayıt yaptırarak iş ve işlemlerini halletmektedir. Bu denli faydalı bir uygulama Türkiye’ de halen tam anlamıyla kullanılmamaktadır. Buna örnek olarak belediyeleri ele alırsak Türkiye’ de sadece 72 il ve 300 belediye e-Devlet üzerinden hizmet sağlamaktadır. Tüm belediyelerin veya tüm kurumların e-Devlet üzerinden işlem yapmamasının temel sebebi dijital okuryazarlığının ve bilgisayar alt yapısının eksik olmasından kaynaklanmaktadır. Ayrıca bireylerin kullandığı teknoloji ve bilgi yönetimi süreçlerinin efektif olarak kullanılamaması e-Devlet uygulamalarının yeterince gelişemediğinin açık bir göstergesidir. e-Devlet sisteminde karşılaşılan en önemli sorunlardan birisi de bilgi güvenliğidir. Bazı kurum ve kuruluşlar internet üzerinden veri paylaşımının güvenilir bir yöntem olduğuna inanmamaktadır. Bunun en önemli sebebi ise sayısal suçlardaki ve bilgisayar korsanlığında ki artıştır. Bu durum e-Devlet kullanımında ki en önemli dezavantajlardan birisidir. Bu tür kısıtlayıcı bir engeli aşmak için devletlerin kendi güvenilir bilgi güvenliği politikalarını geliştirmeleri gerekmektedir (Erdal, 2004).

Bunların yanı sıra e-Devlet sistemi bilinen devlet teoremini de kökünden sarsan bir uygulamadır. e-Devlet ile birlikte devletteki bürokratların ve karar mercilerinin güvenilirliği daha fazla sorgulanır hale gelmiştir. Özellikle yapay zekânın hızla geliştiği günümüzde, e-Devlet sisteminden alınan verilerle bir yapay zekâ oluşturulup kuralların ve yasaların yapay zekâ tarafından belirlenmesi teoremleri dahi ortaya atılmıştır. Ancak günümüzde bu teoremler, kabul gören teoremler arasında yer almamaktadır. Gelecekte böyle bir teoremin ne denli kabul göreceği de tartışma konusudur (Demirel, 2006).

e-Devlet uygulamaları yapılandırılmış bir teoreme sahip olmamasına rağmen, sağladığı avantajlar sayesinde kullanımı hızla yaygınlaşmakta ve bu alanda geliştirilen uygulamalar artmaktadır. Bu sebeple e-Devlet uygulamalarının eksikliklerinin belirlenmesi ve güncel platformlarda güvenli e-Devlet uygulamalarının oluşturulması için bilimsel olarak incelenmesi gerekmektedir. Bu tez çalışmasında e-Devlet uygulamalarının yaygın kullanımı için teknoloji ve bilgi yönetiminin kullanılmasının gerekliliğinden bahsedilecektir. Ayrıca, bilgi güvenliği açısından e-Devlet uygulamaları değerlendirilecektir. Bununla beraber, e-Devlet uygulamasının günümüzde kullandığı güvenlik alt yapısından bahsedilecek ve gelecekteki teknolojilerin bilgi güvenliğine etkisi tartışılacaktır.

1. Çalışmanın Amacı ve Önemi

Kamu hizmetlerinin etkin ve verimli bir şekilde verilebilmesi için e-Devlet yaşam döngüsünün sürekliliği bir amaç olarak karşımıza çıkmaktadır. Bahsedilen yaşam döngüsünün en önemli bacaklarından birisi de bilgi güvenliğidir (Koçak ve Memiş, 2018). Bilgi güvenliğinin temel amacı bireylerin verilerine müdahale edebilecek yetkisiz erişimlerin engellenmesi ve kullanıcıların ilgili platformda özgürce hareket edebilmesinin sağlanmasıdır. Ayrıca literatürde çok disiplinli bir bakış açısının olmaması (sosyal ve fen bilimlerinin bir arada kullanılarak çalışmaların oluşturulmaması) e-Devlet ve bilgi güvenliği ilişkisinin net bir şekilde ortaya koyulmasının önünde büyük bir engel teşkil etmektedir. Bu tez çalışmasının temel amacı bilgi güvenliği ve e-Devlet ilişkisini net bir şekilde ifade etmek ve bu konuyu teknoloji ve bilgi yönetimi açısından ele almaktır.

2. Çalışmanın Hipotezleri

e-Devlet uygulamalarında bilgi güvenliğinin önemini tartışmak ve maddi örneklerle desteklemek için kullanılan hipotezler aşağıdaki gibi verilmiştir.

- e-Devlet uygulamaları yüksek gelişmişlik indeksine sahiptir.
- Türkiye’deki e-Devlet uygulamaları Dünya’da üst sıralardadır.
- e-Devlet uygulamaları yüksek bilgi güvenliği alt yapısına sahiptir.
- e-Devlet uygulamalarına yapılabilecek olası saldırılar yasalar ile koruma altına alınmıştır.

3. Çalışmanın Yöntemi

Günümüzde elektronik sözcüğü “e” harfiyle ifade edilmektedir. Bu sebepten dolayı elektronik devlet uygulamaları e-Devlet kısaltması kullanılarak ifade edilmiştir. Bu tez e-Devlet incelemeleri ve uygulamaları üzerine temel bir nitelik taşımakta, elde edilen veriler, örnekler ve istatistiki bilgilerle ifade edilmeye çalışılmıştır. Konuya ilişkin araştırma yapılırken, geniş ölçekli makale ve kitap taraması gerçekleştirilmiştir. Teknolojik gelişmelerin önemli oranda hız kazandığı ve toplumların yaşamını etkilediği 1972-2019 yılları arasındaki bazı çalışmalarla sınırlandırılması yapılmış, bu çerçevede yayınlanan kitap ve makaleler kullanılmıştır. Ayrıca uluslararası kuruluşların yayınladığı bilimsel çalışmalar incelenmiştir. Science Direct, PubMed, Google Scholar, YÖK Tez arama motorlarında yapılan e-Devlet, e-government, bilgi güvenliği, information security anahtar sözcükleri ile aramalar yapılmıştır. Toplanan bilimsel çalışmalar incelenmiş ve tez içerisinde analizleri sunulmuştur.

4. Çalışmanın Sınırlılıkları

- Çalışmadaki bilimsel araştırmalar 1972-2019 yılları arasındakiler ile sınırlıdır.
- e-Devlet, e-government, bilgi güvenliği, information security anahtar sözcükleri bilimsel araştırmaların anahtar kelimelerinde hem İngilizce hem Türkçe dillerine ait olarak araştırılmış olup yalnızca bu anahtar kelimelerdeki çalışmalar ile sınırlıdır.
- Science Direct, PubMed, Google Scholar, YÖK Tez arama motorları ile sınırlıdır.

BİRİNCİ BÖLÜM

1. BİLGİ GÜVENLİĞİ

1.1. Bilgi Güvenliğini Etkileyen Temel Kavramlar

Güvenlik düşmanca davranışlardan veya durumlardan etkilenmeyen, aynı zamanda koruyucu önlemlerin oluşturulması ve sürdürülmesinden kaynaklanan bir durum olarak tanımlanabilmektedir. “Bilgi güvenliği” terimi, bilginin bulunduğu her platformu kapsar, böylece bilgi güvenliği sadece bilgisayar güvenliği olarak değil aynı zamanda herhangi bir bilgi biçimini korumak anlamına da gelir (Topaloglu, Calp, & Turk, 2019). Bilgi güvenliği, bilgi sürekliliğini sağlamak, riski en aza indirmek, bilgilerin işlendiği sistemlerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için temel yapının çeşitli tehditlere karşı korunması olarak tanımlanabilir. Dünya ağ merkezli hale geldikçe, güvenlik önemli bir sorun olmaya devam ederken, bilgi ve veri güvenliği çoğu ülkenin gündeminde yer almaktadır. Devlet kurumlarının ve kritik altyapıların (örneğin savunma sanayii, sağlık, enerji, finans) güvenlik kaygıları üzerine pek çok yöntem ve teknik geliştirilmektedir (Akman, 2019). Ayrıca, devletlerin çoğu, savunma tarafında kendi mahremiyetini korumak ve hücum tarafında istihbarat çalışmaları ve elektronik savaşı yürütmek için siber ordular kurmaktadır. Öte yandan, gittikçe artan bilgi akışı ve giderek nitelikli veri varlıklarına hızlı bir şekilde erişme fikri nedeniyle genişleyen veri havuzları, herhangi bir devletin görmezden gelemeyeceği bir sorun teşkil etmektedir. Bir devlet olarak, bu nitelikli verileri korumak için yeterli kaynak tahsis etmemek ve sorunun önemini göz ardı etmek kesinlikle ağ sistemlerindeki zayıflıkları doğuracak ve kaçınılmaz olarak ülke imajına zarar verecektir (Durankaya, Gökşen, & Eminağaoğlu, 2018).

Ancak günümüzde internet bankacılığı ve e-Devlet gibi kritik verilerin olduğu çevrimiçi sistemler yaygın olarak kullanılmaktadır. Bireyler şubelere gitmek yerine mevcut bankacılık işlemlerini uygulamalar veya tarayıcılar kullanarak çevrimiçi yapmaktadır. Mağazaya gitmek yerine kredi kartı ile çevrimiçi alışveriş yapabilmektedirler.

e-Devlet açısından da hizmetler ele alınacak olursa, vatandaşlar, sıra beklemeden sadece belirli bir zamanda e-Devlet ortamını kullanarak devlet hizmetlerinden kolayca yararlanabilmektedir. Ancak bu platformlarda paylaşılan kritik verilerin güvenliğinin

sağlanması yönetim açısından hayati öneme sahiptir. Bu sebepten dolayı e-Ticaret ve e-Devlet platformları benzer bilgi güvenliği protokollerini kullanarak bilgi güvenliğini sağlamaktadır. Tek fark e-Devlet platformlarında güvenlik seçeneklerinin daha geniş yelpazede sunulmasıdır (Balcı, 2008).

Bunların da ötesinde, insanlar düşüncelerini dünyaya açıklayabilmekte ve sosyal medya yardımı ile milyonlarca kişiye ulaşabilmektedir. Ayrıca Mısır'da gerçekleşen Müslüman Kardeşler devriminin bir sosyal ağ kullanılarak örgütlendiği de unutulmamalıdır.

Son on yılda gerçekleşen tüm bu gelişmeler insanlık tarihinde yer alan devrimci yeniliklerdir. Ancak, tüm bu yenilikler günlük işleri kolaylaştırmanın yanı sıra çok önemli riskleri de içermektedir. İnternete bağlı cihaz sayısının artması, geniş bir yelpazedeki cihazların saldırılara maruz kalabileceği anlamına gelmekte ve aynı zamanda riskin büyüklüğünün ne kadar olduğunu göstermektedir. Bu bağlamda, güvenliğin ne kadar iyi ve kesin bir şekilde sağlanabileceği ile ilgili sorular ortaya çıkmaktadır. Algoritmalar, yöntemler ve cihazlar ne denli güvenilir olursa olsun, bilgi güvenliği varlıklarından birisi de insandır. Eğer bir bireyin bilgi güvenliği farkındalığı göz ardı ediliyorsa, sistemde güvenliğin sağlanması imkânsız hale gelmektedir. Bununla birlikte birçok araştırmacı bilgi güvenliği yapısının en zayıf halkasını insan olarak tanımlamaktadır. Örneğin kamu kurumlarının bilişim alt yapılarının son teknoloji ve güvenilir cihazlarla yapılandırılması bilgi güvenliğinin %100 sağlandığı manası gelmemektedir çünkü idari personelin yanlış veya eksik bilgi birikimi işlemlerinin başarısızlıkla sonuçlanmasına neden olabilmektedir. Bu nedenle bilgi güvenliğinin bir bütün olarak ele alınması ve yönetiminin profesyonelce yapılması gerekmektedir.

Bilgi güvenliğini oluşturan temel üç etmen vardır ve bu etmenler bilgi güvenliği üçgenini oluşturmaktadır. Bunlar:

- **Erişilebilirlik:** Bilgilerin veya kaynakların izinsiz olarak durdurulmasının önlenmesi anlamına gelmektedir. Bilgi, yetkili kullanıcılar için mümkün olduğunca serbest olmalıdır.
- **Bütünlük:** Bilginin hatalı olarak değiştirilmesinin önlenmesi basamağıdır. Yetkili kullanıcıların eksik bilgiler sonucunda yaptığı işlemler hataların oluşmasının ve verilerin değiştirilmesinin en büyük nedenidir. Yanlış veriyi sistem içinde saklamak veri kaybetmek kadar kötü olabilir.

- **Gizlilik:** Bilgilerin yetkisiz elde edilmesinin önlenmesi bu basamağın temel amacını oluşturmaktadır. Bu, güvenlik önlemlerinin düşük olmasının veya personel tarafından bilgi sızmasının bir sonucu olabilir. Zayıf güvenlik önlemlerine bir örnek, hassas bilgilere isimsiz erişim şeklinde olabilir (Balay, 2004; H. Koçak & Memiş, 2018).

Bilgi güvenliğinin daha net anlaşılması için bu bölümde bilgi güvenliğini etkileyen temel kavramlardan bahsedilmiştir. Bilgi güvenliği ve e-Devlet kavramları teknoloji ve bilgi yönetimi açısından ele alındığı için temel kavramlar aşağıdaki gibi sıralanmıştır.

- Teknoloji kavramı
- Bilgi kavramı
- Bilgi yönetimi kavramı
- Bilgi toplumu

Yukarıda belirtilen kavramlarla ilgili bilgiler aşağıdaki alt bölümlerde verilmiştir.

1.1.1. Teknoloji Kavramı

Bilgi yönetimini etkileyen unsurlardan biri de teknolojidir. Yaşadığımız çağ bilgi çağı olarak adlandırıldığı için BİT hayatımız sıklıkla yer almaktadır. BİT'deki gelişmeler bilgi yönetimini etkilemektedir ancak teknoloji tek başına bilgi yönetimini tanımlayamamaktadır. Bilgi yönetimi süreci, teknolojiyle olanaklı kılındığında oldukça iyi başarı göstermektedir. Teknolojinin bilgi yönetimi içindeki önemini daha iyi kavrayabilmek için teknolojinin tanımlarına bakmak daha açıklayıcı olacaktır. Kökeni eski Yunancadan gelen (techne- sanat, hüner, maharet ve logia- söyleme, düzenleme yani sanat üzerine konuşma) teknoloji kavramı, çok yaygın olarak kullanılmaktadır. Ancak tanımlaması çok kolay olmayan bir kavramdır (Karakoçak, 2007).

Teknoloji genel olarak, makine, alet, donanım gibi maddi nesneleri çağrıştırıyor olsa da örgüt metotları, sistemler ve teknik gibi anlamları da kapsamaktadır. Türk Dil Kurumu teknolojiyi “bir sanayi dalı ile ilgili yapım yöntemlerini, kullanılan araç, gereç ve aletleri kapsayan bilgi” olarak tanımlanırken, Meyer-Stamer teknolojinin kapsamlı ve yüzeysel iki tanımının yapılabileceğini ifade etmektedir. Yüzeysel anlamda teknoloji, “teknik metotları uygulamak ve geliştirmek için gerekli olan yapma-bilgisidir”. Meyer-Stamer, kapsamlı olarak teknolojinin tanımının dört unsur içerdiğini ve bunların, teknik donanım, yapma bilgisi, örgüt ve ürün olduğunu belirtmektedir. Teknik donanım ile kastedilen; bir ürünü üretmek veya bir hizmeti yerine getirmek için kullanılan özgül

makine veya gereçlerdir. Yapma-bilgisi bilimsel, teknik ve örtük bilgiyi içermektedir. Örgüt ile ifade edilmek istenen, donanım ile yapma-bilgisinin ilişkisi için kullanılan yönetsel metotlar ve son olarak ürün ile ifade edilmek istenen ise üretim sonucunda ortaya çıkan mal veya hizmettir (Karakoçak, 2007).

Teknoloji kavramıyla ilgili yapılan bazı tanımlar incelendiğinde teknolojinin anlamı ekonomik, teknik ve kültürel boyutları olan bir olgu olarak görülmektedir. Teknolojinin bilişim alanındaki tanımı göz önüne alındığında bu tanımın yazılım, donanım ve yapay zekâ bileşenlerinden oluştuğu görülmektedir. Donanım olarak ifade edilmek istenen bir makine veya ekipmanın ve bileşenlerinin fiziksel yapısı ile birlikte mantıksal planıdır. Donanım ürünlerinden bazıları, hacmi küçük kapasiteleri büyük sunucu bilgisayarlar, depolama birimleri, ağ cihazları, mobil cihazlar ve tarayıcılardır. Yazılım, amaçlanan bir işi yapabilmek için veya donanımları amaca uygun kullanabilmek için oluşturulan algoritmaların kod seti olarak ifade edilmiş halidir. Kısacası yazılım, bilgisayar ile son kullanıcı arasındaki irtibatı sağlayan bir köprüdür. Yazılım, bilgi çağıının lokomotif olarak görev yapmaktadır (Sze, 2008). Gelişmiş ülkelerin birçoğu yazılım alanına çok büyük yatırımlar yapmakta ve yazılım bu ülkelere çok önemli katma değerler sağlamaktadır. Örneğin silikon vadisinde bulunan şirketlerin yıllık kazancının 4 trilyon dolar olduğu tahmin edilmektedir ve bu gelir Amerika Birleşik Devletleri (ABD)'nin gayri safi milli hasılasının yaklaşık %20'sini oluşturmaktadır (Hingorani, Gyugyi, & El-Hawary, 2000). Yapay zekâ günümüzün popüler konuları arasında yer almaktadır. Yapay zekânın temel amacı bir işi bilgisayarın otomatik olarak yapması ve olası çözümleri tahmin edebilmesidir. İşlem hızlarının artması nedeniyle yapay zekâda bir devrim yaşanmaktadır. Derin ve aktif öğrenme algoritmaları sayesinde yüz tanıma, kişi sayma, oyun oynama görüntülerdeki nesneleri sınıflandırma gibi birçok uygulama bilgisayarlar tarafından kolaylıkla yapılabilmektedir (Williams, 2004). Bu teknoloji sağlık, savunma, sosyal medya, robotik gibi alanlarda sıklıkla kullanılmakta ve hayatımızı kolaylaştırmaktadır. Yapay zekânın sonucu olarak nesnelerin interneti ve endüstri 4.0 geliştirilmiştir. Nesnelerin interneti kullanılarak akıllı evlerden akıllı şehirlere doğru giden bir süreç meydana gelmektedir. Endüstri 4.0 kullanılarak ise 7/24 üretim yapabilen fabrikalar kurulmaktadır. Buradan anlaşılabileceği gibi yazılım ve bilişim teknolojileri insan hayatında köklü değişikliklere sebep olmaktadır. Bu üç bileşen birbirinden bağımsız değildir ve eşit derecede öneme sahip

olup teknolojinin çekirdeğini oluşturmaktadırlar. Herhangi bir BİT (bilgisayar, Internet, uydu sistemleri gibi) sistemleri bu bileşen aracılığıyla tanımlanabilir (Sze, 2008).

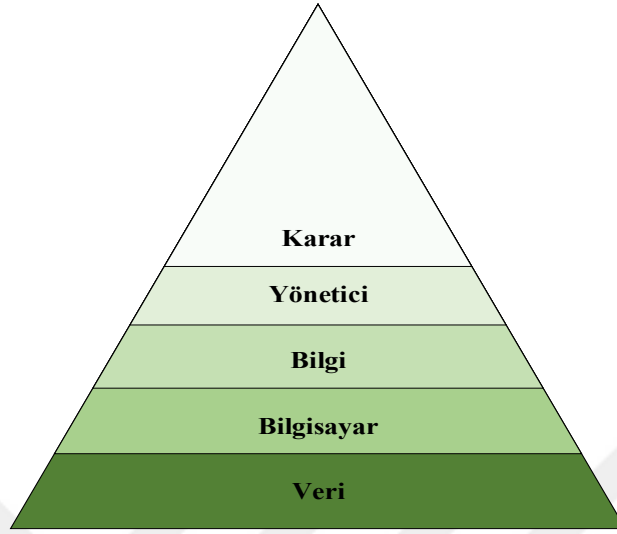
Teknoloji, kurum yaşamında kendini çeşitli şekillerde yansıtır ve etkisini hissettirmektedir. Bu yansıtma alet, araç ve gereçlerde, makinelerde veya üretimin bilinmesinde ortaya çıkarmaktadır. Teknoloji insan yeteneklerini geliştirir ve insan yeteneklerini geliştiren bütün teknik ve süreçleri kapsamaktadır.

Teknoloji ile birlikte hızlı değişim, uygun örgüt yapılarının seçilmesi ve yeni öğrenmeler de beraberinde gelmiştir. Teknoloji ile ilişkili birçok nitelikli uzmanın görev aldığı kurumlarda bu uzmanlara verilen değerin farkı, diğer kurum üyelerini de öğrenmeye yönlendirmektedir. Ayrıca bu nitelikli uzmanların yaptıkları uygulamalar ve diğer kurum çalışanlarına, bilgi ve tecrübelerini aktarmadaki istekleri de, kurumsal öğrenmeye olumlu katkılar sağlamaktadır. Kurum çalışanlarının iş ve işlemlerini daha kolay yapabilmeleri için teknolojik olanakların sağlanması, kurum çalışanlarının teknolojiyle ilgili yeni işlemler öğrenmesi için bir platform oluşturabileceği gibi, kaliteli ürünler vermelerini de sağlamaktadır. Bilgi aracı olarak teknoloji, bilgiyi paylaşma ve yapılan iş ve işlemleri basitleştirme süreçlerindeki engelleri ortadan kaldıracığından, öğrenme etkinliğini ve kurumda öğrenmenin yayılmasını da gerçekleştirir (Balay, 2000).

1.1.2. Bilgi Kavramı

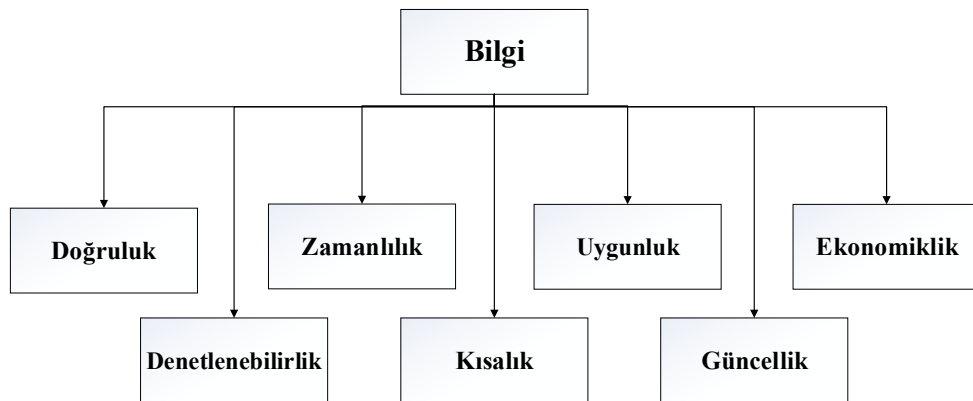
Modern çağın vazgeçilmez unsurları arasında yer alan bilgi ve veri kavramları çağdaş teknolojinin ve bilgi toplumunun can damarıdır. Bununla birlikte, veri ve bilgi kolayca karışır ve sıklıkla birbirinin yerine kullanılmaktadır (içeriğe bağlı olarak) ancak ikisi arasında ince bir fark bulunmaktadır. Bu fark verinin tek başına bir kavramı ifade edememesi ve bilginin kavramları ifade etmede kullanılmasıdır (Balay, 2004). Bu nedenle, onlara ayrı olarak bir varlık olarak bakmak ve ikisi arasındaki farkı ve ilişkiyi anlamak önemlidir. Sözlüklerde, makalelerde veya ders kitaplarında, temelde verileri “gerçekler topluluğu veya bir bilgi ögesi” olarak ifade eden birçok veri tanımı yer almaktadır. Veri “Metin, sayı, grafik, görüntü, ses veya video gibi gerçek dünya olgularının temsili olarak nitelendirilir (Jones et al., 2009). Öte yandan, bilgi veri yığınları içerisinden istenen anlamlı verinin bütünleşmiş formudur yani veriler işlendiğinde veya yorumlandığında ortaya çıkan anlamlı veya faydalı bilgiler oluşturulur. Bilgi keşfi insanların verileri nasıl işlediklerinin incelenmesi ile daha iyi bir

şekilde anlaşılabilir. Veri, bilgiye dönüştürülen hammaddedir; Şekil 1.'de verinin bilgiye dönüştürülme süreci gösterilmiştir.



Şekil 1. Verinin Bilgiye Dönüştürülme Süreci (Jones et al., 2009)

Bireysel veriler kendi başına çok kullanışlı değildir, ancak miktarları, eğilimleri ve kalıpları tanımlanarak daha kolay anlamlandırılabilir (Baeza-Yates & Ribeiro, 2011). Bu ve diğer bilgi kaynakları bilgiyi oluşturmak için bir araya gelirler. En basit anlamıyla bilgi, amaca uygun anlamlandırılan ve farkında olunan olgudur. Bilgi zaman içinde değişiklik göstermektedir ve bilginin ortaya çıkma süreci verinin toplanması ve işlenmesi ile başlamaktadır. Bu bağlamda bilginin genel özellikleri Şekil 2. 'de verilmiştir.



Şekil 2. Bilginin Genel Özellikleri (Baeza-Yates & Ribeiro, 2011)

Mosley'e göre veriler, yorumlandığında veya işlendiğinde, sürekli olarak karar vermede rehberlik eden veya kullanılan çeşitli biçimlerde bilgiye dönüşmektedir (Jones et al., 2009). Bu nedenle, bilgi temel olarak kurum/kuruluşlarda veya bireysel seviyede de kullanılan temel bir işletme varlığıdır, çünkü ister idari, ister yönetim veya stratejik kararlar almak gibi günlük işlemleri ve uygulamaları desteklemektedir (Coleman, 1994).

1.1.3. Bilgi Yönetimi Kavramı

Bilgi yönetimi, bilginin sistematik olarak oluşturulması, paylaşılması ve uygulanması için bireylere ve kurumlara uygun platform sağlayan yeni bir disiplindir. Bu anlayıştan yola çıkarak bilgi yönetimi, bireyler ve kurumları bir bütün halinde incelemektedir. Bütün aşamalarda bilginin açığa çıkarılması temel fonksiyondur (Cover & Thomas, 2012). Aynı zamanda mümkün olduğunca hızlı ve kapsamlı bir şekilde bu bilginin paylaşılması ve organize edilmesi gerekmektedir (Selimoğlu, 2005).

Günümüz rekabet ortamında bilgiyi önemsemek ve katma değer olarak görmek kaçınılmaz hale gelmiştir. Bilgiyi rekabette bir güç olarak önemseyen firmaların ayakta kaldığı, diğer firmaların bu yolda sağlıklı ve başarılı bir şekilde ilerleyemedikleri görülmektedir. Bilginin edinilmesi, kullanılması, saklanması gibi eylemlerle birlikte, bilginin yönetilmesi kavramının önemi çok daha artmıştır. Firmalar için bilgiyi yönetmek, bir eylemden çok bir gereklilik haline gelmiştir. Bilgi yönetiminde başarılı olan firmalar rekabette daha cesur davranabilmişlerdir (Eker et al., 2006). Bilgi yönetimi ile ilgili işletmelerde, bilgiye ulaşmada yaşanan sorunlar ve işletmelerde bilgi yönetimi ile ilgili temel faaliyetleri belirlemek için yapılan işlemler şu şekilde sıralanabilir (Ataman, 2002):

- Bilgi yönetimi ile farklı işletmelerle işbirliğine giderek, farklı deneyimler elde edilebilir.
- Bilgiyi elde etme, paylaşma ve bilgiyi kullanır hale getirme sürecinde, kurum kültürü ve çalışanlarının rolü çok önemlidir.
- Bilgiyi elde etme, değerlendirme çalışmaları, bir performans değerlendirme kriteri olarak alınmalıdır.
- Kurum içerisinde veya doğal çevrede bilgiyi toplamak için bir kadro oluşturulmalıdır.

- Kurumlar bilgi organizasyonu olmayı amaçlamalıdır. Bilginin yönetilmesi için net bir vizyon geliştirilmelidir.
- Örtülü bilgilerin açık bilgilere dönüştürülmesi sağlanmalı ve bilgi kaybını önleyecek çalışmalarda bulunulmalıdır.

Ayrıca bilgi yönetimi konusuyla ilgili birçok tez çalışması yapılmıştır. Bu çalışmaların bazıları aşağıdaki gibi verilmiştir.

Bilgi yönetimi alt yapı yeteneklerinin bilgi yönetimi sürecini ve örgütsel etkinliği ne şekilde etkilediğini ortaya koymayı amaçlamaktadır. Siemens Şirketi' nin Tıp Çözüm Bölümünde anket çalışması yapılmıştır. Anket verilerine göre korelasyon analizi, regresyon analizi ve ANOVA testi uygulanmıştır. Araştırma sonucu, örgütün etkinliğini artırmak için bilgi yönetimi sistemi kurmanın oldukça önemli olduğunu göstermektedir (Selimoğlu, 2005).

Kurumsal bilgi yönetimiyle ilgili yapılan çalışmada; Silivri Hayat Hastanesi' nde anket çalışması uygulanmıştır. Yapılan çalışma sonunda Hayat Hastaneler Grubu'nun, özellikle günümüzde işletmelerin varlıklarını sürdürebilmeleri için son derece önemli olan bilgi yönetiminin önemini kavradığı, eksiklikleri olsa da bilgi yönetimini uygulandığını söylemek mümkün olmuştur (Fırat, 2013).

The Nielson Company'de müşteri ilişkileri yönetiminde bilgi yönetimi ve teknoloji desteği ile CRM (Customer Relationship Management, Müşteri İlişkileri Yönetimi) analizi yapılmıştır. Yapılan araştırma sonucunda; The Nielsen Company müşteri ilişkileri yönetiminde bilgi ve teknolojiyi yeterli düzeyde kullandığı, ancak bilgi ve teknoloji altyapısını güncelleyip geliştirmezse, gelecekte müşteri ihtiyaç ve beklentilerine yanıt veremeyeceği bulgularına ulaşılmıştır (Yıldırım, 2012).

Bilgi yönetimini gerekli kılan nedenleri özetlersek; örgüt içerisindeki bilgi akışının devam ettirilmesi, bilgi yönetimi sistemleri için temel husustur. Ayrıca BİT'deki gelişmeler, yeni, bütüncül ekonomi, müşterilerinin ve beklentilerinin niteliği, bilgi yönetimini örgütler açısından ele alınması gereken bir öncelik haline getirmiştir (Celep, 2003).

Tarihten bugüne bilgi yönetiminin gelişimi incelendiğinde; ilk yıllarda hedefe yönelik yönetim, kantitatif yönetim, çeşitlilik, elektronik veri işleme, program evrimi ve gözden geçirme kavramları ön plana çıkmıştır (Atılğan, 2009). İlerleyen süreçte gelişmelere paralel olarak örtük bilgi kavramı ortaya çıkmıştır. Örtük bilgi özellikle tecrübe eğrisinin önemini artırmıştır ve beraberinde portföy yönetimi, otomasyon ve

stratejik planlama konusu gündeme gelmiştir (Konuskan, 2015). Bir diğer süreçte işin içine kültürel özellikler katılmış ve yerinde yönetim kavramı oluşmaya başlamıştır. Toplam kalite yönetimi, kurumsal kültür, teori Z ve küçülme kavramları önem kazanmıştır ve aynı dönemin sonlarına doğru öğrenme ve öğrenileni unutma stratejilerine doğru gelişme göstermiştir. Daha sonra bu stratejiler ışığında öğrenen örgüt kavramı gündeme oturmuş ve temel beceriler, yeniden yapılanma, stratejik enformasyon sistemleri, intranetler, extranetler ve piyasa değerleri önem kazanmıştır. Bilgi yönetiminin öneminin tam olarak anlaşılıp uygulanmaya başlandığı son yıllar ise bilgi yönetimi birleştirici kuruluş hedefi olarak belirlenmiştir. Bilgi yönetimi kavramının önem kazanması ile düşünsel sermaye, teşebbüs örgütü ve bilgi paylaşım örgütü iş hayatında yerini almıştır. Hali hazırda bilgi yönetimi şuanda kurumların rekabet üstünlüğünde en çok kullandığı yönetim şeklidir (Konuskan, 2015).

Bilgi yönetiminin özellikleri şöyle sıralanabilir:

- Bir kurumda bilgi yönetiminin aktif olması bilginin aktif kullanılmasına bağlıdır.
- Bilginin üretilmesini, saklanmasını, aktarılmasını, erişilmesini, kullanılmasını sağlar. Bilgi yönetimi ile insanların yaratıcı düşüncesi bir araya getirilerek kurumun veya bireylerin problemlerine doğru ve hızlı çözümler sunulur.
- Bilgi yönetimi disiplinler arasıdır. Bilgi yönetimi uygulamalarında bilgi, iletişim, teknoloji, ekonomi, sosyoloji, psikoloji, finans, işletme, mühendislik dallarından yararlanan disiplinler arası bir faaliyettir.
- Bilgi yönetimi, işbirliği ve bilgi paylaşımı üzerine kurulmuştur. Böylelikle bilgi yönetimi kültürün kurum içerisinde ilerlemesi sağlar.
- Bilgi yönetimi ile gizli kalmış örüntüler açığa çıkarılarak kurum için önemli ve kritik öneme sahip bilginin açığa çıkarılması sağlanır (Çapar, 2005).

Bilgi yönetiminin oluşumuyla birlikte belirgin bu özellikler ön plana çıkmış ve bilgi yönetimini benimseyen firmalar da bu özellikleri benimsemişlerdir. Bilgi yönetimi sadece bir yönetim şekli değil, firma kültürünü de değiştiren bir olgudur. Bilgi yönetimiyle hem yönetim anlayışı hem de firma kültürü değişmiş olmaktadır. Bilgi yönetimi firmanın yeniliğe, teknolojiye eğilimini artırır. Firmanın atmosferini değiştirir. Bu bağlamda bilgi yönetimi açısından e-Dönüşüm ile elde edilen sonuçlara göre aşağıdaki sonuçlara ulaşılmaktadır (Kurttepe, 2008):

- e-Dönüşüm sistemleri yöneticinin yönetsel faaliyetlerinde alacağı kararlarda kendisine yardımcı olan, bazı noktalarda kendi başlarına kararlar verebilen sistemlerdir.
- Bu sistemlerin kendilerine ait karar verme mekanizması bulunmaktadır. Ancak bu mekanizma kendilerine e-Dönüşüm yöneticileri tarafından, daha sistemin ilk planlanmaya başladığı andan itibaren verilmeye başlanan bir süreç haline gelmiştir.

İşletmeler arasında bilgi yönetiminin, bilgi teknolojilerini yoğunlukla kullanan açık bilgiye yönelik bir paylaşım olduğu, yöneticilerin tecrübelerinden dolayı elde ettikleri örtük bilgileri işletme içerisindeki diğer bireylerle paylaşımı noktasında yoğun bir çabanın sergilenmediği ortaya çıkmıştır (Gökçe, 2006).

Bilgi yönetim süreci ölçek alınarak KOBİ (Küçük ve Orta Boy İşletmeler) bilgi yönetiminin varlığı tespit edilmeye çalışılmıştır. Türk KOBİ'leri küreselleşmeye ayak uydurmak ve dünya ile uyum sağlamak istiyorlarsa bilgi yönetimine gerekli ilgiyi gösterme zorunluluğu olduğu sonucuna varılmıştır (Koçak, 2004).

Bilgi haritaları iş süreçlerindeki bilgi akışlarını, alt iş süreçlerini ve bu süreçlerde bilgilerin sınıflandırılmasına duyulan gereksinimin açık hale getirilmesi sağlanmıştır. Bilginin oluşturulma sürecinde geline aşamaları göstermede yetersiz kalan çalışma iş süreçleri ve bu süreçlerdeki iş akışlarını, anlamayı kolaylaştıracak şekilde görselleştirmiştir. Hazırlanan program ile organizasyon çalışanlarının tüm dokümanlara, kişisel ve organizasyonel bilgilere ulaşması, bu bilgiler üzerinde değişiklik yapabilmeleri sağlanmıştır (Gürsu, 2003).

Örgütsel kültür, yapı, stratejinin bilgi yönetimine etkisini, bilgi yönetimini olumlu etkileyenlerin sıralamasını örgütsel kültür, yapı ve strateji olarak belirlemiştir ve sonuca göre, olumlu yönde en fazla etkileyen örgütsel kültür, en az olumlu etkisi olan ise örgüt stratejisidir (Zheng et al., 2013).

Bilgi yönetimi uygulamalarında başarılı olmak zordur çünkü kurumların genelindeki bilgi genellikle örtülü bilgidir. Bilgi yönetiminde karşılaşılan engelleri; sektörde yaşanan güncel ve kritik alt yapıya sahip başarı kriterlerinin farklılaşması, teknolojiye yaşanan gelişmeler, orta ve üst kademe yöneticilerin iştiraki (katılımsızlığı), farklı kültür seviyesinden gelen kullanıcılar, üst yönetimin baskısı, mevcut müşterilerin istekleri ve teknolojik zorluklar şeklinde sıralanmaktadır (Martini & Pellegrini, 2005).

Bununla birlikte bilgi yönetimi başarısızlıklarının nedenleri dört ana faktör altında kategorize edilmiştir. Bu faktörler teknoloji, kültür, içerik ve proje yönetimi faktörü olarak sıralanmaktadır. Bilgi yönetiminde bu faktörler dikkate alındığında planlama, uygulama, hayata geçirme ve kurumsallaştırma olarak tanımlanan sonuçlar ortaya çıkmaktadır. Aynı zamanda bilgi yönetimi ve uygulamalarında olumsuz sonuçlar ile karşı karşıya gelmemek için yöneticilerin çeşitli çözüm önerilerinde bulunmaları gerektiğini savunmuşlardır (Lam & Chua, 2005).

Kurumların bilgi yönetimini uygulamadaki başarısızlık faktörleri pozitif getirilerin farkında olunmaması, bilgi yönetiminin bilinmemesi, yeteri kadar insan kaynağının olmaması, zaman problemi, bilgi yönetimi kavramının tam olarak anlaşılamaması, finansal kaynaklarda karşılaşılan yetersizlik ve üst yönetimin yeniliklere kapalılığı şeklinde sıralanmaktadır. Bilgi yönetiminin en büyük problemi örgüt kültürü olarak tespit edilmiştir. Son olarak ortaya çıkan problemin nitelendirilememesi, yöneticilerin beklenenden az desteklemesi, örgütsel yapı, bireysel çalışmaya odaklanması, örgüt içerisinde çalışanların ödül bazlı güdülenmemesi şeklinde sıralanmaktadır (Dwivedi et al., 2015).

İncelenen bazı çalışmalarda da bilgi transferi sürecinde ortaya çıkan engellere odaklanılmıştır. Bilginin bireyden takıma, takımdan bireye, takımdan örgüte, örgütten takıma, örgütten örgütler arasına transferinde yaşanan güçlükler maddeler halinde toplanmıştır. Sonuç olarak da bu güçlüklerin kaynağının neler olduğu belirlendiğinde bilgi transferinde ortaya çıkan engellerin aşılabileceği vurgulanmıştır.

1.1.4. Bilgi Güvenliği Kavramı

Ülke olarak her ne kadar pek çok alanda siber bağımlılık düzeyimiz yüksek olsa da yukarıda belirtilen hususlar siber savunma gücümüze olumlu etki edecektir. Bu sayede bu geçiş sürecinin en az zararlar atlatılması sağlanabilecektir. Ülkelerin siber bağımlılığı, sahip oldukları siber savaş ve siber savunma gücünü de yakından etkilemektedir. Ülkelerin siber savaş kapasitesinin belirlenmesinde, siber savaş kabiliyeti açısından olumlu bir katkıda bulunan bir unsur (bilgi ve iletişim ağı altyapısının yaygınlığı gibi) aynı zamanda siber saldırılara karşı hedef de olduğundan, siber bağımlılık ve siber savunma açısından da negatif olarak da etkileyebilen bir ikilem olarak karşımıza çıkabilmektedir (Çiftçi, 2013).

Güvenlik düşmanca davranışlardan veya durumlardan etkilenmeyen, aynı zamanda koruyucu önlemlerin oluşturulması ve sürdürülmesinden kaynaklanan bir durum olarak tanımlanabilmektedir. “Bilgi güvenliği” terimi, bilginin bulunduğu her platformu kapsar, böylece bilgi güvenliği sadece bilgisayar güvenliği olarak değil aynı zamanda herhangi bir bilgi biçimini korumak anlamına da gelir (Topaloglu, Calp, & Turk, 2019). Bilgi güvenliği, bilgi sürekliliğini sağlamak, riski en aza indirmek, bilgilerin işlendiği sistemlerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için temel yapının çeşitli tehditlere karşı korunması olarak tanımlanabilir. Dünya ağ merkezli hale geldikçe, güvenlik önemli bir sorun olmaya devam ederken, bilgi güvenliği ve veri güvenliği çoğu ülkenin gündeminde yer almaktadır. Devlet kurumlarının ve kritik altyapıların (örneğin savunma sanayii, sağlık, enerji, finans) güvenlik kaygıları üzerine pek çok yöntem ve teknik geliştirilmektedir (Akman, 2019). Ayrıca, devletlerin çoğu, savunma tarafında kendi mahremiyetini korumak ve hücum tarafında istihbarat çalışmaları ve elektronik savaşı yürütmek için siber ordular kurmaktadır. Öte yandan, gittikçe artan bilgi akışı ve giderek nitelikli veri varlıklarına hızlı bir şekilde erişme fikri nedeniyle genişleyen veri havuzları, herhangi bir devletin görmezden gelemeyeceği bir sorun teşkil etmektedir. Bir devlet olarak, bu nitelikli verileri korumak için yeterli kaynak tahsis etmemek ve sorunun önemini göz ardı etmek kesinlikle ağ sistemlerindeki zayıflıkları doğuracak ve kaçınılmaz olarak ülke imajına zarar verecektir (Durankaya, Gökşen, & Eminağaoğlu, 2018).

Ancak günümüzde internet bankacılığı ve e-Devlet gibi kritik verilerin olduğu çevrimiçi sistemler yaygın olarak kullanılmaktadır. Bireyler şubelere gitmek yerine mevcut bankacılık işlemlerini uygulamalar veya tarayıcılar kullanarak çevrimiçi yapmaktadır. Mağazaya gitmek yerine kredi kartı ile çevrimiçi alışveriş yapabilmektedirler.

e-Devlet açısından da hizmetler ele alınacak olursa, vatandaşlar, sıra beklemeden sadece belirli bir zamanda e-Devlet ortamını kullanarak devlet hizmetlerinden kolayca yararlanabilmektedir.

Bunların da ötesinde, insanlar düşüncelerini dünyaya açıklayabilmekte ve sosyal medya yardımı ile milyonlarca kişiye ulaşabilmektedir. Ayrıca Mısır’da gerçekleşen Müslüman Kardeşler devriminin bir sosyal ağ kullanılarak örgütlendiği de unutulmamalıdır.

Tüm bu gelişmeler son on yılda insanın karşılaştığı devrimci yeniliklerdir. Ancak, tüm bu yenilikler günlük işleri kolaylaştırmanın yanı sıra çok önemli riskleri de içermektedir. İnternete bağlı cihaz sayısının artması, geniş bir yelpazedeki cihazların saldırılara maruz kalabileceği anlamına gelir ve aynı zamanda riskin büyüklüğünün ne kadar olduğunu gösterir. Bu bağlamda, güvenliğin ne kadar iyi ve kesin bir şekilde sağlanabileceği ile ilgili sorular ortaya çıkmaktadır. Algoritmalar, yöntemler ve cihazlar ne denli güvenilir olursa olsun, bilgi güvenliği varlıklarından birisi de insandır. Eğer bir birey bilgi güvenliği farkındalığını göz ardı ediyorsa, sistemde güvenliğin sağlanması imkânsız hale gelir. Bununla birlikte birçok araştırmacı bilgi güvenliği yapısının en zayıf halkasını insan olarak tanımlamaktadır. Örneğin kamu kurumlarının üretim ağıları için tüm üst düzey cihazların ve uygun yapılandırmaların sağlanmasına rağmen, idari personelin yanlış veya eksik bilgi birikimi işlemlerinin başarısızlıkla sonuçlanmasına neden olabilir. Bu nedenle bir bütün olarak ele alınması gereken bir konudur.

Bilgi güvenliği kavramının kullanılabilirlik, bütünlük ve gizlilik olmak üzere 3 temel ögesi mevcuttur. Bu ögeler aşağıdaki gibidir:

- **Kullanılabilirlik:** Bilgilerin veya kaynakların izinsiz olarak durdurulmasının önlenmesi anlamına gelmektedir. Bilgi, yetkili kullanıcılar için mümkün olduğunca serbest olmalıdır.
- **Bütünlük:** Bilginin hatalı olarak değiştirilmesinin önlenmesi basamağıdır. Yetkili kullanıcıların eksik bilgiler sonucunda yaptığı işlemler hataların oluşmasının ve verilerin değiştirilmesinin en büyük nedenidir. Yanlış veriyi sistem içinde saklamak veri kaybetmek kadar kötü olabilir.
- **Gizlilik:** Bilgilerin yetkisiz elde edilmesinin önlenmesi bu basamağın temel amacını oluşturmaktadır. Bu, güvenlik önlemlerinin düşük olmasının veya personel tarafından bilgi sızmasının bir sonucu olabilir. Zayıf güvenlik önlemlerine bir örnek, hassas bilgilere isimsiz erişim şeklinde olabilir.

1.1.5. Bilgi Toplumu

Son yıllarda, bilgi toplumu kavramı oldukça popüler hale gelmiştir. Bu kavram, bilgi ve iletişim teknolojilerinin (BİT) ve ilgili alanların gelişmeleri ile şekillenen yeni bir sosyal yapıyı ifade etmektedir. Günümüzde mevcut yapıyı ve yeni ekonomik-sosyal değişimleri açıklamak için teoriler geliştirilmiştir. Bu teoriler özellikle yeniçağ iletişim teknolojilerine odaklanmaktadır. Yeni teknolojileri mevcut kitle iletişim

teknolojilerinden farklı kılan ayırt edici özellikler bulunmaktadır. Bu özellikler, bilgilerin erişim, depolama, işleme ve dağıtım kapasitesini arttırmaktadır (Balay, 2004). Yeni iletişim teknolojilerinin, yeni ekonomik faaliyet alanlarının yaratılması ya da ilgili alanlarda iyileştirmeler yapılması konusundaki beklentileri ve özellikleri nedeniyle sosyal ve ekonomik değişimlerin itici gücü olarak görülmüştür. Bu yeni teknolojiler, iletişim teknolojilerinin sosyal, kültürel ve ekonomik etkileri üzerine geliştirilen farklı teorilerin oluşmasını tetiklemektedir. Bilgi toplumunun mevcut altyapıyı kullanan toplumlardan daha farklı olduğunu vurgulanmakta ve bilgi çağını diğer dönemlerden ayıran beş temel özelliğin bulunduğu savunulmaktadır. Bu öğeler;

- Bilgiye dayalı toplumun yükselişiyle bilgi çağı ortaya çıkar (Van Dijk, 2005).
- Bilgi teknolojilerine dayalı iş ortamı bilgi çağının getirdiği avantajlar arasındadır.
- İş süreçleri bilgi çağında verimlilik artışına dönüşür.
- Bilgi çağının başarısı, bilgi teknolojilerinin kullanımındaki verimlilik ile ölçülür.
- Bilgi çağında birçok ürün ve hizmet bilgi teknolojileri çevresinde iç içe geçmiştir.

Tarım, endüstri ve bilgi devrimi bazı çalışmalarda kronolojik olarak verilmiştir. Bu tür çalışmalarda bu devrimlerin tanımları şu şekilde yapılmaktadır. Tarım devriminin ekilebilir alanlara erişime bağlı olduğunu bilinirken endüstri devriminin temel amacı hammadde kaynaklarına ulaşp elde edilen mamül maddeleri satarak servet sahibi olmaktır. Bilgi devriminin ise ekonomideki bilgi ve iletişim verimliliğinin arttırılması amaçlı olduğu bilinmektedir. Bunların yanı sıra bilgi devriminin gücünü bilgi ve bilgidan aldığını savunulmaktadır (McLuhan, Powers, & Düzgören, 2001).

Bununla birlikte “endüstri sonrası toplum” ve “bilgiye dayalı endüstri sonrası toplum” terimleri geliştirilmiştir ve “bilgi toplumu” terimini sanayi sonrası topluma alternatif bir ifade olarak kullanılmıştır. Bilgilerin niteliğinin değiştirilmesinin sanayi toplumundan sanayi sonrası topluma geçişe neden olduğunu savunulmaktadır. Bununla beraber, bilginin sanayi sonrası toplumun stratejik kaynağı ve dönüştürücü unsuru haline geldiğini ve bu toplumun imalattan daha hizmetli bir ekonomiye geçişle tanımlanacağını savunulmaktadır. Ayrıca, ekonomik büyüme ve bilgi arasındaki ilişkiyi de incelenmiştir (Bell, 1972).

Bilgi toplumu toplumsal bir dönüşüm olarak tanımlamaktadır ve sanayi toplumundan tamamen farklı bir yapı olarak değerlendirilmektedir. Sanayi toplumunda fabrikaların modernleşme sembolü olduğunu ancak bilgi toplumunda bilgisayarın ve BİT'in modernleşme sembolü olacağını savunulmaktadır (Mauss, 2002).



İKİNCİ BÖLÜM

2. e-DEVLET GELİŞİMİ

Bu bölümde e-Devlet ile ilgili literatürde yapılmış çalışmalardan alınan genel tanımlar, e-Devletin tarihsel perspektifi ve e-Devlet uygulamalarında kullanılan bilgi güvenliği yöntemlerine temel bir bakış verilmiştir. Bu bölümde aktarılan veriler tezler, kitaplar, yayınlar ve internet sayfaları kullanılarak toplanmıştır.

2.1. e-Devlet

Dünya genelinde birçok yönetimin kamu sektöründe daha fazla verimlilik elde etmek için Bilgi ve İletişim Teknolojileri (BİT) kullanarak hizmet sağlama sistemlerinde reform yapması e-Devlet kavramını doğurmuştur (Vural & Bat, 2010). Ancak e-Devlet kavramı, devlet yetkililerine bilgisayar verme veya eski uygulamaları otomatikleştirme anlamına gelmemekte, kamu yönetimini modernize etme ve reform yapmayı hedeflemektedir. BİT kullanımı yoluyla devlet kurumları, işletmeler ve vatandaşlar arasındaki ilişkileri dönüştürmede e-Devlet hakkında pek çok tanım yapılmıştır.

e-Devlet, “yönetim alanında bir e-Ticaret şekli” olarak tanımlanmıştır ve elektronik hizmetleri vatandaşlara ve işletmelere sunma, kamu kurum ve kuruluşları ile işbirliği yapmak için gerekli süreçler ve yapılan işlemler şeklinde ifade edilmiştir. Kamu sektöründe yapılan bu büyük reformun öncelikli amaçları; verimliliği, rekabeti ve modernizasyonu artırmaktır (Backus, 2001).

“Kamu kurumlarının faaliyetlerini geliştirmek için bilgi ve iletişim tekniklerinin kullanılması” olarak tanımlanmıştır (Van der Molen & Wubbe, 2007).

e-Devlet, BİT açısından hükümet süreçlerini hızlandıracak bir uygulama olarak görülmüştür. Farklı devlet kurumları arasında içsel ilişkiler ve bağlantıların basit olabilmesi için kurum içi yönetim hiyerarşisinin ayrı tutulması gerektiğini savunulmuştur (Otubu, 2009).

e-Devlet, kamu kurumları ile bu kurumların hizmet ve bilgi sağlayıcıları ve bu hizmetlerden faydalananlar arasında BİT aracılığıyla kurulan ve sürdürülen ilişkiler süreci olarak tanımlanmaktadır ve bu hizmetleri 7/24 vatandaşların hizmetine sunmayı amaçlayan bir yapı olarak karşımıza çıkmaktadır (Yıldız, 2003).

e-Devlet devletin, vatandaşların, işletmelerin etkin ve verimli olmalarını sağlamada önemli bir rol oynayabilecekleri internet teknolojisine bağlı bir kavram olarak açıklanmıştır (Nawafleh, Obiedat, & Harfoushi, 2012).

e-Devlet, internet ve BİT aracılığıyla kurumlara, vatandaşlara bilgi ve hizmet sunumu olarak tanımlanmaktadır (AbuShanab ve El-Azzam, 2012)

e-Devletin, devlet kurumunun insanlarla bağlantı kurmasını ve geniş bir yelpazede farklı teknolojilerin etkin bir şekilde uygulanmasını sağlayan daha iyi hizmetler sunmayı amaçlayan bir olgu olduğu açıklanmaktadır (Kayrouz & Atala, 2014).

e-Devlet BİT araçlarını yaygın kullanan ve uygulayan, kullanıcılara daha etkin hizmet veren vatandaşları, işletmeleri ve diğer toplum kuruluşlarını da kapsayan bir kavram olarak tanımlanmaktadır aynı zamanda e-Devleti, BİT'nin bütünsel olarak kullanılması ve uygulanmasıyla ilgili olarak hükümet içindeki ilişkilerin ve ağların tüm yelpazesini ele alan daha geniş bir kavram olarak ifade etmişlerdir (Şahin, 2008).

e-Devlet uygulamalarının yaygınlaşmasının bir çok sebebi vardır. Bunlar şu şekilde açıklanabilmektedir. e-Devlet uygulamaları çok geniş bir alanda hizmet sunmaktadır. Bunun yanı sıra, kamu kurumlarının yönetiminin hantal ve verimsiz olması, bu kurumları vergileriyle finanse eden vatandaşların gözünde ciddi bir imaj kaybına sebep olmaktadır. Bu durum devlete ve kamu kurumlarına olan güveni doğrudan zedelemektedir. Çünkü Türkiye gibi devletlerde devlet yapısı aşırı büyüktür. Büyümüş ve hantallaşmış devlet yapıları meydana gelen ekonomik krizlerin en önemlisi sebebi gereksiz kamu harcamaları olarak ta görülmektedir. Bu tür problemlerin çözümü için BİT'in efektif olarak kullanılması gerekmektedir. BİT sayesinde efektif e-Devlet uygulamaları geliştirilmekte ve bu uygulamalar yaygınlaştırılmaktadır. Böylelikle zaman ve maliyet açısından yüksek tasarrufun sağlanması hedeflenir. e-Devlet uygulamalarının yaygın olarak kullanıldığı ülkelerde, bu amaca erişildiği gözlemlenmiş ve bu sebepten dolayı e-Devlet uygulamaları hızlı bir şekilde yaygınlaşmıştır. (Uçkan, 2003).

e-Devlet kavramının genel hatlarından bahsedilerek e-Devlet hizmetlerinin farkındalığının artırılması ve aksaklıklarının giderilmesi için;

- e-Devlet kavramının ve işlevlerinin farkındalığının artırılmasına yönelik kursların düzenlenmesi gerektiğini,

- Mevcut yapıdan e-Devlet yapısına geçmek için kâğıt üzerinde pek çok dokümanın bulunduğunu ve bunların elektronik ortama aktarılmasındaki zorlukların bulunduğu,
- Elektronik ortamda alt yapının oluşturulmasında teknik altyapının yetersizliği,
- Elektronik ortamlara olan güvensizliğin büyük oluşu
- Bu hizmetlerin bakımını ve onarımı sağlayacak insan faktörünün yetersiz oluşu
- Geleneksel altyapıya oluşan bağımlılık

şeklinde sıralanabilir (Abdelsatar, 2018).

Ülkeler arasında e-Devlete geçme süreçleri, farkındalıkları ve zorlukları kıyaslanacak olursa Şili ve Uruguay (Amerika), Tunus ve Moritus (Afrika), Singapur ve Bahreyn (Asya) karşılaştırılmıştır. Ülkeler arasında e-Devlete geçme arasındaki farklılıkların o ülkelerde yaşayan insanların sosyo-ekonomik ve eğitim düzeyi farklılıklarına dayandığı belirlenmiştir. Aynı zamanda etkili bir denetim ile bu sistemlerin etkin kullanılabileceği gösterilmiştir (Bojang, 2017).

Politika, iktidar, iletişim, kalite yetkinlik, kültür, altyapı gibi etkenler dikkate alınarak Türkiye’de 3 farklı kademede bulunan bireylerden veriler toplanarak bir değerlendirme yapılmıştır ve elde edilen sonuçlar aşağıda sıralanmıştır;

- İnsanların e-Hizmetler alanlarında yeterli bilgiye sahip olmadıkları,
- Kamu kurumlarının bu alanda bilgilendirme düzeylerinin yetersiz olduğu,
- İnsanların köklü alışkanlıklardan yeni sistemlere geçmede isteksiz oluşları.
- Teknik altyapıyı kullanma becerilerinin yetersizliği
- Teknik altyapı problemlerini çözme yetisine sahip insan gücünün azlığı

Yukarıda bahsedilen bu nedenlerden ötürü e-Hizmetler alanındaki mevcut yapıların kullanım oranlarının düşük olduğu tespit edilmiştir (Sancaktutar, 2013).

e-Devlet kavramı ve unsurları ayrıntılı bir şekilde incelenmiştir. Geleneksel devlet anlayışından e-Devlet anlayışına geçiş süreci ortaya konmuş ve farklılıkları vurgulanmıştır. Aynı zamanda Türkiye’deki e-Devlet uygulamaları ayrıntılı bir şekilde sunulmuştur. Türkiye’de e-Devlet uygulamasının tarihçesi, amaçları, özellikleri, kullanım alanları irdelenmiştir. e-Devlet yapısının aksatılmadan yürütülmesi için gerekli teknik alt yapının gereklerini ortaya koymuştur (Demirel, 2006).

e-Devlet kavramı ülkemizde yürütülen e-Devlet projelerinin Avrupa Birliği vizyonuna uygun olarak geliştirilmesi için temel adımları sunmuşlardır (Baştan & Gökbnar, 2004).

e-Devlet kavramının evrenselliğinden bahsederek gelişmekte olan ülkelerde e-Devlet kavramının sağlıklı bir şekilde yürütülmesi için çözüm önerileri sunulmuştur. Bu çözüm önerileri gelişmiş ülkelerde uygulamada olan e-Devlet hizmetlerinin sosyal etkileri, karşılaşılan zorluklar ve engeller baz alınarak oluşturulmuştur. Çalışmada belirlenen zorluklar ve engeller e-Hizmetlere olan güven eksikliği, finansal yetersizlik, güvenlik ihlallerinin çözümünde bulunan sorunların çokluğu, bütçe ve maliyet yapıları şeklinde sıralanmıştır (Ibraheem, 2017).

Burada; en önemli ortak faktör internet ve BİT kullanımıdır. Bu faktörler dikkate alındığında dünyada e-Ticaretin başarısı, ülkelere e-Devlet uygulamasını gerçekleştirme düşüncesine teşvik etmiştir (Metaxiotis & Psarras, 2004). e-Ticaret ile e-Devlet arasındaki fark, e-Devletin daha fazla müşteriye (vatandaşlar, işletmeler, çalışanlar ve hükümetin kendisi) hizmet sunması olarak görülmüş ve son yirmi yıldır, dünyanın dört bir yanındaki hükümetler e-Devlet projelerini hayata geçirmeye başlamışlardır. e-Devlete yönelik küresel dikkat, e-Devletin önemi ve çağdaş toplumların ilerlemesi ve büyümesindeki rolünün tanınması noktasında büyük bir hızla artmaktadır. e-Devletten bahsedildiğinde, tüm devlet işlemlerinin bir e-Devlet portalı üzerinden (tüm bilgilerin ve hizmetlerin çevrimiçi olarak sağlandığı büyük bir web sitesi) yapıldığı ve bir vatandaşın e-Uygulamalar ile tüm işlemleri tamamlayabildiği anlamına gelmektedir. e-Devlet projesi, dünyadaki her hükümet için en büyük öneme sahiptir, çünkü idari reformda, israfın azaltılmasında ve kamu sektöründeki iş verimliliğinin artırılmasının yanı sıra iyileştirilmesi sırasında elde etmek istenenlerin yürütme kolunu oluşturur (Al-adawi, Yousafzai, & Pallister, 2005). Farklı devlet sektörlerinin vatandaşlara, işletmelere ve hükümetin kendisine bilgi ve hizmetleri sağlama kabiliyeti olarak bilinen e-Devlet, BİT kullanarak hızlı ve güvenli bir şekilde internetteki tek bir site aracılığıyla herhangi bir zamanda titizlikle işlemleri yapma kapasitesi sağlar (Almarabeh & AbuAli, 2010; Ndou, 2004).

Ayrıca, e-Devlet sosyal olarak ele alınması gereken bir konudur. Bu hususta e-Devlet'in kullanımı ve sosyal hataya etkileri irdelenecek olursa; bilgisayar okur-yazarlığı, uzman istihdamı, gelir seviyesi, değişime direnç gösterme, kentli olup olmama, vatandaşın eğitim ve bilinç düzeyi, dijital bölünme, gizlilik ve mahremiyet,

gibi konular e-Devlet uygulamalarının kullanımını ve içselleştirilmesini doğrudan etkiler. e-Devlet uygulamalarını kullanarak azami sosyal etkiyi sağlayabilmek için yatırım yapılması gereken en önemli faktör eğitimidir. Eğitimle bilgisayar okur-yazarlığının arttırılması ve kalifiye iş gücünün yetiştirilmesi sayesinde, BİT kavramının içselleştirilmesi yönünde adımlar atılmalıdır (Şahin, 2008).

Modern dünyada, bilgisayar uygulamaları e-Devletin, iş dünyasının ve bireysel kullanımın her alanında kendine yer edinmiştir. Bilgisayarlı sistemler aracılığı ile devlette yer alan e-Hizmetler devlet kurumlarında oluşacak etkinliği ve verimliliği arttırmaktadır (Werhahn, Brown, Thompson, & Marsden, 1997). İnternet, etkinliği ve verimliliği nedeniyle e-Devlet dünyasında etkili olan bilgisayar uygulamalarından biridir. Etkin bir bilgisayar uygulaması kullanmaya duyulan ihtiyaç, gelişmiş hizmetler sağlama konusunda örgütlerin öncelikli kaygısı haline gelmiştir (Vassilakis, Lepouras, & Halatsis, 2007). Bu kaygının sonucu olarak, kuruluşlar hizmetlerini vatandaşlarının ihtiyaçlarına göre uyarlamak için öncelikler belirlemiştir (Wei & Zhao, 2005). İnternet sayesinde e-Devlet, hükümetlerin şeffaf ve insan odaklı önceliklere sahip hizmetler geliştirmeyi amaçladıkları büyük bir adım haline gelmiştir (Ong & Wang, 2009).

e-Devlet, kamu yönetimlerini geliştirme ve düzenlemede önemli bir araç olarak istikrarlı bir şekilde önem kazanmaktadır. Başlangıçta, e-Devletteki gelişmeler hem vatandaşlarda hem de hizmet sağlayıcılarda sürekli olarak değiştirebilecek bir araç olarak görülmüş ve olumlu tepkilere yol açmıştır. Birleşmiş Milletler'in (BM) yakın tarihli bir raporu, e-Devletin yönetim ve uygulama aracı olarak kullanıldığını belirten 193 ülkede kabul edildiğini ortaya koymaktadır (Unpan, 2014). e-Devlete gösterilen yoğun ilgiye rağmen, bazı çalışmalar teknolojik bir araç olarak e-Devletin potansiyelini yerine getirmediğini savunmuştur (Teo, Srivastava, & Jiang, 2008). Bir istatistikte, 2014 yılında, gelişmekte olan ülkelerdeki tüm e-Devlet girişimlerinin yalnızca yaklaşık %15'inin başarılı olduğunu göstermektedir (Heeks, 2003). BM'nin yakın tarihli bir başka anketi, 2015'te ankete katılan 193 ülkenin çoğunluğunun, e-Devlet gelişiminin düşük ve orta düzeyde kaldığını göstermektedir. Şekil 3.'de BM değerlendirme için dört aşamalı bir model önermiştir (Unpan, 2014).



Şekil 3. BM Önerdiği Model (Unpan, 2014)

Bu şekilde,

- Yeni teknolojiler: Çevirim içi uygulamalar
- Geliştirilmiş teknolojiler: e-Hizmetler, e-Araçlar
- İnsanlar arası ilişkiler: İnteraktif uygulamalar
- Bağlantılı teoriler: e-Devlet için geliştirilen teorilerin uygulamasını belirtmektedir.

e-Devlet portallarında işlemlerin güvenlik tehditlerinin artmasına bağlı olarak yeni ve mevcut teknolojik gelişmeler daha da zorlaşmaktadır. Bu problemin çözümüne yönelik birçok ülke (Avrupa Birliği ülkeleri) son zamanlarda, e-Devlet işlemlerini verimli, etkili ve tatmin edici hale getirmek için bulut bilişimi önemli bir teknolojik yenilik olarak sunmayı düşünmüşlerdir (Tweneboah-Koduah, Endicott-Popovsky, & Tsetse, 2014). Bulut bilişimin teknolojik bir faktör olarak kullanılması, e-Devlet güvenliği konusunda kullanıcı ile ilgili güvenlik hususları ve e-Devlet hizmet sağlayıcısının güvenlik tedbirleri açısından büyük bir etkiye sahip olduğu gözlenmiştir. Ayrıca, bağlamsal olarak bulut bilişim, mobil teknoloji, internet, sosyal medya ve Coğrafi Bilgi Sistemleri (CBS) gibi birçok teknolojik yenilik e-Devletin gelişimini önemli ölçüde etkilemiştir (UNPAN, 2014). Teknoloji alanında sürekli yenilikler yaşanırken, e-Devlet servis sağlayıcıları, e-Devlet hizmeti sağlamak için gereken teknolojik yönleri sürekli olarak yükseltmek zorunda kalmaktadır. Teknolojide meydana gelen ilerlemeler genellikle onlarla birlikte insanların e-Devlet portalı üzerinden işlem yapma şeklindeki değişiklikleri ve kullanıcıları nasıl etkilediklerini ve ne yapılması gerektiğini anlama zorunluluğunu da beraberinde getirmektedir. Teknolojideki değişiklikler, e-Devlet araştırmalarındaki bir parçasını oluşturmaktadır (Srivastava & Teo, 2005). Örneğin, bulut bilişim kullanan bir e-Devlet gelişimi bağlamında,

vatandaşlar e-Devlet portalı üzerinden iş yaparken bilgi güvenliği ile ilgili ciddi zorluklara maruz kalmaktadır. Günümüz teknolojisi ile insanlar masaüstü kişisel bilgisayarları kullandıkları teknolojiyen, bulut bilişim tabanlı uygulamalarla e-Devlet hizmetlerine erişmek için mobil cihazları kullanabilmektedirler. Böylece insanlar, insan-bilgisayar ara yüzü, teknolojinin kullanım kolaylığı, kullanışlılık, güvenlik, risk, gizlilik sorunları ve kalite konuları gibi yeni bağlamsal faktörlerle tanışmaktadır. Örneğin, Facebook ve Google haritaları, e-Devlet kurumlarının çevrimiçi depolama gibi özel bulut hizmetleri aracılığıyla benimsemiş oldukları iki mükemmel örnektir (IBM, 2015). Her ne kadar bulut bilişim hala erken gelişim aşamasında olsa da, pek çok ülke bu teknolojiyen faydalanmaya başlamışlardır (Tweneboah-Koduah et al., 2014; Unpan, 2014). Bulut bilişim, özellikle vatandaşların güvenlik ve mahremiyetinin e-Devlet ile geliştirilen web portallarında işlem yapabilme potansiyelinin düşük olmasından dolayı ortaya çıkmıştır. Değişen durumlarla karakterize edilen e-Devlet web portalı üzerinden işlem yaptıklarında, kullanıcı veri güvenliğinin ve gizliliğinin nasıl etkilendiğine dair bilgi eksikliği, kullanıcıların devletlere olan güvenini etkileyebilmektedir (Çelen, Çelik, & Seferoğlu, 2011).

Örgütsel bağlamda ise yeni teknolojilerin veya çalışma uygulamalarının tanıtılması, öncelikle proje ve program yönetimi, değişim, teknoloji transferi ve iş mühendisliği gibi disiplinler veya tekniklerle sağlanır. Bir e-Devlet uygulamasında, amaca göre bu tekniklerin bir kısmının uygulanması veya bunların pragmatik bir karışımı etkin bir web portalı oluşturmaktadır. e-Devlet kavramını dört kritik aşamada sınıflandırılmaktadır (Şahin & Örselli, 2003):

- Web ara yüzleri: Haber web siteleri e-Devlet süreçlerinin ve kurallarının şeffaflığı. Örneğin yeni modellerin farkındalığının sağlanması.
- Sınırlı etkileşimler: İntranet bağlantıları - vatandaşlar için zaman ve seyahat masraflarından tasarruf sağlanması. Örneğin kuralların, formların ve bilgilerin standartlaştırılması ve basitleştirilmesi.
- İşlemler: Hizmetlerin ve otomatik sistemlerin elektronik olarak sağlanması. Örneğin güçlü ağ altyapısı ve yüksek işlem gücüne sahip bilgisayarlı işlemler.
- Dönüşümler: Hizmetlerini e-Devlet üzerinden sağlayan ülkeler, örneğin devletin kurum portalları ve erişimin yaygınlaştırılması.

Dönüşüm aşaması uygulama basamağını içerdiği için devletler açısından düşünüldüğünde genellikle günümüzde yeni yeni uygulama alanı bulmakta ve gelişmekte olan ülkelerde yaygınlaşmaya başlamaktadır (Bhatnagar, 2004).

e-Devletin yararları sadece vatandaşlar için e-Hizmetler sunmak değildir. Aynı zamanda özel sektörler de (küçük, orta ve büyük firmalar), şirketlerin gelişimi ve değişimi için e-Devlet uygulamalarından yararlanabilir (Beynon-Davies & Williams, 2003). Kamu sektörünün çoğu zaman bürokratik, verimsiz ve düşük teknoloji uygulamalarından dolayı, e-Devlet, özellikle gelişmekte olan ülke bağlamında gerçekleşmeyi bekleyen bir devrim olarak kabul edilebilmektedir. Bu bağlamda, e-Devlet kamu sektöründe radikal bir şekilde değiştirme ve daha önce öngörülmemiş birçok fayda sunma potansiyeline sahip görünmektedir. e-Devlet başarıyla uygulandığında, devlet kurumları içindeki süreçlerde iyileşme olmasını, verimliliğin sağlanmasını ve kamu hizmetlerinin daha iyi yönetilmesini ve sunulmasını sağlayacaktır (Riley et al., 2003). Bununla birlikte, e-Devlet uygulamalarının yaygınlaştırılması ve başarılı olması için, etkin hale getirilecek süreçlerin oluşturulması ve öncelikle örnek stratejiler ve uygulamaların tanımlanması gerekmektedir. Ayrıca, her e-Devlet programı vatandaşlara önerilen faydalar hakkında net bir fikir sahibi olmalı, hangi zorlukların aşılması gerektiği ve belirli bir bağlamda başarılı olabilmesi için yapılması gereken kurumsal değişimin seviyesi hakkında bilgi sahibi olmalıdır (Hazlett & Hill, 2003). Birçok gelişmiş ülke başarılı stratejiler belirleyerek e-Devlet kavramına öncülük etmenin önündeki engelleri aşmaktadır (Irani, Love, & Jones, 2008).

e-Devleti kullanmanın bazı avantajları aşağıda maddeler halinde verilmiştir (Evans & Yen, 2006; Lee, Kim, & Ahn, 2011):

- Elektronik kamu hizmetlerine 7 gün 24 saat erişim sağlamak
- Toplumdaki her vatandaşa hükümetten aynı türde bilgi ve hizmetler sunulmasını sağlamak
- Vatandaşlara kişiselleştirilmiş hizmetler sağlayarak müşteri ilişkilerini yeniden kurmak
- Maliyet tasarrufu
- Ekonomik kalkınmanın teşvik edilmesi ve yerel işletmelerin küresel olarak genişlemelerine yardımcı olmak
- Kullanım kolaylığı

- Çevrimiçi tartışma, oylama ve bilgi alışverişini teşvik ederek daha katılımcı bir hükümet şekli oluşturmak
- Müşteri hizmetleri düzeyinde gelişim
- Daha iyi verimlilik sağlamak için merkezi karar verme
- Yüksek maliyeti düşürme
- Verimlilik kazancı
- Vatandaşlara sunulan hizmet kalitesi
- Şeffaflık
- Yolsuzlukla mücadele
- Bireylerin etkin çalışma kapasitesini artırma
- Ortak platformlar için ağ oluşturma
- Karar verme kalitesini iyileştirme
- Bilgi teknolojileri (BT)' nin toplumun diğer sektörlerinde kullanılmasını teşvik etme.

Bununla birlikte, e-Devlet hizmetlerinin sağlanmasını desteklemek için gerekli olan uygulamalar, vatandaşlar tarafından teknik alt yapının yetersizliği, bilgisayar ve internet kullanımındaki eksiklik, e-Hizmetlere olan güvensizlik gibi nedenlerden dolayı eşit olarak kullanılmamaktadır. Bu alt yapıya sahip olmayan uygulamaların yaygın kullanımı mümkün olmamaktadır. Ayrıca, e-Devletin uygulanmasındaki zorlukların kullanıcıları uygun BİT altyapısının eksikliği, güvenlik, mahremiyet, siyasi ve kültürel engeller, e-Devlet portallarının tasarımı ile ilgili konular, örgütsel konular, yasal sorunlar açısından etkilediği de görülmektedir (Haider, Shuwen, & Burdey, 2016). e-Devlet işlemlerinin gerçekleştirilmesinde özellikle portal üzerinden işlem yaparken ortaya çıkabilecek riskler nedeniyle güvenlik ve mahremiyet gibi hususların ele alınması gerekmektedir. Bu hususlar, vatandaş merkezli yaklaşımların araştırmacılar tarafından önemli zorluklar olarak görülmesine sebep olmuştur. Bu nedenle, e-Devlet hizmetlerinin vatandaşlara sunulan hizmetleri iyileştirirken aynı zamanda bilgi güvenliğini sağladığını göstermelidir (Alshehri, Drew, & Alfarraj, 2012; Burn & Robins, 2003). Mevcut yapıda oluşabilecek boşlukları tespit etmek ve güvenli, tatmin edici e-Devlet hizmetlerinin vatandaşlara sunulmasını sağlamanın yollarını bulmak için bu faktörlerin incelenmesi zorunludur (Curran, Carlin, & Adams, 2012; Duffany, 2012; Gharehchopogh & Hashemi, 2012; Heeks, 2003; IBM, 2015; Shareef, Kumar, Kumar,

& Dwivedi, 2009; Wyld, 2010) . Bu faktörler hakkında vatandaşların ve araştırmacıların e-Devlet hizmeti ile ilgili güvenlik ve uyumluluk konularını anlamak için bir temel oluşturması beklenmektedir. Bununla birlikte, vatandaşlar tarafından istenilen çevrimiçi güvenliğin öznel veya nesnel olabileceği belirtilmektedir (Shah, Peikari, & Yasin, 2014). Çevrimiçi güvenlik öncüllerini öznel bakış açısından incelemek önemlidir, çünkü güvenlik öncülleri öznel ve objektif bakış açısından farklıdır. Bireylerin çevrimiçi güvenlik algılarını etkileyen çeşitli faktörlerin, kendi aralarında yetersiz olduğu ve bilgi eksikliğinin olduğu durumlarda e-Devlet hizmetlerinin sağlanması ciddi bir şekilde engellenmektedir. Bu durumda, e-Devlet kullanıcılarının çevrimiçi güvenliklerini etkileyen durumlar için çözüm stratejilerine ihtiyaçları vardır.

e-Devlet uygulamasının önündeki engeller aşağıdaki şekilde sıralanabilir:

- Teknoloji veya web personeli eksikliği
- Mali kaynak eksikliği
- Farkındalık eksikliği
- e-Devlet web sitelerinin kullanılabilirliği
- BİT altyapısı: e-Hazırlık, bilgisayar okuryazarlığı, telekomünikasyon ekipmanları
- Güvenlik eksikliği ve endişeleri
- Mevcut BT'yi yükseltme ihtiyaçları
- Değişime direnç
- Siyasi sorunlar
- Hükümet desteğinin eksikliği
- Mevzuat
- İnsan sermayesi gelişimi ve yaşam boyu öğrenme: Beceriler, yetenekler, eğitim ve öğrenme
- Değişim yönetimi: Kültür, değişime direnç
- Veri koruma kanunları yetersizliği
- İşbirliği ve ortaklık: Kamu ve özel topluluk
- Strateji: Vizyon ve misyon
- Liderlik

2.2. e-Devletin Tarihsel Perspektifi

İçinde yaşadığımız çağ bilgi çağı olarak adlandırılmaktadır. BİT ve devlet kavramları tarihsel olarak değerlendirilecek olunursa, e-Devlet kavramının bu çağda meydana çıkması ve yaygınlaşması tarihsel bir zorunluluk olarak yorumlanmaktadır. Bunun yanı sıra devlet klasik ve modern süreçlerin birleşiminden oluşan bir kurallar ve kurumlar bütünü olarak tanımlanmıştır (Delibaş ve Yiğit, 2005). Bu tanıma göre e-Devletin tarihsel perspektifinin ortaya konması gerekmektedir.

e-Devletin ortaya çıkışı, teknolojiye uymanın ve mevcut performansın geliştirilmesinin bir sonucudur. e-Devlet kavramı çoğu gelişmekte olan ülkede oldukça yeni uygulama alanı bulmaktadır. Bu bağlamda, teknolojik uygulamalar ve kamu yönetiminin temel özelliklerini birleştiren iki kutuplu bir platformdur. Bu amaç doğrultusunda e-Devlet uygulamaları müşteri hizmetleri, ön işlemler ve arka plan uygulamaları üzerinde yoğunlaşmaktadır (Zürcher & Gönen, 1999). e-Devlet ilk olarak gelişmiş ülkelerde ortaya çıkmıştır. Sayısal çağın başlangıcında rol oynayan ve teknolojinin efektif olarak kullanıldığı ülkelerde e-Devletin ilk uygulamalarıyla karşılaşmaktadır. ABD’de e-Devletin ortaya çıkışı, devletin vatandaşlarla etkileşime gireceği elektronik bir çerçeveye ihtiyaç duyulduğunda başlamıştır. Genel protokoller ve merkezi erişim amacıyla, büyük ölçüde sunucu tabanlı arka plan uygulamaları ile çalışma alanı bulmuştur. Böylece e-Devlet fikri, hükümeti yeniden şekillendirmek amacıyla (devlet hizmeti sunumunu arttırmak için bilgi teknolojisinin kullanılması) yaygın kabul görmüştür. Bu durum, federal linkler portalı “FirstGov”’un kurulmasına yol açmıştır. Proje ve yöntemler, e-Devletin başarılı bir şekilde benimsenmesinin anahtarı haline gelmiştir. Hükümet reformu olarak adlandırılan “FirstGov”, bilgi sağlamak için e-Devletin alt düzeyiyle sınırlı bir bağlantı sayfası haline gelmiştir. Sonrasında hükümet reformlarının 'modernizasyonu' kapsamında, Bush yönetimi İcra dairesi Yönetim ve Bütçe Bürosu kurulmuştur ve bu gelişme ile pek çok e-Hizmet uygulaması farklı platformlarda yayınlanmıştır (Firstgov, 2018).

ABD’nin ardından diğer bir gelişmiş ülke İngiltere e-Devlet kavramını tam anlamıyla kullanan ülkelerin ilklerinden birisidir. 2004’de İngiltere’deki mevcut devlet teknolojisinde değişiklik e-Devlet fikri ile oluşturulmuştur. ABD'nin aksine, ilk reform patlaması, e-Ticaretin aksine teknolojinin devlet uygulamalarına odaklanmıştır. Çünkü küreselleşen Dünya’ da malların sınırların ötesine geçebilmesi için e-Ticaret portallarına ihtiyaç vardı ve e-Ticaret e-Devlet’e göre daha eski ve daha köklü bir sistemdir. e-

Hizmetler ofisi, standartlar için bir koordinatör olarak hareket etmiştir. Başlıca dönüm noktası, 2000 yılında Bakanlar Kurulu ofisi tarafından yayınlanan ilk modernizasyon hükümet belgesi ve e-Devlet stratejisidir. Hükümet ve elektronik hizmetlerin ilkeleri, hizmet sunumunda önemli değişikliğe yol açmıştır ve ticarileşmeye başlamıştır. ‘.com’ uygulamaları tüm hizmetlerin 2008 yılına kadar çevrimiçi olacağını belirlemiştir (Kızıldağ, 2011).

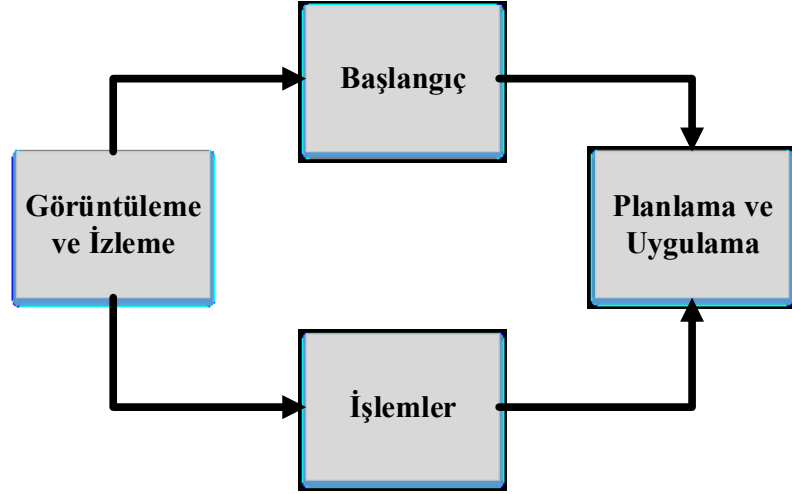
ABD ve İngiltere’nin e-Devlet platformuna geçişinin tamamlanmasından sonra diğer ülkeler hızlı bir şekilde hizmetlerini elektronik ortama taşımışlardır. Özellikle internetin yoğun olarak kullanıldığı Filipinler, Malezya, Singapur ve Hindistan gibi uzak doğu ülkelerinde e-Devlet adaptasyonu gelişmiş ülkelere nazaran daha hızlı bir şekilde gerçekleşmiştir.

Gelişen teknoloji ve internet ağı sayesinde Dünya küçük bir yer haline dönmüştür. Teknolojik gelişmeler sayesinde “yeni dünya düzeni” olarak tanımlanan ve bilginin ışık hızıyla iletildiği bir çağ ortaya çıkmıştır. Türkiye gibi gelişmekte olan devletler bir türlü sanayi devrimini tamamlayamamışken, bilgi çağı ve internet devrimiyle karşı karşıya kalmışlardır. Bu çağ yeni, gelişmekte olan ülkeler için yeni fırsatların habercisi olarak da görülmektedir. Bilgi çağının devlet teoremini en çok etkileyen ürünlerinden birisi de e-Devlettir. e-Devlet büyüyen verinin doğru yönetilmesi, israfın önüne geçilebilmesi ve devlet yapısının hantallıktan dinamik hale dönüştürülebilmesi için büyük bir fırsat aynı zamanda tüm devletler için bir zorunluluktur (Kuran, 2005).

“e-Dönüşüm Türkiye Projesi”ni hayata geçirebilmek için devlet planlama teşkilatında (DPT) çalışmalar yapılmış ve bu çalışmaların bir süreç olarak hayata geçirilmesi ve takibinin sağlıklı bir biçimde gerçekleştirilmesi için Bilgi Toplumu Daire Başkanlığı adında bir birim meydana getirilmiştir. Projenin başarılı olması için ekonomik ve siyasi destekler aranmış ve devlet tarafından bu proje fonlanmıştır. Ayrıca, tüm kurumların ana portalları bu proje kapsamında değiştirilmiş, elektronik belge yönetim sistemi ne geçiş hızlandırılmıştır (Yıldırım vd., 2003).

2.3. e- Devletin Yaşam Döngüsü

e-Devletin yaşam döngüsü 4 aşamadan oluşmaktadır. Bunlar başlangıç, planlama ve uygulama, işlemler ve görüntülemedir. Bu yaşam döngüsü ve birbirleri ile ilişkileri Şekil 4.’de verilmiştir.



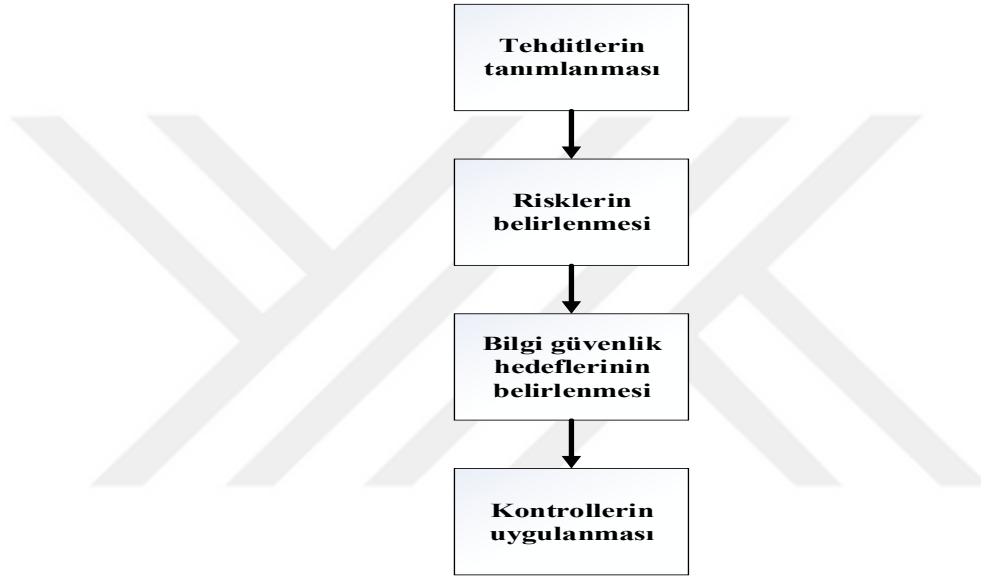
Şekil 4. e-Devletin yaşam döngüsü (Razzaqi, 2013)

Bu yaşam döngüleri aşağıdaki şekilde açıklanabilir (Razzaqi, 2013).

- 1- **Başlangıç:** Hükümetlerin hizmet dönüşümü için amaçlarını ve vizyonlarını açıkça belirttiği e-Devlet proje yaşam döngüsünün ilk aşamasıdır. Dönüşüm, yaşam döngüsü sürecinin nihai sonucudur. Başlama ise hükümetin bu yolculuğa çıkma aşamasında bir fikir olarak açıklanmaktadır. Diğer aşamaların büyük ölçüde ilk aşamada yer alan açıklığa ve gerçekçiliğe bağlı olması nedeniyle en hayati aşama olarak tanımlanmaktadır.
- 2- **Planlama ve Uygulama:** Başarıya katkıda bulunan en önemli iki faktör insan ve finansal kaynaklardır. Değişim yönetimi ise bir diğer önemli konudur ve belirtilen hizmetleri sağlamak için uygulamaların uygun şekilde oluşturulması gereklidir. Bilgi paylaşımı e-Devlet'in temel amaçlarından biridir. Bu aşamadaki temel konulardan bazıları, koordinasyon, teknoloji, kullanıcı dostu olma, kullanılabilirlik, ölçeklenebilirlik, hizmetlerin çeşitliliği şeklinde sıralanabilir.
- 3- **İşlemler:** Güvenilir günlük işlemler ve hizmet dönüşümü sağlamak için sistemlerin aşamalı entegrasyonu bu aşamanın temel amaçlarını oluşturmaktadır.
- 4- **Görüntüleme ve İzleme:** Görüntüleme ve izleme, hizmetlerin optimizasyonu ile ilgilidir; ancak e-Devlet projelerinin yaygın kullanımı uzun zaman alabilir. İşlemlerin gerçekleştirilmesi için günlük kullanıcıların izlenmesini gerekir. Bu aşamadaki en önemli kaygılar hizmetleri oluşturmak, müşteri geri bildirimlerini almak ve çözmektir.

2.4. e-Devlet Uygulamalarında Bilgi Güvenliği

e-Dönüşümle birlikte devletler ve bireyler için önemli olan veriler elektronik ortama aktarılmıştır. İnternet bağlantısının yaygın olarak kullanılması, kötücül yazılımların yaygınlaşması, çıkarılabilir disklerin birden fazla bilgisayara takılması ve hackerlik kültürünün yaygınlaşması elektronik ortamı güvensiz bir hale getirmiştir. Kritik bilgilerin güvenliğinin sağlanması için bilgi güvenliği adı altında bir çalışma alanı ortaya çıkmıştır. Bilgi güvenliği aslında insanlık tarihi kadar eski bir bilim dalıdır. Bilgi güvenlik yönetim sistemleri süreçlerinin genel blok diyagramı Şekil 5.' de verilmiştir.



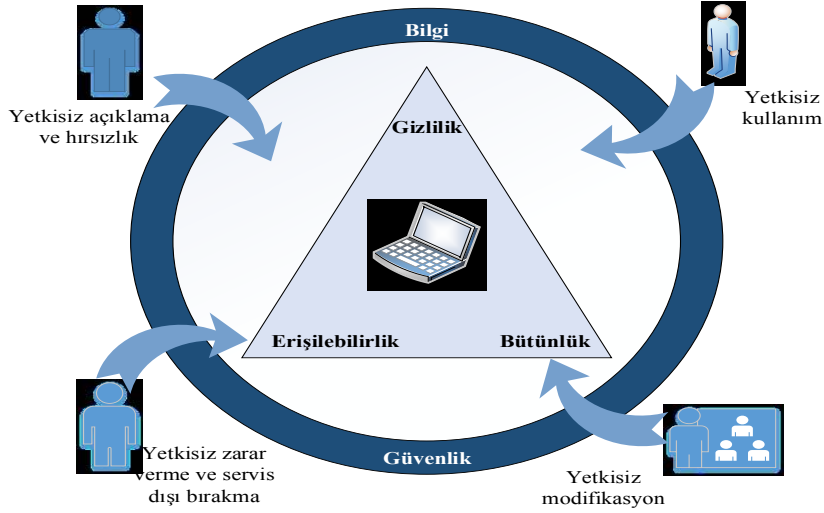
Şekil 5. Bilgi Güvenlik Yönetim Sistemi Süreci (Lum et al., 2016).

Bu çalışma alanının popülaritesinin en üst düzeye vardığı zaman dilimi ise 2. Dünya Savaşı olmuştur. 2. Dünya Savaşında Almanya Enigma adı verilen bir şifreleme cihazını kullanarak telgraf ve telsiz iletişimlerinin dinlenmemesini sağlamıştır. Bu şifreleme cihazını analiz edebilmek ve şifreleri kırabilmek için İngiltere, Alan Turing başkanlığında bir ekibi görevlendirmiş ve şifreleri kırabilmek için Turing makinesi adında bir cihaz geliştirmiştir. Bu cihaz günümüzün en sık kullanan aracı olan bilgisayarın atasıdır. Enigma simetrik bir şifreleme cihazıdır ve 160 bite kadar anahtar boyutunu destekler. Karıştırma işlemi sağlamak için 3 adet silindir kullanır ve modern şifrelemenin başlamasına neden olan cihazdır. Enigma Şekil 6' da gösterilmiştir (Lum et al., 2016).



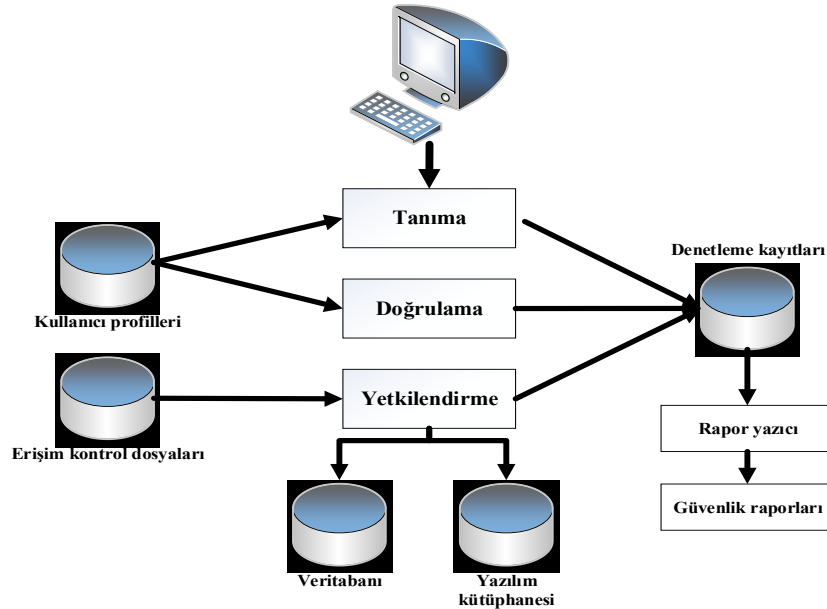
Şekil 6. Enigma Makinesi (Welchman, 1982)

2. Dünya savaşının ardından modern bilgisayarlar icat edilmiştir. Bilgisayarların evlere girmesiyle birlikte internet kullanımı da yaygınlaşmıştır ve günümüzde en yaygın kullanılan iletişim aracı internet olmuştur. İnternetin en önemli problemi ise güvenilir olmamasıdır. Güvenliği sağlayabilmek için modern simetrik şifreleme algoritmaları, asimetrik şifreleme yöntemleri, özet fonksiyonları, kriptolojik protokoller ve son zamanlarda özellikle de kripto parayla adını duyuran blok zinciri protokolleridir. Tüm bu bilgi güvenliği sistemlerin temel olarak sağlamak istediği üç temel unsur vardır. Bunlar gizlilik, bütünlük ve erişilebilirliktir. Gizliliği sağlayan temel bileşen simetrik şifreleme sistemleridir. Erişilebilirlik ise yetkisiz erişimlerin yasaklanmasını sağlar ve bunun için genel olarak elektronik imza yapıları kullanılmaktadır. Bu yapılar e-Devlet uygulamalarının kimlik doğrulamasında da kullanılmaktadır ve en güvenilir yapılar olarak bilinmektedir. Bütünlük ise kriptolojik özet fonksiyonları kullanılarak sağlanmaktadır. Kriptolojik özet fonksiyonlarının uyuşması, belgenin zarar görmediği ve değiştirilmediği anlamına gelmektedir. Şekil 7.'de bilgi güvenliği gereksinimler grafiksel olarak gösterilmiştir.



Şekil 7. Bilgi Güvenlik Sisteminde Risk Faktörleri (Access Control Security Features, 2019)

Güvenilir soket katmanı (GSK) kullanılarak gizlilik ve bütünlük sağlanmaktadır. Çünkü GSK kullanılarak çevrimiçi ticaret yapısı sağlanmaktadır. Bu yapı e-Devlet uygulamalarında da kullanılmaktadır. Ancak e-Devlet uygulamalarını erişim kontrolü özel olarak yapılmalıdır. Çünkü bu tür uygulamalarda erişim hiyerarşisi sistemin temelini oluşturmaktadır. Erişim hiyerarşisiyle ilgili görsel Şekil 8.'de verilmiştir.



Şekil 8. Erişim Kontrolü Blok Diyagramı (Devopedia, 2019)

Şekil 8.'den görüldüğü gibi, kullanıcı profilleri tanınır ve bu profillerin yetkileri etiketlenir. Erişim kontrol dosyalarına yetkilendirme bloklarıyla ulaşılır. Veri tabanı ve yazılım kütüphanelerinden denetimler yapılır.

2.4.1. e-Devlet Güvenliği

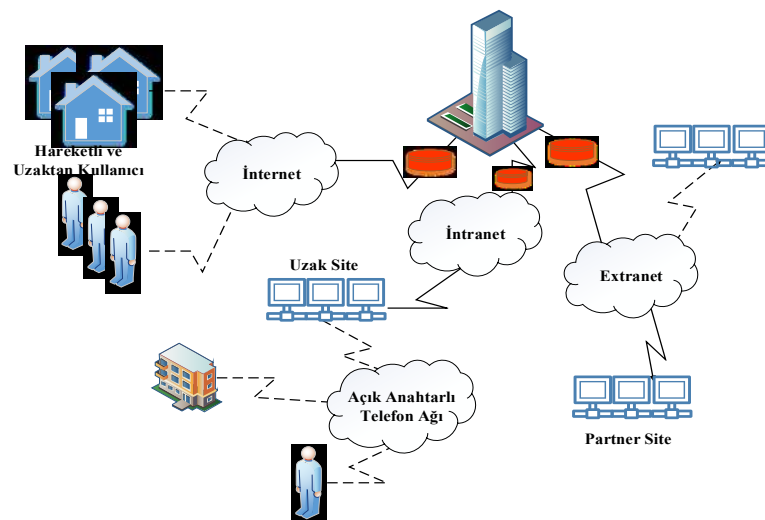
Günümüzde e-Devlet güvenliği, kullanıcılar, servis sağlayıcılar ve araştırmacılar için önemli bir çalışma konusudur. e-Devlet güvenliği, literatürde birçok kişi için bir zorluk olarak kabul edilmiştir (Alshehri et al., 2012; Irvine, 2000; Joshi, Ghafoor, Aref, & Spafford, 2001; Lim, Grönlund, & Andersson, 2015; Milner, 2002; Stephen H, Norris, & Fletcher, 2003). Kullanıcı merkezli bir sorun olan e-Devlet güvenliği, uygulamalar üzerinde işlem yapan kullanıcılar için önemli bir kaygı sebebidir. Bu durumun uygulamalardaki kullanıcı potansiyelini azaltıcı bir etkiye sahip olduğu düşünülmektedir. e-Devlet güvenliğinden kaynaklanan problemlerin kullanıcılarda olumsuz etkiye sahip olduğu ve güvenlik meselesinin e-Devlet gelişimine sekte vuran önemli etkenler arasında yer aldığı gözlenmektedir. Bununla beraber, bir diğer araştırma kaynağında değişen teknoloji, coğrafya, demografi ve kültür gibi bağlamsal konuların, e-Devletin genel politikasının kabul görmesine yol açtığı ancak güvenlik ve gizlilik konularının e-Devlet kullanıcılarını olumsuz etkilediği gösterilmiştir (Gaule & Zilinskas, 2013). Aynı zamanda, değişen koşullar ve teknoloji, demografik senaryolar, kullanıcıların e-Devlet hizmetlerini kullanma becerisi ve kültür gibi sosyal bağlamlardaki değişimlerin dünyanın farklı yerlerindeki uygulamalar için farklı etkilere sahip olduğu gösterilmiştir. Bu nedenle, e-Devlet ile ilgili kullanıcı merkezli zorlukların e-Devlet kullanıcılarını nasıl etkileyebileceği bölgesel ve kültürel farklılıklara göre ele alınmalıdır (European Commission, 2013). Bağlamsal faktörlerle ilgili olan çeşitli zorluklar arasında, kullanıcıların e-Devlet güvenlik kaygıları, birçok araştırmacı tarafından, e-Devlet aracılığıyla işlem yapan vatandaşların ele alınması gereken temel sorunlardan biri olarak tanımlanmıştır (Alshehri et al., 2012). Bu nedenle, e-Devletin, kullanıcıların güvenlik ve gizlilik kaygıları ele alınmadığı takdirde vatandaşlar arasında olumsuz etkiye neden olacağı savunulmaktadır.

Bulunan çalışmaların çoğu, güvenlik kavramını teknoloji ve mühendislik perspektifinden ele almışlardır (Alrashedi, Persaud, & Kindra, 2015). Bununla beraber kullanıcı merkezli e-Devlet hizmet güvenliği açısından, kullanıcıların ve hizmet sağlayıcıların büyük bir endişesi olduğuna dikkat çeken araştırmalar ile de

karşılaşılmaktadır. Ayrıca, e-Devlet alanındaki kullanıcı merkezli e-Güvenlik araştırmalarının, e-Ticaret bağlamında yapılan bazı araştırma örnekleri olmasına rağmen, ihmal edilen bir alan olduğu görülmüştür (Shah et al., 2014). Ancak e-Devletin kabul görmesi için güvenliğinin göz ardı edilememesi önemli bir unsur haline gelmiştir (Shareef, Kumar, Kumar, & Dwivedi, 2011). Web sitesi uygulamalarının başarısında ve çevrimiçi kullanıcı memnuniyetinde güvenlik faktörlerinin etkisini açıkça (Van Greunen, Herselman, & Van Niekerk, 2010) göstermektedir (Chang & Chen, 2009; G. Lee & Lin, 2005; Ribbink, Van Riel, Liljander, & Streukens, 2004). Dünyanın dört bir yanında bulunan ülkelerin vatandaşları e-Hizmet uygulamalarına katılım konusundaki ana aracın güven olduğunu söylemişlerdir (Botterman, Schindler, & Van Dijk, 2010).

e-Devlet hizmetleri vatandaşlara kişiselleştirilmiş hizmetler sunmayı amaçlamaktadır (Botterman, Schindler, & Van Dijk, 2010). Bununla beraber, teknolojik gelişmeler mobil uygulamaların da artmasına sebep olmaktadır. Böylelikle hemen hemen her insanda bulunan akıllı telefonlar aracılığı ile elektronik işlemlere ulaşma potansiyeli artmaktadır. Devlet tarafından geliştirilen mobil uygulamalar ve çok amaçlı hizmet sağlayan platformlar, kullanıcı ihtiyaçlarını karşılamada önemli bir rol oynayacaktır (Dawes, 2009).

Özet olarak günümüzde en sık kullanılan iletişim internettir. İnternet herkese açık bir ağ olduğu için güvenlik önlemlerinin üst düzeyde tutulması gerekmektedir. Açık ağlarda kullanılan güvenlik önlemlerinin blok diyagramı aşağıdaki Şekil 9.'da verilmiştir.



Şekil 9. Günümüz Ağları ve Güvenlik Önlemleri (Dawes, 2009).

2.4.2. e-Devlet Güvenliğini Etkileyen Teorilerin Sentezi

e-Devlet kullanımı, çevrimiçi etkileşim ve internet ile ilgili güvenlik hususlarını açıklamak için bazı teoriler önerilmiştir. Bu tür teorilerin uygulanması, teknolojik ve yönetsel açıdan 2 şekilde sınıflandırılabilir (Shah et al., 2014). Bu sınıflandırmaların odağında teknoloji ve yönetimin birleşimi gelmektedir. Bununla birlikte, teorik odaklanma, e-Devlet hizmetlerine yöneliktir. Hizmet öncelikli sistemlerde teknoloji bir araç olarak kullanılmaktadır. Özellikle araştırmaların odağı, fayda sağlayan kullanıcılar ve verilen hizmetlerdir. e-Devlet araştırmalarında geniş ilgi gören alanlardan biri, teknolojinin kullanıcı tarafından kabul edilmesi ve e-Devlet kabulüne yönelik kullanıcı davranışını açıklamak için bir dizi teori ve model geliştirilmiştir. Bunlardan bazıları aşağıda verilmiştir.

- **Roger'ın İnovasyon Yayılımı ve Türevleri:** Bilgi teknolojisi uygulandığında kullanıcı davranışı üzerindeki etkisi ve teknolojik özelliklerin kullanıcı algısı ile ilgilenir.
- **Teknoloji Kabul Modeli:** Bireyler alışkanlıklarından kolayca vazgeçememektedirler ve yeni teknolojilere adapte olabilmek için bir oryantasyon sürecine ihtiyaç duymaktadırlar. Teknoloji Kabul Modeli (TKM) bilgi sistemlerindeki yeni teknolojileri kabul etmek ve benimsemek için kullanıcı eğilimlerinin (kişisel inançlar ve tutumlar) oluşumunu açıklayan bir modeldir. 3 farklı şekilde geliştirilen bu model bir toplumun ve toplumdaki bireylerin yeni bir teknolojiyi kabul etme sürecini açıklamaya çalışmaktadır (Taylor & Todd, 1995).
- **Uygulama-Teknoloji Modeli:** Bu modele göre 'uygulama-teknoloji uyumunun bilgi sisteminin kullanımını etkilemesi beklenir ve bu uyum teknoloji temellidir' ilkesini savunmaktadır (Goodhue & Thompson, 1995).
- **Birleşik Kabul Teorisi:** Bu model uygulama-teknoloji modeli, teknoloji kabul modeli gibi farklı modellerin bir kombinasyonu olarak oluşturulmuştur. Bir teknolojiyi yüksek bir yüzdede benimseme ve kullanma niyetindeki varyansı açıklayan en kapsamlı model olduğu iddia edilmektedir (Venkatesh, Morris, Davis, & Davis, 2003).
- **Sosyo-Teknik Teorisi:** Bir örgütün teknik bir alt sistem ile sosyal alt sistemden oluştuğunu ve ikisinin arasında bir uyum olması gerektiğini savunan sosyo-teknik teorisi; sistemlerin başarılı olması için sistemin teknik,

organizasyonel ve sosyal yönlerinin paralel olarak yapılandırılmasına bağlı olduğunu anlatmaktadır (Bostrom & Heinen, 1977). Sosyo-teknik teorisinin, sosyal ağ gibi teknolojik yeniliklere yönelik kullanıcı davranışını açıklamak gerektiğini vurgulamaktadır. Teknoloji kabul modeli gibi diğer modelleri birleştirerek geliştirilmemiştir (Shipps, 2013). Dolayısıyla, bu teori, e-Devlet kullanıcılarının davranışlarını açıklamak için kapsamlı bir teori olarak kullanılabilir.

- **İnsan Bilgisayar Etkileşimi:** Günümüzde birçok problem bilgisayarlar ve bilişim teknolojileri kullanılarak çözülmektedir. Bu durum İnsan Bilgisayar Etkileşimi'ni (İBE) önemli bir konu haline getirmiştir. İBE psikoloji, bilgisayar bilimi, bilişsel psikoloji, mühendislik, yapay zekâ ve diğer disiplinler ile bağlantılı olduğu için bu konuda kesin bir teori olarak geliştirilmemiştir çünkü her bilim dalı İBE'yi kendi penceresinden ele almaktadır (Carroll & Campbell, 1989). İBE tasarımı için önemli olan psikoloji ve bilgisayar bilimi arasındaki ilişkidir ve İBE tasarım aşamasında çoğunlukla bilgi teorisi ve bilgi alışverişinde bulunduğunu savunmuşlardır. Bilgi alışverişi matematik kullanılarak tanımlanır. Böyle bir durum, İBE topluluğunu ekonomik ve davranışsal modellere odaklanmaya zorlamıştır. İBE, güvenilirliğini ve geçerliliğini değerlendirmek ve oluşturmak için ampirik çalışmalara ihtiyaç duyar.

Bu teoriler ve modeller e-Devlet hizmetlerinin kullanıcılarını nasıl etkilediğini ve e-Devlet güvenliğine olan inançlarını anlamak için bir takım teorilerin kullanılabileceğini açıkça belirtmektedir. Bu teoriler ile ele alınan bağlamsal faktörler arasında güvenlik, gizlilik, hizmet kalitesi, kullanım kolaylığı (Papadomichelaki & Mentzas, 2012), teknolojiye karşı tutum, teknolojik faktörler, kullanışlılık, vatandaş merkezilik ve insan bilgisayar etkileşimi gelmektedir (Gulliksen, 2014).

Günümüzde yeni mobil uygulamaların, yeni platformların (tablet, akıllı telefon, cep bilgisayarları) ve sosyal medyanın ortaya çıkmasıyla, değişen teknolojilerden kaynaklanan kullanıcı sorunlarını gidermek için mevcut teorilerin uygulanıp uygulanmayacağına dair artan bir endişe mevcuttur. Aynı argüman, mevcut teoriler tarafından açıklandığı ve ampirik araştırmalarla kanıtlandığı sürece, diğer teorilere, kavramsallaştırmalara ve geliştirmelere

uygulanabilir. Teknolojideki her bağlam ve değişim, e-Devlet kullanıcılarının nasıl etkilendiğini ortaya koymak için incelenmesi gereken önemli faktördür.

2.4.3. e-Devlete Politik Bağlılık ve Halkın Güveni

BM'in 2030 Sürdürülebilir Kalkınma Gündemi (SKG) başlıklı çalışması ülkelerin e-Devlet aktarımındaki sürekliliğinin sağlanması için pek çok araştırma ve yönlendirmeyi içermektedir. Kurumlar, SKG'ye destek sağlamak ve hiçbir ülkeyi geride bırakmamak için yeni kapasitelere ve bilgiye ihtiyaç duyarlar. Pek çok ülke, SKG hedeflerini ulusal koşullarına ve önceliklerine uyarlama konusunda ve bunları gerektiğinde politikalarına ve stratejik gelişim planlarına dâhil etmede ilerleme kaydetmişlerdir. SKG ile BİT ve e-Devlet ile ilgilenenler de dâhil olmak üzere ulusal stratejilerin kapsamlı ve dengeli gelişmesini amaçlamaktadır (Desa, 2019).

Ulusal planlar ve stratejiler genel yönü ve öncelikleri belirleyerek SKG çabalarını ulusal düzeyde tutarlı bir şekilde ifade etmek için bir fırsat haline gelmiştir. Entegre bir çerçeve olarak SKG'ler, tüm ülkeler ve toplumun bütünü ile ilgili yaklaşımların oluşturulmasını amaçlamakta ve pek çok ülke bu amaca uygun olarak ilerlemektedir.

SKG birçok ülkenin politikalarını ve kurumsal çerçevelerini e-Devlet uygulamalarına aktardıklarını ve uyarladıklarını göstermektedir. Bununla beraber devletin tüm bölümlerini, parlamentoları, yüksek denetim kurumlarını aktif olarak e-Devlet'e geçirme isteklerini hızlı ve güvenli bir şekilde devam ettirmek için olası sorunlara çözüm önerileri sunmaktadır. 2030 SKG'nin uygulanmasına yönelik ulusal kurumsal düzenlemelerin özeti, ülkelerin farklı bağlamlar ve şartlarla karşı karşıya kaldıkları kurumsal yaklaşımları yansıtmaktadır. SKG ile her ülke için toplanan bilgiler dokuz kategoride sınıflandırılmıştır (Desa, 2019):

- Ulusal stratejiler ve planlar;
- Ulusal kurumsal düzenlemeler;
- Yerel makamlar;
- Parlamento;
- Kamu görevlilerini işe almak ve donatmak;
- Sivil toplum ve özel sektör;
- İzleme ve inceleme;
- Üst denetim kurumları;
- Bütçeleme.

Ağustos 2016 - Aralık 2017 arasında gerçekleştirilen ve raporda yer alan tüm ülkeler, kendileriyle ilgili bilgileri inceleme ve New York'taki BM temsilcileriyle geri bildirimde bulunarak bu başlıkların oluşturulmasına katkı sağlamışlardır.

2030 SKG, Birleşmiş Milletlere Üye Devletlerin ulusal müdahalelere hızlı ve etkin bir şekilde cevap verilmesine yönelik çalışmaların artırılmasının sağlanmasına teşvik etmiştir. Bu çalışmaya göre SKG ülkelerin, hedef kitlenin ve küresel hedeflerin ulusal planlama süreçlerine, politikalarına ve stratejilerine nasıl dâhil edilmesi gerektiğine karar verme mekanizmasının her ülkenin bu alandaki ulusal kalkınma ve sürdürülebilir kalkınma stratejileri gibi mevcut planlama araçlarına bağlı olduğunu belirtmektedir.

SKG sürdürülebilir ve esnek toplumlara dönüşüm konusuna odaklanmaktadır. SKG sürdürülebilir kalkınmanın tüm boyutlarında esneklik sağlanması gerektiğini vurgulamakta ve kamu hizmetlerini desteklemek, sosyal güvenlik ağlarını iyileştirmek, etkin makroekonomik ve kentleşme politikaları gibi sistemlerin ve acil durum planlarının ötesine geçen bir dizi stratejiyi içermektedir (Desa, 2019).

Etkili e-Devlet uygulamalarında halkın güvenini sağlamak, SKG hedeflerine ulaşmak için atılan bir diğer temel adımdır. Bu, öncelikle insanların kurumsal performans konusundaki önceliklerini ve kaliteli kamu hizmetlerine eşit erişimlerini yansıtan sağlam kamu politikasının uygulanmasına bağlı olacaktır. Etkili hizmet sunumu için e-Devlet uygulamaları ihtiyaçları karşılayacak şekilde tasarlanmalı ve insanların bunları tanımlamaya aktif katılımını teşvik etmeli ve en önemlisi her seviyede güvenilir planlar ve projeler uygulayabilmelidirler. Yerel otoritelerin sürdürülebilir kalkınmadaki rolü, tüm bireylere ulaşmak olmalıdır. Bu nedenle, yenilikçi katılımcı mekanizmalar aracılığıyla tüm topluluklarla yerel olarak çalışmak şarttır. Vatandaşların etkili, adaletli ve vatandaş merkezli hizmet beklentilerindeki artış, uygulamaların sorunsuz bir şekilde sunulması ve gelişmiş kalkınma etkisi için yüksek işbirliğine dayanan çerçevelere geçişi zorunlu hale getirmektedir. Kamu hizmetinde teknoloji kullanımı ve uygulamaları için güvenilir, gizlilik ilkelerini içeren kapsayıcı, etkili bir ortam sağlamak için uzun vadeli politika ve stratejik çerçevelere ihtiyaç vardır. Bu çerçeveler, sürdürülebilir kalkınmanın temel ilkelerinin uygulanmasını destekleyen kamu hizmetlerine taslak niteliğindedir. Güvenilir kurumların performans beklentilerini karşılama kapasitesi, yeterlilik algıları ve herkes için etkin kamu hizmeti sunumu, kamu sorumluluğunun yanı sıra, kamu yönetiminde ve kamu sektörü reformunun altında yatan

hedeflerin başında gelmelidir. Cinsiyet eşitsizliği, özellikle katılımcı toplumsal cinsiyete duyarlı uygulamalar yoluyla, çok sayıda kamu politikası ile aşılmalıdır. Şeffaflık, katılım ve işbirliği ilkeleriyle vatandaşlar ve hükümetleri arasında güven inşa edilmesine özel önem verilmelidir (BM, 2019).

2.4.4. Teknoloji ve e-Devlet Güvenliği İlişkisini Etkileyen Faktörler

Teknoloji ile e-Devlet güvenliği arasındaki ilişkiyi etkilediği iddia edilen farklı faktörler arasında, kullanıcıların mahremiyeti, web tasarımı kalitesi, teknolojinin kullanım kolaylığı, e-Hizmetlerin yararlılığı gelmektedir. e-Devlet teknolojisini veya çevrimiçi teknolojileri etkileyen bir faktör olarak İBE gelmektedir. İBE, teknolojinin önemli bir belirleyicisi olarak ön plana çıkmaktadır. İBE bir kullanıcı ile e-Devlet uygulamaları arasında köprü görevini üstlenmektedir. Bilgisayarlar veya teknolojiyle ilgili insan davranışını ve etkileşimini sorgulayan araştırmacılar, bu etkileşime dâhil olan pek çok kavramın, teknolojilerdeki son gelişmelerden ve birçok karmaşık uygulamanın nispeten kolay geliştirilmesinden sorumlu olduğunu vurgulamışlardır. Son teknolojilerdeki gelişmeler günümüzde giderek daha fazla insanı etkilemektedir (Karakuş, Çağıltay, Kaşıkçı, Kurşun, & Ogan, 2014). Gelişmelerin yanı sıra, kullanıcı ara yüzü ve insan faktörleri problemi nedeniyle bu yeniliklerin kabulü ve yayılmasının ardında sıkıntılar bulunmaktadır (Zhang, Galletta, Sun, & Li, 2009). İBE'nin teknolojinin kabulü ve kullanımına nasıl katkıda bulunduğunun araştırılması önemli bir husustur. Her gün daha yeni uygulamalar geliştirildiğinden ve her bir yeniliğin kullanıcı teknolojileri için araştırılması gerektiğinden, e-Devleti etkileyen teknolojiler bilişsel uyum, görev teknolojisi uygunluğu, bireysel farklılıklara sahip kullanıcılar, ekonomik etkenler, kullanıcılar gibi faktörlere dayanmaktadır.

2.4.5. Kullanıcıların Gizliliği

İnsanların bilgi toplumuna geçmesiyle birlikte ciddi zorlukların ortaya çıktığını; özellikle bilgi ve ağ toplulukları ile ilgili popüler bir kavram olan dijitalleşmenin, toplumsal izolasyon ve yabancılaşmanın yanı sıra istihdam ve mahremiyetle ilgili endişelere neden olduğu savunulmaktadır (Gulliksen, 2014). Çevrimiçi gizlilik ve güvenlik siber saldırılardan etkilendiğinde gizliliğin ihlal edildiği görülebilir (Gulliksen, 2014). Ayrıca, e-Devlet kavramı, gizlilik sorunları, özellikle teknoloji değiştiğinde ve bağlamsal unsurlar söz konusu olduğunda her zaman bir endişe kaynağı olarak

görülmüştür. e-Devlet teknolojisinin çevrimiçi ödeme yöntemleri ve özel bilgilerin saklanması gibi protokolleri açıklamasının gerekliliği e-Devlet uygulamalarında ilk koşul olduğu vurgulanmıştır (Abunadi, 2015). Bu nedenle, teknoloji ve e-Devlet uygulamalarının güvenliği arasındaki ilişkiyi incelemek teknolojik bağlamlar değiştiğinde önem kazanmaktadır. (Hashim, Hassan, & Hashim, 2015; Sarabdeen & Ishak, 2015). Tüm bu teoriler, e-Devlet ile ilgili kullanıcıların gizlilik ve güvenliğine yönelik bireysel davranışları açıklamak için uygulanabilir. Bununla birlikte, sürekli değişen teknoloji dünyasında, gizlilik sorunlarının e-Devlet teknolojisini nasıl etkilediğini anlamak için bu teorileri genişletmek ve geliştirmek günümüzün önemli çalışma konuları arasında yer almaktadır (Gülbahar, Kalelioğlu, & Madran, 2010).

2.4.6. Web Tasarım Kalitesi

e-Devlet teknolojisini etkileyen bir diğer önemli faktör, web tasarımı ve kalitesidir. Web tasarım kalitesi e-Hizmet uygulamalarının kalitesinin bir unsurudur. e-Devlet hizmetlerinin çeşitliliği ve e-Hizmetlerin kalitesi dâhil olmak üzere birçok konuyu ele alan bir dizi çalışma bulunmaktadır (Papadomichelaki & Mentzas, 2012). Bu bağlamdaki e-Devlet ile ilgili çalışmalar incelendiğinde, e-Devlet kalitesinin etkileyen etmenler aşağıdaki şekilde sıralanabilir (Papadomichelaki & Mentzas, 2012):

- Etkileşim ortamının işlevselliği,
- Güvenilirlik,
- Vatandaş desteği (etkileşim),
- İçerik ve görünüm (kullanıcı arayüzü),
- Gizlilik,
- Mahremiyet,
- Kullanım kolaylığı (navigasyon, kişiselleştirme, teknik verimlilik).

Güvenilirlik, gizlilik, verimlilik ve vatandaş desteğini içeren e-Devlet kalitesi modelleri göz önüne alındığında e-Devlet web sitelerine daha fazla önem verilmesi gerektiği ifade edilmektedir. Sonuç olarak e-Devlet sistemleri web tabanlı uygulamalardır ve bu tür uygulamalarda kullanım kolaylığı, platformun anlaşılabilir olması ve kullanıcıya güven vermesi en önemli değerlendirme parametreleri arasında yer almaktadır. Bu parametreler e-Devlet platformunun kalitesini doğrudan etkilemektedir (Chang & Chen, 2009; Papadomichelaki & Mentzas, 2012). Ayrıca, web tasarımı kalite faktörleri nedeniyle ortaya çıkabilecek herhangi bir engeli belirlemek ve

e-Devleti etkili kullanmak gerektiğini vurgulamışlardır (Papadomichelaki & Mentzas, 2012).

Web sitesi tasarım kalitesinin, değişen teknoloji ile beraber, e-Devlet teknolojisi üzerindeki etkisinin araştırılması önemli bir faktör olarak görülmüştür. Aynı zamanda web tasarım uygulamalarındaki “e” hizmet kalitesini anlamak için uygulanan yaklaşımların daha ayrıntılı bir şekilde hazırlanması gerektiği önerilmektedir (Halaris ve diğerleri, 2007).

2.4.7. e-Devlet Güvenliği ve Kullanıcı Merkezliliği

e-Devlet güvenliğini etkileyen bağlamsal faktörler arasında en önemlisi olarak kabul edilen teknoloji faktörüdür. Çevrimiçi hizmet sağlayıcısı tarafından web sitesinde yerleşik olan ve müşterilerin verilerinin güvenliği konusundaki gizliliğini belirten bir faktörü oluşturan teknik yapının, kullanıcılar tarafından algılanan genel güvenliği doğrudan etkilediğini tespit edilmiştir (Gülbahar, Kalelioğlu, & Madran, 2010). Genel güvenlik, çevrimiçi şifre uygulamaları, kredi kartı bilgileri gibi alanların bilgi güvenliğinin sağlanması anlamına gelmektedir. Teknolojinin, kullanıcıların bilgilerini koruma yollarını sağladığını ve böylelikle kullanıcıların güvenlik inancını olumlu yönde etkilediği belirtilmektedir (Chang & Chen, 2009). Teknoloji kullanımı yaygınlaşmakta ve bu durum bazı güvenlik bazı risklerini de sebep olmaktadır. Bu bağlamda teknolojinin güven ve risk analizi faktörlerinin kullanılarak değerlendirilmesi büyük bir önem arz etmektedir. e-Devlet hizmetleri güvenliğini etkileyen bir faktör olarak doğrudan güven ve risk analizi arasındaki ilişkinin geliştirilmesi gerektiğini belirtilmektedir (Shah et al., 2014). Bir yandan teknoloji, diğer yandan güven ve risk analizi arasındaki ilişkinin kurulmasına yönelik teorik destek, sosyo-teknik teorisi ile sağlanmaktadır. Sosyo-teknik teorisi, teknik alt sistem ile sosyal alt sistem arasında bir uyumun olması gerektiğini savunmaktadır (Bostrom ve Heinen, 1977). Böylece, teknoloji ile güven ve risk analizi arasında kullanıcı merkezli ilişki kurmak mümkündür.

Bu ilişkiler aşağıda verilen 3 başlık şeklinde sıralanabilir (Bostrom & Heinen, 1977):

- Risk ve Kullanıcı Odaklı e-Devlet Güvenliği Arasındaki İlişki
- Kullanıcı Güveni ve Kullanıcı Odaklı e-Devlet Güvenliği Arasındaki İlişki
- Teknoloji ve Kullanıcı Odaklı e-Devlet Güvenliği Arasındaki İlişki.

2.4.8. e-Devlet Güvenlik Problemleri

e-Devlet portallarının en fazla karşılaşılan en önemli problemlerden birisi de güvenlik problemleridir. Bu tür sistemlerde kritik veriler kaydedilmektedir. Bu verilere ulaşmak için birçok saldırı yöntemi mevcuttur. Hatta devletlerin kritik bilgilerini ele geçirebilmek için e-Devlet portallarına sürekli olarak saldırılar düzenlenmektedir. e-Devlet sistemlerinde güvenlik açıkları iki şekilde meydana gelmektedir. Bunlar sistem ve kullanıcı kaynaklı güvenlik açıklarıdır. Genel olarak sistemlerin güvenlik alt yapısı uluslararası güvenlik protokolleri kullanılarak sağlanmaktadır. Bu sebepten dolayı sistem tarafında çok önemli güvenlik zafiyetleriyle sıklıkla karşılaşmamaktadır. Burada en önemli risk faktörü insandır. Bundan dolayı e-Devlet güvenliği konusu sosyal bilimlerin bir çalışma alanıdır. e-Devlet kullanıcıları ile ilgili faktörler, özellikle de sosyal bilim ve yönetim perspektifinden bakıldığında, e-Devlet hizmet güvenliği açısından iyi bir şekilde ele alınmamaktadır (Shah et al., 2014). Pratik açıdan bile, e-Devlet portalları, kullanıcıları güvenlik hususları hakkında bilgilendirmek veya güvenlik ihlallerinden haberdar olmaları konusunda eğitmekle ilgilenmiyor gibi görülmektedirler. Bu durum, e-Devlet hizmetlerinin yanlış yönetilmesine neden olan önemli bir faktördür. Kullanıcı merkezli faktörler hakkındaki bilgi eksikliği, e-Devlet hizmeti sağlayan kurumların ve e-Devlet hizmeti güvenliğini içeren kullanıcıların başarısını etkileyebilir (Shareef et al., 2011). Kullanıcıların e-Devlet uygulamaları ile işlem yaptıklarında güvenlik konusunda büyük endişe duydukları açıkça gözlenmektedir (Jarvenpaa, Tractinsky, & Vitale, 2000).

Teknolojik faktörlerin, kullanıcılara daha iyi hizmet sunmak amacıyla, teknolojiye meydana gelen değişikliklere uyum sağlamak için e-Devlet hizmet sağlayıcılarını sürekli değiştirmeye ve altyapılarını düzenlemeye zorladığı görülmektedir (Castells & Cardoso, 2006; Cruz, Tan, & Yonaha, 2015). Bununla birlikte, e-Devlet hizmetlerindeki yenilikler arasındaki temel odak e-Devlet hizmet güvenliğidir (AlKalbani, Deng, & Kam, 2015). e-Devlette yeni teknolojiler ortaya çıktığında mevcut güvenlik unsurları,

- Kullanıcılarda uygulamalara yönelik güvensizlik (Abu-Shanab & Al-Azzam, 2012),
- Yeni teknolojilerle ilgili risk faktörlerinin varlığı,
- Gizlilik sorunlarından kaynaklanan problemler (Lim et al., 2015),
- Kalite sorunları,
- İnsan bilgisayar etkileşimi sorunları (Gulliksen, 2014),

- Teknolojinin kullanım zorlukları (Ayyash et al., 2013),
- Kültürel ve maddi konular(Abunadi, 2015),

şeklinde sıralanabilir. Bu konuların, kullanıcılar tarafından e-Devlet hizmetlerinin kullanımını etkileme potansiyeli vardır ve e-Devlet hizmetlerinin kullanımının azalmasına neden olmaktadır. Kullanıcılar için endişe verici olan bir diğer önemli husus ise e-Devlet alanındaki kullanıcıyı merkeze alan araştırma sonuçlarının eksikliğidir (Elsheikh & Azzeh, 2014). Yapılan araştırmaların çoğunun kullanıcı odaklı çalışmalardan ziyade e-Devlet güvenliği ile ilgili teknolojik konulara odaklanılmış olmasıdır (Shah et al., 2014). Böylece iki önemli nokta ortaya çıkmaktadır. Birincisi, e-Devlet alanında meydana gelen teknolojik değişikliklerin ve bunun sonucunda ortaya çıkan güvenlik kaygılarının oluşmasıdır. İkincisi ise bu kaygıların üstesinden gelmek için kullanıcı merkezli yaklaşımların eksikliğidir.

ÜÇÜNCÜ BÖLÜM

3. DÜNYADA VE TÜRKİYE'DE e-DEVLET

Bu bölümde temel olarak Dünya' da ve Türkiye' de e-Devlet kullanımı hakkında bilgiler verilmiştir ve bu bilgilerin ışığında bilgi güvenliği konusu ele alınmıştır. Bilgi güvenliğinin e-Devlet platformlarının kullanımına etkisi analiz edildiğinde, ülkenin gelişmişlik düzeyi ve e-Devlet kullanımının doğru orantılı olduğu varsayımı çıkarılmaktadır. Ayrıca internet okuryazarlığı, sisteme olan güvenin de e-Devlet kullanım indeksinde etkili olduğu hipotezi ortaya konulmuştur. Hipotezi desteklemek için sırasıyla Dünya' da e-Devlet gelişmişlik analizi, Dünya'daki büyük şehirlerde e-Devlet kullanımı, Türkiye' de e-Devlet kullanım indeksi ve sıklıkla kullanılan e-Devlet uygulamaları ele alınmıştır. Bir önceki bölümde tanımı yapılan e-Devlet'in detayları bu bölümde verilmiş olup, bilgi güvenliğiyle olan temel ilişkisi ele alınmıştır. Ayrıca, bilgi güvenliğinin ayrılmaz bir parçası olan bilişim hukukuyla ilgili mevzuatlar da bu bölümde verilmiştir.

3.1. Dünyada e-Devlet Gelişmişlik Analizi

e-Devlet Gelişim İndeksi (EGI), BM üye devletlerinin e-Devlet Gelişim durumunu göstermektedir. Bir ülkedeki web sitesi geliştirme modellerinin değerlendirilmesinin yanı sıra, EGI, bir ülkenin halkının bu hizmetlere erişimini ve katılımını teşvik etmek için bilgi teknolojilerini nasıl kullandığını yansıtmada altyapı ve eğitim düzeyleri gibi erişim özelliklerini içermektedir. EGI, e-Devletin üç önemli boyutunun, yani çevrimiçi hizmetlerin sunulması, telekomünikasyon bağlantısı ve insan kapasitesinin birleşik bir ölçüsüdür. Aynı zamanda, BM'nin 2008-2018 yılları arasında yaptığı anket çalışmasında dünyada e-Devlet alanında gelişmiş ilk 10 ülke Tablo 1.'de verilmiştir.

Tablo 1. e-Devlet Alanında Gelişmiş İlk 10 Ülke İndeksi (BM, 2019)

2008		2010		2012	
Ülke	İndeks	Ülke	İndeks	Ülke	İndeks
İsveç	0,9157	Kore	0,8785	Kore	0,9283
Danimarka	0,9134	ABD	0,8510	Hollanda	0,9125
Norveç	0,8921	Kanada	0,8448	İngiltere	0,8960
ABD	0,8644	İngiltere	0,8147	Danimarka	0,8889
Hollanda	0,8631	Hollanda	0,8097	ABD	0,8687
Kore	0,8317	Norveç	0,8020	Fransa	0,8635
Kanada	0,8172	Danimarka	0,7872	İsveç	0,8599
Avustralya	0,8108	Avustralya	0,7863	Norveç	0,8593
Fransa	0,8038	İspanya	0,7516	Finlandiya	0,8505
İngiltere	0,7872	Fransa	0,7510	Singapur	0,8474
2014		2016		2018	
Ülke	İndeks	Ülke	İndeks	Ülke	İndeks
Kore	0,9462	İngiltere	0,9193	Danimarka	0,9150
Avustralya	0,9103	Avustralya	0,9143	Avustralya	0,9053
Singapur	0,9076	Kore	0,8915	Kore	0,9010
Fransa	0,8938	Singapur	0,8828	İngiltere	0,8999
Hollanda	0,8897	Finlandiya	0,8817	İsveç	0,8882
Japonya	0,8874	İsveç	0,8704	Finlandiya	0,8815
ABD	0,8748	Hollanda	0,8659	Singapur	0,8812
İngiltere	0,8695	Yeni Zelanda	0,8653	Yeni Zelanda	0,8806
Yeni Zelanda	0,8644	Danimarka	0,8510	Fransa	0,8790
Finlandiya	0,8449	Fransa	0,8456	Japonya	0,8783

Tablo 1’ de 2008-2018 yılları arasındaki çift yılların e-Devlet kullanım indeksi verilmiştir. Tablo 1 ele alındığında ilk yıllarda ABD ve Avrupa ülkelerindeki kullanım ilk sıralarda yer alırken, ilerleyen yıllarda uzak doğu ülkelerinin (Kore, Japonya, Singapur) sıralamaya girdiği gözlemlenmiştir. Bunun başlıca sebebi, uzak doğu ülkelerinin çok hızlı bir şekilde teknolojik süreçlere entegre olmaları, kendi bilgi güvenliği yöntemlerini önermeleri (Türkiye gibi ülkelerde ABD ulusal standartlar enstitüsü tarafından kabul edilen şifreleme yöntemleri kullanılmaktadır) ve teknoloji okur-yazarlığının ileri seviyede olması gibi sebepler verilmektedir. Ayrıca BM’rin raporuna göre 2014 yılı itibari ile 193 ülkenin e-Devlet uygulamalarında aktif olduğu sonucuna varılmıştır ve Tablo 1’de analiz edildiğinde en iyi 3 ülkenin Danimarka, Avustralya ve Güney Kore şeklinde sıralandığı görülmektedir. BM’in yaptığı araştırma ve Tablo 1 incelendiğinde aşağıdaki sonuçlara ulaşılmaktadır:

- Tek noktadan platformlarla çevrimiçi kamu hizmeti sağlamak için e-Devleti kullanan ülkelerin sayısında keskin bir yükseliş olmuştur.
- Kamu kurumlarının daha kapsayıcı, etkili, hesap verebilir ve şeffaf olmasını sağlamak için pek çok ülke e-Devlet hizmetlerine katılmaktadır. Dünyanın dört bir yanındaki birçok hükümet kamuya açık bilgi erişimi için verilerini e-Devlete aktarmaktadır.
- Gelişmiş elektronik ve mobil hizmetleri kullanma çabaları artmıştır.
- Dünya genelinde Avrupa devletlerinin e-Devlet gelişmelerine öncülük ettiği gözlenmiştir.
- Ülkelerin gelir seviyesi ile e-Devlet sıralaması arasında pozitif bir ilişki olduğu görülmektedir. Öte yandan, düşük gelirli ülkelerin, indeks bileşenlerinin nispeten düşük seviyede olması nedeniyle geride kaldığı görülmektedir.
- e-Devlet kullanımı sonucunda oluşan hız ve karmaşıklıklarla başa çıkılabilmesi için yasal reformun temeli oluşturulmuştur.
- e-Devletin, yöneticilere sosyal eşitlik ve dijital bölünme sorunları ile mücadele etmek için güçlü araçlar sağladığı görülmüştür (Atılgan, 2009).

BM yapmış olduğu araştırmada 2008-2018 yılları için Türkiye’nin indeks değerleri Şekil 10’da verilmiştir.



Şekil 10. 2008-2018 Yılları Arasında Türkiye e-Devlet İndeks Sonuçları (BM, 2019)

Şekil 10'daki değerler dikkate alındığında e-Devlet uygulamalarının Türkiye'de her geçen yıl arttığı gözlenmiştir. 2008 yılında e-Devlet durumunu kıyaslama yönündeki araştırmalarda BM, son 10 yılda Türkiye'nin hızla büyüdüğünü belirtmektedir. Bununla beraber 2016 yılında Türkiye dünya genelinde 68, 2018 yılında ise 0.7112 indeks ile 53. sırada yer almaktadır. Bu sıralama 2 yıl içerisinde Türkiye'de e-Devlet uygulamaları ve kullanımının 15 puan arttığını göstermektedir. Bu sıralamada çevrimiçi hizmetler, telekomünikasyon bağlantısı ve insan kapasitesi bileşen dağılımının indeks değerleri sırası ile 0.89, 0.43 ve 0.81 olarak verilmiştir (BM, 2019).

BM'in yaptığı araştırma sonuçlarına göre dünya genelinde şehirlerin performansını analiz etmek için bölgesel olarak geliştirilen çevrimiçi hizmetlerin kullanımını gösteren yerel çevrimiçi hizmetler indeksi (YÇHİ) Tablo 2. 'de verilmiştir.

Tablo 2. Çevrimiçi Hizmetler İndeksi Şehirlerin 2018 Yılı Sıralaması (BM, 2019)

Kent	Bölge	Şehir Nüfusu	YÇHİ	2018 Ülke İndeksi
Moskova	Avrupa	11918057	1	0,7969
Cape Town	Afrika	433688	2	0,6618
Talin	Avrupa	413782	3	0,8486
Londra	Avrupa	8135667	4	0,8999
Paris	Avrupa	2243833	5	0,879
Sidney	Okyanusya	4451841	6	0,9053
Amsterdam	Avrupa	821752	7	0,8757
Seul	Asya	9860372	8	0,901
Roma	Avrupa	2867671	9	0,8209
Varşova	Avrupa	1735391	10	0,7926
Helsinki	Avrupa	616690	11	0,8815
İstanbul	Asya	14100000	12	0,7112
Şanghay	Asya	14348535	13	0,6811
Madrid	Avrupa	3186241	14	0,8415
New York City	Amerika	8550405	15	0,8769

BM yaptığı araştırmada Türkiye yüksek ortak gelirli olarak kabul edilmiştir. Tablo 2’de de gösterildiği gibi İstanbul e-Devlet alanında gelişmişlik sıralamasında 2018 yılı için iller bazında 12. sırada yer aldığı gözlenmektedir (BM, 2019). Bu durumun başlıca sebebi İstanbul’da devlet dairelerine erişimin zor olması, kamusal alanlarda kuyrukların fazla olması ve bu nedenle vakit kaybı problemi, araç park problemi, mobil e-Devlet uygulamalarına kullanım eğilimi gibi sebepler İstanbul’un sıralamasını açıklamaktadır. Yerel yönetimlerin de sayısal platformlardan hizmet vermesi ve bu platformların da bilgi güvenliği yerel idare gayretiyle sağlanması elektronik platform kullanımını arttıran diğer bir etmendir. Çünkü bu sistemlerde gerçekleşecek herhangi bir bilgi güvenliği problemi, sistemlerin kullanımının terkedileceğinin en büyük göstergesidir. Tablo 1’ de Rusya yer almazken, Tablo 2’ ye göre 1. sırada Moskova yer almaktadır. Bu durum Moskova’nın kötü trafiği, kamu alanlarının hizmet açısından yeterli olmaması, Moskova’nın gelişmiş internet alt yapısı, Rusya’nın kendine ait yerli ve milli bilgi güvenliği önlemlerinin başarılı bir şekilde uygulanması, Moskova’nın ilk sırada yer almasının maddi sebepleri arasında sayılabilmektedir. Dünya’ da e-Devlet kullanımı seçilen ülkeler bazında Bölüm 3.2’ de kapsamlı bir şekilde verilmiştir.

3.2. Dünyada e-Devlet Kullanımı

Gelişmiş ülkelerde e-Devlet yaygın olarak kullanılmakta ve birçok hükümet-vatandaş etkileşimi bilişim sistemleri kullanılarak çözülmektedir. İnternet alt yapısının yaygınlaşması ve teknolojinin hızla gelişmesinin bir sonucu olarak e-Devlet orta doğu ülkelerinde de aktif olarak kullanılmaya başlanmıştır. Özellikle Arap Bahar'ından sonra ortadoğu ülkelerinin çoğunda iç isyanlar ve savaşlar meydana gelmiştir. Halen devam eden iç savaş ve terör eylemlerine rağmen, bu ülkelerde de e-Devlet birçok problemi çözmek ve hükümet-vatandaş etkileşimini sağlıklı bir şekilde sürdürebilmek için aktif olarak kullanılmaktadır. Ortadoğu ülkelerinin ele alınmasının en önemli sebebi Türkiye'ye komşu olmaları ve mülteci krizinden en çok etkilenen ülkenin Türkiye olmasıdır. Bunun yanı sıra son zamanlar da körfez ülkeleriyle kurulan iyi ilişkiler, bu alanda araştırma yapılmasını zorunlu bir hale getirmiştir. Seçilen ortadoğu ülkelerinin e-Devlet uygulamalarıyla ilgili bilgi aşağıdaki gibi verilmiştir (Saadi,& Almahjoub, 2013).

İş sektöründe sağlanan e-Hizmetler ile vatandaşların iyi etkileşimi, BİT'in kabul edilmesindeki hızlı gelişme ve vatandaşlardan kabulünün arttırılmasına yönelik tutumlar hükümetleri BİT'i vatandaşlarına daha iyi hizmet sağlama aracı olarak kullanmaya teşvik etmektedir. Aynı zamanda, BİT'nin kabul edilmemesi nedeniyle dijital bölünme olarak bilinen yeni bir sorun ortaya çıkmıştır. Bu, bireylerin çeşitli düzeylerde hükümetlere ve milletlere kadar boşluklar oluşmasına neden olmaktadır. Aynı zamanda, e-Devletin performansını da etkilemekte, bu nedenle bir yandan dijital uçurumun kapatılması ile diğer yandan e-Devletin performansının yükseltilmesi arasında bir korelasyon ortaya çıkmaktadır. Bu değişim sadece gelişmiş ülkeleri değil aynı zamanda zengin ve fakir Arap ülkelerine ek olarak gelişmekte olan ülkeleri de kapsayacak şekilde genişlemiştir (Nations, 2012). Bölgeler ve ülkeler arasında e-Devlet, akıllı devlet gibi dijital dönüşüm durumlarında ve dijital dönüşümün ekonominin gelişiminde dünya genelinde gözlemlendiği rolü gibi ülkeler arasında büyük farklılıklar var.

Tek noktadan eşit, kolaylaştırılmış hizmet verme ve kontrolün başarıyla sağlanması için pek çok gelişmiş uygulama e-Devlet üzerinden hizmetleri kullanılmakta ve uygulamaktadır. Dünya genelinde pek çok ülke e-Devlet uygulamalarına öncülük etmektedir. Bu ülkelerin başında ABD ve İngiltere gelmektedir.

3.2.1. Amerika Birleşik Devletleri

BİT’de pek çok alanda liderliğini koruyan ABD e-Devlet alanında da gelişmiş ülkeler alanında dünya genelinde büyük bir yüzdeye sahiptir. e-Devlet alanında pek çok yatırımlar gerçekleştiren ABD e-Devlet çalışmalarına 1993 yılında başkan Bill Clinton ile başlamıştır. Bu dönemde Access America projesi sunularak e-Devlet uygulamalarına bir giriş yapılmıştır. 2001’lerin başlarında “firstgov” isimli portal aracılığı ile ABD vatandaşlarına tek noktadan hizmet verilmesi sağlanmıştır. Bu uygulama sonrasında “usa.gov” olarak kullanılmaya devam etmiştir. Bu uygulamanın “resmi kurumlar, yardım ve bağışlar, toplum, işsizlik, meslekler, alışveriş, seyahat, hizmetler” olmak üzere farklı uygulama alanları bulunmaktadır. Bu başlıkların her biri ilgili alan ile alakalı farklı hizmetler içermekte ve genelleşmektedir. Bu portal geliştirilen diğer uygulamaların da alt yapısını oluşturmaktadır. 2003 yılında ABD’ye ait 35 milyondan fazla web sayfasının tek başlık altında aranmasının sağlanması ile tek noktadan bilgiye erişim sağlanması gerçekleştirilmiştir. ABD 2009 harcamalarının yüzde 10’unu, 2011’de ise yüzde 12’sini e-Devlet uygulamalarına ayırmıştır. Bu ve benzeri gelişmeler ABD’nin pek çok e-Devlet hizmetinde öncü olmasına ve dünya sıralamasında ülke hazır oluş endeksinde üst sıralarda yer almasına sebep olmuştur. e-Devlet şeffaf, vatandaş merkezli, işlem maliyetinin azaltılması, tek noktadan kaynak kontrolü, gizlilik, güvenlik, yenilikçi gibi pek çok avantajından dolayı sadece ABD’de değil dünyanın pek çok ülkesinde yaygın uygulama alanı bulmuştur.

3.2.2. İngiltere

e-Devletin hızla uygulama alanı bulduğu bir diğer ülke İngiltere’dir. İngiltere e-Devlet uygulamalarına çok hızlı adapte olan ülkelerin başında gelmektedir. Bu yaygın kullanımın temelinde geniş internet kullanıcı sayısı gelmektedir. İngiltere’de e-Devlet uygulamaları Blair hükümeti döneminde başlamıştır. Bu başlangıç hükümet bünyesinde kurulan “Office of e-Envoy” uygulaması ile büyük hız kazanmıştır. Aynı zamanda 1998 yılında e-Devlet uygulamalarında e-Ticaretin önemi üzerine bir rapor hazırlanmış ve bu rapor e-Ticaret uygulamalarının önünü açmıştır. Bu gelişme ile beraber e-İmza uygulamaları da e-Devlet uygulamalarında yer almaya başlamıştır. İngiltere 2000 yılında e-Devlet stratejisi üzerine bir rapor yayınlarak geliştirilen uygulamaların belli bir plana uygun olmasını sağlamıştır. Bununla beraber 2001 yılında “Government Gateway” uygulaması ile e-Devlet uygulamalarındaki güvenlik ve doğrulama alt yapısı

oluşturulmuş ve bu kavramların önemi üzerinde durulmuştur. Yaşanan tüm gelişmeler ile beraber 2006 yılında tüm çevirim içi hizmetler cep telefonu aracılığı ile insanların kullanımına sunulmuştur. Bu gelişmeler ile beraber İngiltere’de biyometrik sistemler ve güvenlik ön planda tutulmuş ve pek çok farklı uygulamada kendisine yer bulabilmiştir.

3.2.3. Finlandiya

Finlandiya gelişmiş BİT’ne sahip bir diğer ülkedir. Finlandiya aynı zamanda eğitimde pek çok ülkeye rol model olmuştur. 1999 yılına kadar BİT’ne ve yetişmiş insan gücüne büyük önem vermiş ve büyük destek miktarları ayırmıştır. Bu BİT alanındaki gelişmişlik ve yetişmiş insan gücü e-Devlet uygulamalarına hızlı geçişe sebep olmuş ve e-Devlet uygulamalarında Finlandiya büyük bir yüzdelik dilime sahip olmuştur (Yürük, 2017)

3.2.4. Irak

Gelişmiş ülkeler ile beraber gelişmekte olan ülkelerde de e-Devlet farklı şekillerde karşımıza çıkmaktadır. Örneğin Irak, Ortadoğu ülkelerinden biridir ve stratejik bir konumdadır. Ayrıca Irak’ın eski bir uygarlığı mevcuttur. Tarih boyunca, Irak, özellikle yirminci yüzyılda topraklarında petrolün bulunmasından sonra bölgedeki birçok istilacı gücün hedefi olmuştur (Alshboul, 2012). Irak’taki hükümetler dünyaya petrol çıkarıp ihraç ederek ve büyük kazançlar elde ettiler. Bu nedenle, bu gelirler, 1970’lerin sonunda ülkenin diğer sektörlerin yanı sıra eğitim, sağlık, sanayi gibi çeşitli sektörlerde Irak’ın gelişimine katkıda bulunmuştur. 1980’lerin sonunda, dünyadaki BİT’in evrimi yükseldiğinde, Irak komşusu İran’la bir savaşa girmiştir. Ağustos 1990’da Irak, Kuveyt’i işgal ederek 1991’in başında BM’ye ekonomik yaptırımlar uyguladıktan sonra Amerika Birleşik Devletleri liderliğindeki uluslararası bir koalisyona karşı bir başka savaşa girmiştir. Irak (1991 - 2003) döneminde toplumun her yönünü etkileyen ve ülkeyi modern dünyadan izole eden bu yaptırımlara maruz kalmıştır. 2003 yılının Nisan ayında, ABD İrağı işgal ederek rejimi kaldırdı; böylelikle BM’ler de yaptırımlarını iptal etmiştir. Irak’taki yeni rejim, ilk günden itibaren dünyadaki gelişime ayak uyduracak modern bir ülke kurmaya çalışmaktadır. BİT, İrağın geliştirmek istediği temel unsurlar arasındadır. Irak ‘da, internet kullanıcılarının oranı 2015 yılında yaklaşık (% 17) civarındadır. Bu nedenle, e-Devlet çevrimiçi hizmetlerinden yararlanamayan çok sayıda insan bulunmaktadır. Bir e-Devlet uygulamasına erişmek isteyen herhangi bir kullanıcı,

kişisel bilgilerinin hacklenmeyeceğinden emin olmalıdır (Saadi,& Almahjoub, 2013). Bu nedenle, güvenlik konusu herhangi bir e-Devlet uygulamasında önceliğe sahip olmalıdır. Irak'ta, bazı resmi web siteleri hala, kolayca saldırıya uğrayabilecek veya tahrip edilebilecek vatandaşlarla iletişim kurmak için ücretsiz posta adreslerine dayanmaktadır (Alshboul, 2012).

Irak'ta e-Devlet projesi ve hizmetlerinin değerlendirmesi üzerine BİT'sinin kullanımı e-Devlet hizmetlerinin kullanımının bir parçası olduğu, e-Devlet projesinin devletin ayırdığı kaynaklara ve alt yapıya bağlı olarak gelişim gösterecektir, ayrıca;

- Personellerin bu hizmetleri oluştururken büyük görevinin kâğıttaki verinin elektronik ortama aktarılmasında ve veri tabanlarının oluşturulmasında olduğunu
- Irak'taki ağ ve iletişim alt yapısının e-Devlet hizmetlerine uygun hale getirilmesinin sağlanması gerektiği
- İnsanların bilgisayar yerine akıllı telefon kullandıklarını bu nedenle akıllı telefonlar üzerinde geliştirilecek e-Devlet uygulamalarının daha fazla insana ulaşacağını
- Devlete ait e-Devlet hizmetlerinin artırılması ile başlangıçta insanların güveninin sağlanması gerektiği

gibi unsurlara dikkat çekilmiştir (Ramadhan, 2017).

Irak'ta e-Devlet uygulamalarının başarılı bir şekilde sonuçlandırılması için gereken özellikleri araştırılmıştır. e-Devlet uygulamalarında bilgisayarlı alt yapıyı kullanmanın verimliliği ve şeffaflığı artıracak, e-Devlet projesinin Irak'ta uygulanmasında ilk şartın bu alana ayrılacak bütçenin sağlanması gerekmektedir;

- e-Devlet uygulaması, başlangıçta e-Devletin gerekliliklerine uygun olarak devlet kurumlarının yeniden yapılandırılmasını gerektirir. Bu nedenle eski kurum yapısının varlığı ile e-Devlet projesinin uygulanması proje başarısızlığına yol açmıştır.
- Kamu kurumlarında, bilgi otomasyonu sürecine başlamadan önce iyi yönetim ilkelerinin uygulanması, işlerin düzgün bir şekilde devam etmesini sağlamak için önemli olduğunu belirtmiştir.
- Devlet kurumlarında uzmanlaşmış eğitim merkezleri sağlayarak e-Devlet uygulamalarının kullanımı için personelin rehabilitasyonu ve eğitimi ihtiyacı mevcut olduğu belirtilmiştir

- Bazı vatandaşlar ve çalışanlar arasında e-Devlet kavramı ve uygulamasının önemi konusunda farkındalık eksikliği bulunduğu gösterilmiştir.
- Resmi işlemlerde elektronik imzanın kabulüne ek olarak, e-Devlet projesini uygulamak için uygun mevzuatın geliştirilmesi ihtiyacının olduğu gösterilmiştir.
- Gelişen ve gelişmekte olan ülkelerin deneyimlerinde e-Devlet projesinin uygulanmasındaki engelleri, hatalarından ders almak ve başarılarından yararlanmak için kullanma zorunludur.
- Irak'ın tamamında e-Devlet projesinin uygulanması birçok zorluğa yol açıyor, bu nedenle bu projenin bakanlıklardan veya valiliklerden birinde uygulanması çalışmada önerilmiştir.
- Ülkenin tüm bölgelerine e-Devlet hizmetlerinin verilmesinin zorluğundan dolayı, mobil devlet uygulamaları veya Web 2.0 gibi alternatif teknolojilerin kullanılması önerilmiştir.
- Irak vatandaşlarının e-Devlet uygulamalarını kullanmaya hazır olmadıklarından dolayı, e-Devlet uygulamalarını kullanmak için eğitilmiş çalışanların vatandaşlara hizmet verebilecekleri şehir ve köylerde elektronik servis merkezlerinin yaygınlaştırılması önerilmiştir.

Aynı zamanda bu sonuçlar dikkate alındığında Irak'ta başarılı bir e-Devlet projesi için yol haritası çizmek için vatandaşların devlet kurumlarıyla işbirliği yapması gerektiği vurgulanmıştır (Abdulrahman, 2014).

Irak'ta pasaport ediniminin zorlukları Çalışma Vatandaşlık İşleri Genel Müdürlüğü'nün desteği ile pasaport elde etmenin zorluklarının tespit edilmesi için 219 vatandaşa rastgele dağıtılan bir anket oluşturulmuştur. Elde edilen sonuçlar aşağıda sunulan iki başlık altında toplanmıştır;

- Pasaport müdürlüğünde çalışanların karşı karşıya kaldıkları zorluklar
- Bekleme süresinde meydana gelen uzamalardan dolayı vatandaşların karşılaştığı zorluklar

Aynı zamanda pasaport hizmetlerinin e-Hizmetler başlığı ile ilişkilendirilerek prosedürlerin azaltılması yönünde bir takım çözüm önerileri sunmuştur (Al-Baiaty, 2017).

3.2.5. Libya

Libya ise Afrika'nın kuzeyinde yer alan ve gelişmekte olan bir Arap ülkesidir. Afrika'da ve dünyada 17. sırada yer alan dördüncü büyük ülkedir. Ülke, nüfusu 6,4 milyon olan yaklaşık 1,8 milyon kilometrekarelik bir alanı kaplamaktadır. Büyük alan ve küçük nüfus nedeniyle ana şehirleralarında büyük mesafelere sahiptir (Al-Baiaty, 2017). Ayrıca “Halkın yüzde doksanı, özellikle sahil boyunca olan alanın yüzde 10'undan azında yaşıyor” (Carl, 2015). Libya 49 ilden oluşmaktadır. Libya'nın üç ana kenti Trablus, Bingazi ve Sabah'tır. Trablus, Libya'nın 6.4 milyon nüfusunun yaklaşık% 20'sine ev sahipliği yapan Libya'nın başkentidir. Libya, Afrika'nın kişi başına gayri safi yurtiçi hasılasının % 5'ini oluşturduğu için, dünya petrolünün% 2'si olan büyük petrol yatırımlarına sahiptir (Saadi,& Almahjoub, 2013). Libya, Arap dünyasında en yüksek okuryazarlık oranına ve BM'nin ortalama yaşam, toplum güvenliği, sağlık sıralamasında yer alan İnsani Gelişme Endeksi'ne sahiptir. Libya, Arap dünyasında en yüksek okuryazarlık oranına sahip ve BM'nin ortalama yaşam, toplum güvenliği, sağlıkla ilgili tedbirler ve diğer büyüme konuları arasında yer alan İnsani Gelişme Endeksi, Libya'yı tüm Afrika ülkelerinin en üst sıralarına yerleştiriyor. Hükümet, Libya'da BİT altyapısının geliştirilmesinde ve genel BİT stratejilerinde eğitimde BİT'e katılmasında taktikler uygulamaktadır. Libya, sınır komşu ülkelere karşı ana girişimleri ve planları destekleyerek Afrika kıtasında bir baş gemi parçası kazanmayı hedefliyor. Zayıf mevcut altyapı ve deneyimli ve BİT donanımlı eğitimci eksikliği, son süreç için büyük bir zorluktur (Alshboul, 2012). Öte yandan Libya, vatandaşlara ve iş yerlerine iyi olanaklar sağlayabilecek bir e-Devlet platformunun planlanması ve uygulanması sürecinin ilk adımlarını halen sürdürmektedir ve üstesinden gelmesi gereken ilave zorluklar ve üstesinden gelmesi gereken zorluklar bulunmaktadır (Carl, 2015). 2012'deki iletişim ve bilişim Bakanlığı, devlet süreçlerini desteklemek ve Libya'daki tüm işletmelere ve vatandaşlara sunulan hizmetleri geliştirmek için teknolojiyi kullanmak için birçok girişim önermiştir. Hükümet girişiminin başarısını sağlamak için Bakanlık, tam bir strateji geliştirme ve hükümetin temel özelliklerinin işletilmesi için yol haritasını belirleme konusunda tam bir strateji geliştirme yetkisini aldıktan sonra çok uluslu profesyonel hizmetler ile sözleşme imzalamıştır. Ülke, nüfusunda etkileyici bir okuryazarlık oranına sahiptir, ancak, BT becerilerine sahip daha az personel bulunmaktadır. Sosyal faktörler, yeni teknolojilerin uygulanması üzerinde önemli bir etkiye sahiptir. Planlama, kaynakların kullanılması ve olumlu yönetim

abaları, gelecekte Libya'yı geliřmiř lkelerle birlikte koyabilir. Altyapı hala geliřmektedir ve řehirlerarasındaki geniř alan nedeniyle elektrik ve internet istasyonlarının eksiklięi, gney ve kuzey arasındaki iletiřim gibi elektrik ve internet istasyonları eksiklięi gibi yapılması gereken iřlemler bulunmaktadır. Libya’da grlen e-Devlet uygulamaları ulusal kimlik kartı zerine verilen hizmetlerdir. Ayrıca, Libya iin e-Devlet hizmetlerinin uygulanmasındaki zorluklar zerine bir alıřma yapılmıřtır. alıřmada Libya’nın okuryazar oranının yksek olduęu ancak insanların bilgi teknolojileri alanında eksik yeteneklere sahip olduęu vurgulanmıř ve e-Devlet zerine yapılan yeniliklerin iletiřim alt yapısı alanında ok yeni olduęunu ve yeni teknolojik alt yapıların yksek maliyet gerektirdięi sylenmiřtir. e-Devlet hizmetlerinin nnde beliren zorlukların ařılması iin

- Ulusal birlięi ve ok eřitli toplumlar arasında kapsamlı bir anlayıřı saęlamak
- Teknik alt yapı iin hazırlık yapılması
- Kamu hizmet kanun ve ynetmeliklerin aktivasyonunun saęlanması
- zel ve devlet sektrleri arasındaki iřbirlięinin oluřturulması
- Eęitim programları ve eęitim sisteminde derinlemesine bir reformun saęlaması
- Ekonomiye yeniden yapılandırma ve sanayiye ve ihracata teřviki desteklięi
- lke kaynaklarının verimli ynetiminin saęlanması
- Sanayi iřletmelerinin kurulması
- Teknik ve altyapıya gre yeterlilik ilkesi
- zel sektrn gereksinimlerini saęlamak
- Her trl yolsuzluk ve idari ařırılıkları mcadele
- Beceri ve yetkinlikleri olan insanlar iin st dzey liderlik pozisyonlarına hak yetkinlik ve sorumluluk ve ncelik ilkesinin uygulanması gerektięi sonucuna ulařılmıřtır (Elsteel, 2017).

3.2.6. Grcistan

Grcistan Hkmeti, Grcistan kamu ynetim sisteminin řeffaflıęını, verimlilięini, etkinlięini ve hesap verebilirlięini arttırmayı ve saęlamayı amalamaktadır, bu nedenle 2004'ten beri e-Devletle ilgili birka giriřim ve proje geliřtirip uygulamaktadır. Bu uygulamaların temel amalarından biri de kamu ynetimi

içerisinde Bilgi ve İletişim Teknolojilerini tanıtmak ve Gürcistan Kamu İdaresi genelinde e-Devlet girişimlerini geliştirmek olmuştur. Uygulamalı hükümet girişimleri sırasında Gürcistan'ın ana amaçları vatandaşlarına daha iyi hizmet sunmak, hizmet sunumu sırasında müşterilerin memnuniyetini artırmak ve şeffaflığı sağlamaktır (Chaligava, 2018).

Gürcistan günümüze kadar bağımsızlığını kazandığından bu yana Gürcistan Hükümeti tarafından birkaç kamu yönetimi reformu başlatılmış ve gerçekleştirilmiştir. Gürcistan hükümeti tarafından ilan edilen reformlar hemen hemen tüm devlet kurumlarıyla ilgili ve tüm devlet alanlarını kapsamaktaydı, ancak, Gürcistan Cumhuriyeti'nin bağımsızlığının ilk yıllarının çarpıcı biçimde karmaşık olduğu ve ülkedeki bazı önemli değişikliklere rağmen hala kritik sosyal ve ekonomik sorunlardan muzdariptir. Kamu kurumları verimsiz bir şekilde işletiliyordu ve genel yönetim sistemi kamu ihtiyaçlarına ve çıkarlarına odaklanmadı, hükümet sistemi yüksek merkezi bir modelle, dolayısıyla da yerel yönetimlerin faaliyeti düşük verimlilikle nitelendirilmekteydi. Söz konusu dönemde devlet sadece işverendi ve bu gerçek kamu sektöründe kayırmacılık ve yolsuzluğa yol açtı. 2003 yılına kadar göze çarpan bazı değişikliklere rağmen, sosyal ve ekonomik sorunlar hala çözülmeden kaldı. 2003'ten beri kamu yönetimi sistemi için yeni bir dönem başlamıştır. Gürcistan Hükümeti, kamu sektörünün esnekliğini, etkinliğini ve verimliliğini sağlamak ve arttırmak, yolsuzluk vakalarını en aza indirmek, ilgili yasal ve normatif temelleri geliştirmek ve hükümet faaliyetlerinin şeffaflığını artırmak için kamu yönetim sisteminin aktif ve radikal reformlarını ilan etti ve başlattı. Gürcistan hükümetinin BT altyapısının önemi ve gerekliliğinin farkında olduğu ve desteklemek için optimize edilmiş bir BT altyapısı oluşturmak için çok çalıştığı söylenebilir. Aynı zamanda Gürcistan bilişim altyapısının inşasını desteklemek için gerekli kamu politika ve yönetmeliklerini geliştirip kurulmuştur.

Bu gelişmeleri aşağıdaki şekilde sıralanır (Al-Ameri,2017):

- Ortak yazılım tabanlarının geliştirilmesi, kurumlar arasında daha hızlı bir belgelendirme paylaşım süreci sağlayabilir ve devlet kurumları arasında bilgi alışverişini artırabilir. Sonuç olarak, devlet kurumları arasında daha iyi iletişim sağlayacak ve kamu kurumları arasındaki etkileşim modelini teşvik edecektir.

- Kurumsal olarak nitelendirilen açık verilerin proaktif yayın politikası kamu kurumlarının daha iyi elektronik şeffaflığını sağlayacaktır.
- Vatandaşların tüm idari organlarla bağlantı kurmasını sağlayacak ayrı bir web sitesi oluşturulması, ayrıca elektronik inceleme ve uygulamaların yapılmasını sağlayacaktır.
- Hizmetin herhangi bir açıklama olmadan otomatik olarak oluşturulması ve gerçekleştirilmesi durumunda bazı proaktif hizmetlerin tanıtılması ve geliştirilmesi, bürokratikleşme ve basitleştirilmiş devlet hizmetlerini sağlayabilir.

3.2.7. Bahreyn

Bahreyn, 2003 yılında e-Devlet dünya sıralamasında 46 olarak güçlü bir şekilde başlamıştır. 2010 ve 2014 yıllarında yirmi e-Devlet lideri listesinde yer alan Bahreyn, küçük bir alana sahiptir ve nüfusu 1.25 milyonu geçmeyen çok zengin bir ülke konumundadır. BİT altyapısını inşa etmiş ve İnternet ve bilgisayarları vatandaşlar için sübvans edilmiş fiyatlarla dağıtmıştır. e-Devlet bazında yakın gelecekte Bahreyn'in en iyi 20 ülke arasında bulunması beklenmektedir (Saadi,& Almahjoub, 2012).

3.2.8. Libya

Libya için e-Devlet hizmetlerinin uygulanmasındaki zorluklar üzerine bir çalışma yapılmıştır. Libya'nın okuryazar oranının yüksek olduğu ancak insanların bilgi teknolojileri alanında eksik yeteneklere sahip olduğu vurgulanmış ve e-Devlet üzerine yapılan yeniliklerin iletişim alt yapısı alanında çok yeni olduğunu ve yeni teknolojik alt yapıların yüksek maliyet gerektirdiği söylenmiştir. e-Devlet hizmetlerinin önünde beliren zorlukların aşılması için

- Ulusal birliği ve çok çeşitli toplumlar arasında kapsamlı bir anlayışı sağlamak
- Teknik alt yapı için hazırlık yapılması
- Kamu hizmet kanun ve yönetmeliklerin aktivasyonunun sağlanması
- Özel ve devlet sektörleri arasındaki işbirliğinin oluşturulması
- Eğitim programları ve eğitim sisteminde derinlemesine bir reformun sağlanması
- Ekonomiyi yeniden yapılandırma ve sanayiye ve ihracata teşviki destekliği
- Ülke kaynaklarının verimli yönetiminin sağlanması

- Sanayi işletmelerinin kurulması
- Teknik ve altyapıya göre yeterlilik ilkesi
- Özel sektörün gereksinimlerini sağlamak
- Her türlü yolsuzluk ve idari aşırılıkları mücadele
- Beceri ve yetkinlikleri olan insanlar için üst düzey liderlik pozisyonlarına hak yetkinlik ve sorumluluk ve öncelik ilkesinin uygulanması

gerektiği sonucuna ulaşılmıştır (Elsteel, 2017).

3.3. Türkiye’de e-Devlet Uygulamaları Tarihsel Perspektifi

Ülkemizde e-Devlet sürecine geçiş 1980’li yılların ikinci yarısından itibaren ortaya çıkmıştır. Bu gelişim ülkemizde bilişim ve teknoloji alanındaki hizmetleri sorgulayan politikalar sonucunda başlamıştır. Bu politikaların temel amacı mevcut yapıyı irdelemek ve geçiş alt yapısını değerlendirmektir. e-Devlet kavramı 1990’lı yılların başında bilişim alt yapısına uygulanan yatırımlar ile kendini göstermiştir. Bu yatırımlar ile bilgisayar ve internet kullanım oranında büyük artış gözlenmiştir. Bu gelişme beraberinde ülkemizde bazı devlet kurumlarının erişimlerini sanal ortama taşımaları ile devam etmiştir. 2000’li yıllarda ülkemizdeki e-Devlet uygulamaları ülke politikası içinde yer alarak yaygın bir şekilde uygulama alanı bulmuştur. Çeşitli platformlarda uygulanan plan ve projeler ile farklı kurumlar e-Hizmet sürecine geçiş yapmaya başlamıştır. Özellikle 2006 ve sonrasında hızlı bir şekilde kurumlar uygulama sürecine geçmişlerdir. 2008-Aralık ayında e-Devlet Kapısı Projesi ile e-Hizmet süreci tek noktadan kontrol ile aktif bir şekilde uygulanmaya başlamıştır. Günümüzde “www.türkiye.gov.tr” adresi kullanılarak tek noktadan çoklu hizmet anlayışı benimsenmiş, pek çok işlem hızlı ve düşük maliyetli bir şekilde insanların kullanımına sunulmuştur (Kızıldağ, 2011).

3.4. Türkiye’de Yaygın Olarak Kullanılan e-Hizmetler

Ülkemizde e-Hizmetler başlığı altında yer alan uygulamalar aşağıda verilen başlıklar ile sunulmuştur.

- **Eğitim:** Ülkemizde eğitim veren kuruluşların kayıt, burs, sınav işlemleri gibi hizmetler
- **Kariyer:** Çalışanlar ve işletmelerin ihtiyaç duyacağı bilgi ve hizmetler
- **Sağlık:** Kişisel sağlık hizmetleri

- **Şikâyet ve Bilgi Edinme:** Devlet kurumları ve ticari işletmeler ile ilgili talep ve şikâyet hizmetleri
- **Trafik:** Kara, deniz ve hava taşımacılığı ile ilgili hizmetler
- **Sosyal Güvenlik ve Sigorta:** Sigorta, sosyal güvenlik e-Yardım ile ilgili hizmetler
- **Telekomünikasyon:** İletişim kaynaklarına erişim ve kullanım hizmetleri
- **Vergi, Harç ve Cezalar:** Ceza, vergi ve harç bilgileri için bireysel sorgulama ve takip hizmetleri
- **Kişisel Bilgiler:** Bireysel takibi sağlanan hizmetler
- **Adalet:** Adli işlemler ve dava detay bilgilerine erişim hizmetleri
- **Çevre, Tarım ve Hayvancılık:** Tarım, hayvancılık ve çevre ile ilgili bilgi edinme hizmetleri
- **Mevzuat:** Mevzuat, ihaleler ve seçmenler hakkında bilgi edinme hizmetleri

Bu hizmetler Şekil 11’de verilmiştir.



Şekil 11. Türkiye’de Resmi Kurumların Sunduğu e-Hizmetler (e-Devlet, 2019)

3.4.1. e-Nabız

Sağlık alanında bilgilerin güvenliğinin sağlanması yasal bir zorunluluktur. Üçüncü şahısların eline geçmemesi gereken sağlık verileri ülkemizde e-Nabız sistemi kullanılarak işlenmektedir. Bu sistem insanların tüm sağlık verilerini analiz etmekle kalmayıp bu verilerin depolanmasını da sağlamaktadır. Bu sistem aracılığı ile doktor hastasının tüm geçmiş sağlık verilerine ulaşabilmektedir. e-Nabız sisteminde kişisel verilerin korunması hususunda hastanın doktorlar ile paylaşacağı veriyi hastanın tercihi bırakmış olması önemli bir husustur. Bu uygulama ile hasta istediği doktor ile

geçmiş sağlık verilerini paylaşabilmektedir. Aynı zamanda e-Nabız sisteminde tüm veriler hasta mahremiyetine uygun bir şekilde şifrelenerek saklanmaktadır. Sağlık verisini üreten sunucu ile hizmeti alan bireyler arasında güvenli iletişim protokolleri oluşturularak amaçlanan verinin sadece muhatabı tarafından görülmesinin sağlanması sistemin bir diğer avantajı olarak görülmektedir (e-Nabız, 2019).

3.4.2. UYAP

Bu proje Adalet Bakanlığı tarafından yürütülmektedir. Projenin temel amacı adalet sisteminde yer alan faaliyetlerin sanal ortamda yürütülmesini sağlamaktır. Böylelikle yargı sürecindeki verilerin sanallaştırılması ile hızlı ve etkili çözümün bulunmasına olanak tanınmıştır. UYAP ülkemizde adalet sistemi içerisinde yer alan tüm ögelerin tek bir noktadan kontrol edilmesini sağlamaktadır. UYAP sisteminin elektronik ortamdaki bazı yaygın avantajları aşağıdaki gibi sıralanabilir:

- İlgili belgeye erişme
- Sonuçların yayınlanması
- Sorgulama işlemlerinin hızlı bir şekilde sunulması

UYAP sistemi ile kullanıcıların yaptığı işlemler kayıt altında tutulmaktadır. Böylelikle hangi kullanıcının hangi saatte ne yaptığı kayıtlardan gözlenebilir. Aynı zamanda kullanıcı yetkilendirmesi sağlanarak kullanıcı bazlı izinler verilebilmektedir. UYAP sayısal imza ve kriptolojik özet fonksiyonları kullanarak verilerin güvenliğini ve bütünlüğünü koruma alt yapısına sahiptir. Böylelikle UYAP sistemi içerisinde yer alan bilgiler şifrelenerek saklanır ve sadece sayısal imzası uyuşan kişiler için verilere erişim sağlanır (Uyap, 2019).

3.4.3. MERNİS

Vatandaşların devlet nezdinde tanınmasını sağlayan ve kullanıcı kayıtlarının tutulduğu sisteme MERNİS denilmektedir. Ülkemizde vatandaşların nüfus kayıt sisteminde kayıt altına alınması hususu, 3152 sayılı kanunla İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri'ne verilmiştir. Bu amaçla Türkiye'de her bireye kendini eşsiz bir birey olarak tanıtmaya ve kimliğini teyit etmesi için Türkiye Cumhuriyeti kimlik numarası verme uygulamasına geçilmiştir. Böylelikle her birey kamu kurum ve kuruluşlarında kendisini kolay ve sorunsuz bir şekilde teyit etmektedir. Bu uygulama ile insanlar Türkiye Cumhuriyeti kimlik numarası ile işlemlerini hızlı bir şekilde

gerçekleştirmektedirler. MERNİS sisteminde bilgi güvenliğinin sağlanması için birçok şifreleme yöntemi kullanılmaktadır. Burada açık anahtar tabanlı şifreleme sistemleri, simetrik şifreleme sistemleri ve özet fonksiyonları kullanılmaktadır. Bu yöntemler aracılığı ile bir güvenlik protokolü kullanılmakta ve bu güvenlik protokolü sayesinde sistem güvenliği sağlanmaktadır (Mernis, 2019).

3.4.4. e-Eğitim

e-Eğitim genel olarak uzaktan eğitim kavramı ile birlikte kullanılmaktadır ve MEB'in e-Eğitim tabanlı projeleri gün geçtikçe artmaktadır. e-Eğitim tabanlı sistemlerin güvenliği genel olarak kimlik doğrulama tabanlı oluşturulmaktadır. Ancak bu sistemler web üzerinden hizmet verdikleri için, web için sıklıkla kullanılan güvenlik protokolleri aracılığı ile e-Eğitim sisteminin güvenliği sağlanmaktadır (e-Eğitim, 2019).

3.4.5. e-Vergi

İnteraktif vergi dairesi sistemi kullanılarak internet üzerinden vergi ödemeleri gerçekleştirilmektedir. Bu uygulama hem web üzerinden kullanılabilen hem de mobil uygulamaları olan bir sistemdir. Bu tür sistemlerin bilgi güvenliğinin sağlanması için web ve mobil tabanlı güvenlik protokolleri kullanılmaktadır (e-Vergi, 2019).

Yukarıda açıklanan elektronik hizmetlerin yaygın olarak kullanılabilmesi ve e-Devlet yapısının gelişiminin olgunlaşması için güven faktörünün sağlanması çok önemlidir. Bu nedenle, günümüzde e-Hizmetler ile ilgili pek çok farklı şifreleme algoritmaları ve güvenlik protokolleri geliştirilmiştir. Bu protokollerin temel mantığında şifreleme prosedürleri yatmaktadır. Şifreleme işleminin özünde ise bilgi güvenliğini sağlamak gelmektedir. Farklı şifreleme algoritmaları ile e-Hizmetlerde yer alan uygulamaların özellikle veri tabanlarının şifrelenerek saklanması ve muhafaza edilmesi gerekir. Bu prosedür uygulamalarda iki farklı formda oluşturulmaktadır. Bunlardan birincisi veritabanındaki ilgili alanın yönetici pozisyonunda olan kullanıcılara bile görünmez olmasıdır. Bir diğeri ise veritabanının bütünüyle şifrelenmesidir. Ancak bu prosedürlere rağmen sanal ortamda bulunan veriler siber saldırılara açık olabilmektedir. Bu açığın kapatılabilmesi için:

- Alanında uzman kişilerin kritik görevlere getirilmesi
- Kritik görevlerde yer alan kişilerin sürekli eğitim almaları
- Son teknolojilerin takip edilmesi ve sistemlere uygulanması

- Verilerin belirli aralıklar ile yedeklenmesi
 gelmektedir. Bununla beraber hukuksal açıdan bilgi güvenliği kanunlarının düzenlenmesi ve caydırıcı olması sağlanmalıdır (e-Vergi, 2019).

3.5. Taşrada Kullanılan e-Devlet Uygulamaları

İl bazında e-Devlet uygulamaları İl Valilik ve Belediye siteleri incelendiğinde Tablo 3. ve Tablo 4.' de verilen hizmetler sıralanmaktadır. Türkiye genelinde kullanılan uygulamalar Elazığ ilinde de kullanılmaktadır. Tablo 3.'de valiliğin elektronik uygulama tabanlı hizmetleri listelenmektedir. Bu uygulamalar sayesinde vatandaşlar taşra hizmetlerinden faydalanmaktadır. Valilik genel olarak muhtar bilgi sistemi, Cimer, işçileri bakanlığı hizmetleri ve yasalarla ilgili uygulama hizmetlerini vermektedir.

Tablo 3. Elazığ Valiliğinin Kullandığı e-Uygulamalar (Elazığ Valiliği, 2019)

Valilik	
1	Muhtar Bilgi Sistemi
2	e-Devlet
3	Cimer
4	e-İçişleri
5	e-Mevzuat
6	e-Genelge
7	Resmi Gazete
8	e-Arşiv
9	MERNİS
10	Türkiye İstatistik Kurumu
11	Türkiye İş Kurumu

Belediyenin elektronik uygulamalarında ise çevrimiçi yapılabilecek belediye hizmetleri sunulmaktadır. Ayrıca her vatandaşın temel hakkı bilgi edinme hizmetleri de sunulmaktadır. Beyaz masa, nöbetçi eczane uygulaması ve e-Ödeme sistemleri bunlar

arasında en sık kullanılanlarıdır. Belediye tarafından sağlanan elektronik uygulamalar ise Tablo 4’ de listelenmiştir.

Tablo 4. Elazığ Belediyesinin Kullandığı e-Uygulamalar (Elazığ Belediyesi, 2019)

Belediye	
1	e-Ödeme
2	e-Makbuz
3	Borç Sorgula Öde
4	Meclis Gündem Kararları
5	e-Sayaç
6	Beyaz Masa
7	Bilgi Edinme
8	Evrak Sorgula
9	İhale ve Doğrudan Teminler
10	Hal Fiyatları
11	Nöbetçi Eczane
12	Hava Durumu
13	Vefat Edenler

u uygulamalar Tablo 3 ve Tablo 4 incelendiğinde, listelenen elektronik uygulamalar Türkiye genelinde kullanılan uygulamalardır. Genel olarak büyük şehirlerin siteleri incelendiğinde e-Ulaşım, aski, ego, engelli hizmetleri, yaşlı destek hizmetleri, spor hizmetleri, yeme içme ve alışveriş gibi özel uygulamalarda geliştirilmiştir. Elazığ gibi orta çaplı şehirlerde genel uygulamalar dışındaki uygulamalar çok fazla kullanılmamaktadır.

3.6. Türkiye’de 2016-2019 Ulusal e-Devlet Strateji ve Eylem Planı

Ülkemizde 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı geliştirilmiş ve e-Devlet vizyonu, temel değerleri, stratejik amaçları ve hedefleri bu eylem planı ile tanımlanmıştır. Bu planda, Türkiye’nin e-Devlet alanındaki hizmetlerinin geliştirilmesi ve kullanıcı açısından yaygınlaştırılması amaçlanmıştır. Bu amaç paralelinde e-Devlet politikasının geliştirilmesi için yol haritası çizilmiş ve bu planda bilgi güvenliği

farkındalığının artırılmasına büyük önem verilmiştir. Bu eylem planının temel hedefleri aşağıda sıralanmıştır (Eylem Planı, 2016-2019):

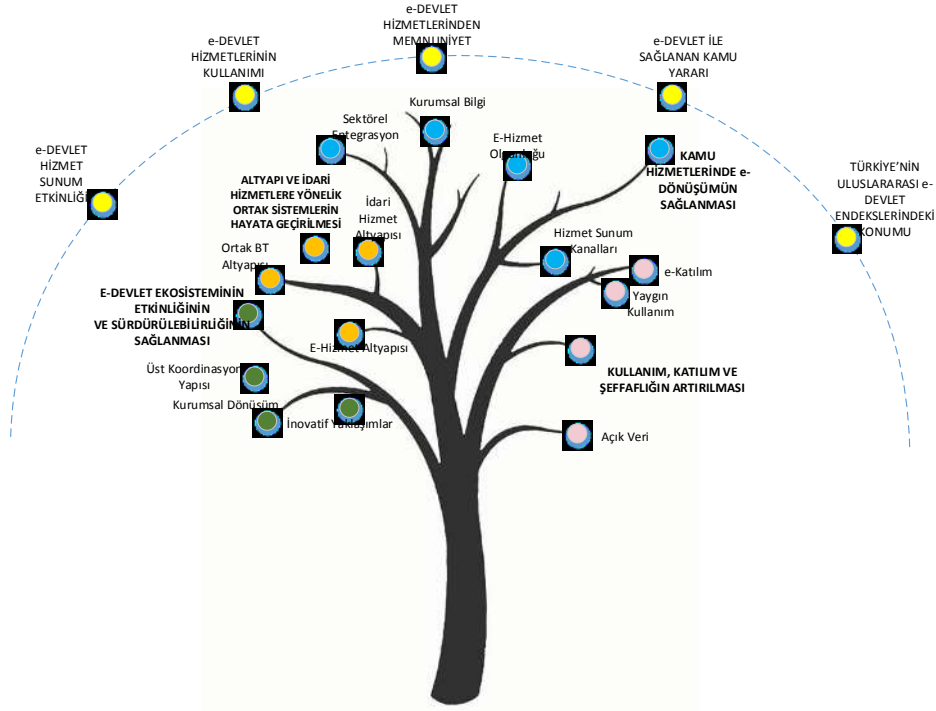
1. Ülkemizin devlet ve kamu kurumlarındaki hizmet seviyesini üst düzeye çıkarmak
2. Alınacak hizmetin mümkün olduğunca zaman ve mekândan bağımsız hale getirmek
3. Gelişen teknoloji paralelinde küresel bir yapı oluşturmak
4. Toplumun yaşam kalitesinin üst düzeye çıkarmak
5. e-Devlet uygulamalarının tek merkezden kontrolünü ve güvenliğini sağlamak
6. Ülkemize özgü etkin, aktif ve güvenli bir sistem alt yapısı oluşturmak

Bu plan Türkiye'nin ilk kapsamlı ulusal e-Devlet stratejisi ve eylem planıdır. Bu plan oluşturulurken dünyadaki mevcut e-Devlet örnekleri incelenmiştir. Bu inceleme dünyada e-Devlet gelişmişlik düzeylerine göre üst sıralarda yer alan ülkeler dikkate alınarak gerçekleştirilmiştir. Eylem planı oluşturulurken bu ülkelerin (Güney Kore, Avustralya, Singapur, Fransa, Amerika Birleşik Devletleri, İngiltere, Estonya, Malezya)

e-Devlet uygulamaları, kullanım oranları ve eğilim analizleri göz önünde bulundurulmuştur.

Eylem planı hazırlanırken tümdengelim ve tümevarım yöntemleri birlikte kullanılmıştır. Dünyada gerçekleştirilen uygulamalar ve eğilimler baz alınarak temel gereksinimler Tümdengelim yöntemi ile oluşturulmuştur. Durum analizi, sınıflandırmalar, tespitler, eylemler, hedefler ve stratejik amaçlar tümevarım yöntemi ile hazırlanmıştır. Yürütülen çalışmalarda da mevcut durum analizi sonucunda elde edilen tespitler sınıflandırılmış, tespitler gerekçelere dönüştürülmüş, gerekçelerden yola çıkılarak aday eylemler, hedefler ve stratejik amaçlar tanımlanmıştır. Oluşacak yeni durumların değerlendirilmesi ve eş zamanlı geri dönüş alınması ile eylem planının her zaman güncel tutulması amaçlanmaktadır.

Şekil 16' da e-Devlet ekosistem yapısını anlatan bir ağaç verilmiştir. e-Devlet yaşayan bir sistemdir. Bu sebepten dolayı bir yaşam döngüsü vardır ayrıca bu sistem birçok alt modülden oluşan bir ekosistemi ifade etmektedir. e-Devletin sosyal hayattaki kaliteyi arttırabilmesi için ekosistemin etkin ve sağlıklı bir şekilde işletilmesi gerekmektedir (Eylem Planı, 2016-2019).

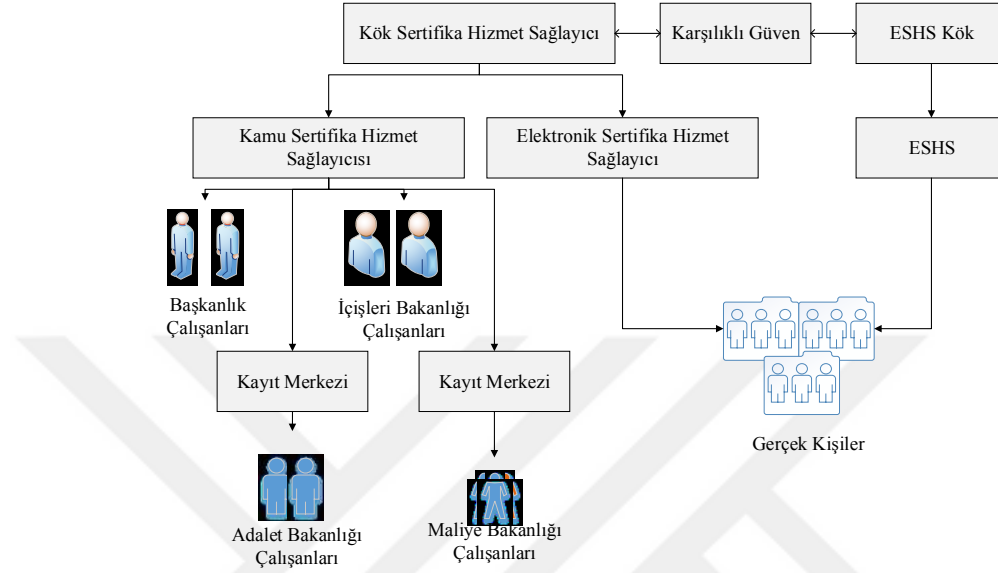


Şekil 12. Etkin e-Devlet Ekosistemi (Eylem Planı, 2016-2019)

3.7. e-Devlet Uygulamalarının Güvenlik Alt Yapıları ve Analizi

Bu uygulamalarda simetrik, asimetrik ve anahtarsız şifreleme yöntemleri kullanılmaktadır. Simetrik şifreleme yöntemleri insanlık tarihi kadar eski yöntemlerdir ancak bu tür yöntemlerin en önemli kusuru, şifreleyen taraf ve şifre çözen tarafın aynı anahtarı kullanmasıdır. Bu problemin çözülebilmesi için 1970'li yılların başlarında matematiksel modeller kullanılarak anahtar değişimi yöntemleri önerilmiştir. Bu yöntemlerin en çok bilineni ve en fazla kullanılanı RSA yöntemidir. RSA yöntemi sonlu cisim teoremi kullanan basit bir yöntemdir. Üst alma ve mod işlemlerini kullanarak şifreleme ve anahtar değiştirme görevlerini yerine getirir. Asimetrik şifreleme sistemlerinde açık anahtar ve gizli anahtar olmak üzere iki tür anahtar yapısı kullanılmaktadır. Açık anahtar herkes tarafından bilinirken, gizli anahtar sadece onu kullanan birey tarafından bilinir. Asimetrik şifreleme sistemlerinin gelişmesiyle birlikte e-İmza şemaları ortaya çıkmıştır. e-İmza şemaları kullanılarak kişisel veriler kriptolojik protokoller kullanılarak doğrulanmaktadır. e-İmza şemalarının güvenliğini tamamıyla sağlayabilmek için sertifika hizmet sağlayıcılar kullanılmaktadır. Sertifika sistemi, bilgi güvenliğinin en zayıf parçası olan insanı, anahtar belirleme işleminde devre dışı bırakmak için kullanılmaktadır. Hatta bu amaçla fiziksel imzalar kullanılmaktadır.

Fiziksel imzalar bir USB cihazı (kart okuyucu) ve bir akıllı karttan oluşmaktadır. Bu sistemi kullanmak için bilgisayara basit bir uygulama kurulur ve web tabanlı uygulamalarda e-İmza sistemi kullanılır. e- İmzanın blok diyagramı Şekil 17'deki gibidir (BM, 2019).



Şekil 13. e-İmza Altyapısının Blok Diyagramı (Desa, 2019).

Şekil 17' de ESHS: Elektronik Sertifika Hizmet Sağlayıcısıdır. Burada en önemli kısım ESHS'in güvenilir olmasıdır. Çünkü bu protokol ESHS'nin güvenilir olduğunu varsayarak kriptolojik işlemleri gerçekleştirmektedir.

Özellikle, e-Devlet gibi uygulamalarda çok seviyeli güvenlik protokolleri kullanılmaktadır. Bu tür sistemlerin internet güvenliğini sağlayabilmek için GSK (Secure Güvenilir Soket Katmanı) kullanılmaktadır. Bu protokolda anahtar üretmek için e-İmzadaki gibi güvenilir sertifika yöneticileri kullanılır. Kullanıcı tarafı güvenlik e-İmza yapılarıyla, internet güvenliği GSK-TLS gibi güvenilir bağlantılarla sağlanır. Ayrıca e-Devlet uygulamasının kullanıcılar için parola tabanlı, mobil imza tabanlı, e-İmza tabanlı, kimlik kartı tabanlı ve internet bankacılığı tabanlı kimlik doğrulama seçenekleri bulunmaktadır. Bunların yanı sıra bu tür sistemlere sürekli sızma testleri uygulanmakta ve açıkları beyaz şapkalı bilgisayar korsanları tarafından listelenerek mevcut açıklar kapatılmaktadır (Coleman, 1994).

3.8. Bilişim Suçları ve İlgili Mevzuatlar

e-Devletin yaygınlaştırılması ve içselleştirilmesi için bilişim hukuku alt yapısının oluşturulması hayati önem arz etmektedir. e-Devlet uygulamalarında temellerini oluşturan bilgi güvenliği önlemlerinden birisi de elektronik imza uygulamasıdır. Bu nedenle hem e-Devlet hem de saldırılara karşı hukuki altyapının oluşturulması gerekliliği ortaya konmuştur (Arifoğlu vd., 2002).

Günümüzde önemli bilgileri çoğu sayısal ortamda depolanmaktadır. Bu bilgilere yetkisiz erişimin sağlanması, bilgisayar korsanlığının artması ve bilgilerin çalınması gibi sebeplerden dolayı bilişim hukuku adı verilen yeni bir kavram ortaya çıkmıştır. Bilişim hukuku, sayısal verilerin erişimini konusu üzerinde çalışan hukuk dalıdır. Bilişim hukuku, bilişim sistemlerinin yaygın olarak kullanılması sonucu birçok alt dala sahiptir. Ayrıca bilişim hukuku ve bilişim suçlarını temel alan ve bu alanda mühendis yetiştiren Adli Bilişim Mühendisliği adında bir alan da mevcuttur. Bilişim Hukuku ise Bilgi Teknolojisi Hukuku ve İnternet Hukuku başlıkları altında ikiye ayrılarak incelenmesi gerekir (Avşar & Öngören, 2010).

Günümüzde en çok kullanılan iletişim aracı internettir. İnternetin kullanımına ilişkin yasal düzenlemeler ise internet hukukunun konusu olarak yer almaktadır. İnternet üzerinden yapılan yayınlar, yayınların gizliliği ve yayınlardaki ifadelerin özgürlüğü internet hukuku kapsamında değerlendirilmektedir.

Bilgi Teknolojisi Hukuku hem dijital hale getirilmiş bilginin hem de bilgisayar programlarının dağıtılması ile ilgili hükümleri düzenler. Bilgi güvenliğinin sağlanması ve e-Ticaret konularında düzenlemeler içerir. İnternet Hukuku, İnternet'in kullanılması ile ortaya çıkan hukuki meseleleri inceler. İnternet Hukukunun hukukun birçok alanı ile etkileşim içerisinde bulunması gerekir. İnternet erişimi ve kullanımı, güvenlik, ifade özgürlüğü ve yargılama gibi hukukun diğer alanları ile ilişkilidir.

Bilişim suçları 6 ana bölümde incelenmektedir ve bu bölümler aşağıdaki gibidir:

- Bilgisayar sistemleri ve servislerine yetkisiz erişim ve bu sistemleri dinleme
- Bilgisayar sistemlerinin sabotajı
- Bilgisayar sistemleri ve bilişim teknolojilerini kullanarak dolandırıcılık yapma
- Bilgisayar sistemleri ve bilişim teknolojilerini kullanarak sahtecilik yapma
- Fikri mülkiyet hakkı kanunu tarafından korunan ticari bir yazılımın yama dosyaları yardımıyla ücret ödmeden kullanmak

- Bilişim teknoloji kullanılarak işlenen diğer suçlar.

Sömürme ve bilgisayar korsanlığı araçlarının gelişmesiyle birlikte, çok fazla bilgiye sahip olmayan kullanıcılar dahi bilişim suçlarını rahatlıkla işleyebilmektedir (Sınar, 2001). En sık görülen bilgisayar suçları ise aşağıdaki gibidir:

Yetkisiz erişim, bir bilişim sistemine yetkisiz girme, verileri izinsiz bir şekilde kopyalama ve dinleme gibi suçlardır.

Yetkisiz erişim saldırısı algılanması en zor saldırdır çünkü saldırgan bu saldırıyı yaparken sisteme herhangi bir zarar sadece sistemde var olan sayısal bilgilere odaklanarak onları elde etmeye çalışır (Demir, 2000).

Hedef sisteme zarar verme ve sistemi engelleme, bu saldırının temel amacı sistemi devre dışı bırakmak ve sisteme hasar vermektir. En sık kullanılan saldırılardan birisidir. Özellikle internet veri iletişim bandı yüksek olan saldırganlar birçok sistemi servis dışı bırakabilmektedir. Bu durumda maddi kayıplara sebebiyet vermektedir.

Özellikle kritik alt yapılara bu atak sıklıkla uygulanmaktadır. Buradaki temel amaç vatandaşların kritik sistemlerden hizmet almasını engelleyip devletlerin ve bireylerin mağdur edilmesidir. Bu tür ataklar genel olarak internet veri iletişim bandının geniş olduğu ülkelere dar veri bandına sahip olan ülkelere yapılmaktadır. Bu sebepten dolayı birçok ülkenin güvenlik konseyinde, kritik alt yapılara yapılacak bu tür ataklar savaş sebebi sayılmaktadır (Demir, 2000).

Değiştirme saldırısının temel amacı yetkili kullanıcıya gönderilen verileri manipüle etmektir. Böylece kullanıcı gerçek veriler yerine değiştirilmiş verilere erişecektir. Değiştirilen veriler ise şu şekildedir. Statik (depolanmış) veri, yazılım kodları ve iletim hattındaki verilerdir (Demir, 2000).

Üretim saldırısı, değiştirme saldırısında benzerdir ancak aradaki tek fark gönderici bir veri göndermeden saldırgan ürettiği veriler alıcı tarafa gönderilir.

Yukarıda bahsedilen saldırıları kullanmak için genellikle zararlı yazılımlar kullanılmaktadır. Zararlı yazılımlar Truva atı, virüsler, ağ solucanları, casus yazılımlar, mantık bombaları, şifre kırıcılar, ağ kollarıcıları, zafiyet avcılar ve şantaj yazılımları olarak sınıflandırılmaktadır. Kurumsal ve bireysel uygulamalar sayılan zararlı yazılımlar kullanılarak zarara uğratılmaktadır. Türkiye’de özel olarak bir bilişim kanunu yoktur ancak bilişim suçlarıyla ilgili kanunlar TCK’nın ilgili maddeleriyle karara bağlanmaktadır. Bu maddeler aşağıda verilmiştir (Demir, 2000):

3.8.1. Bilişim Alanındaki Suçlar

Dünya’ da ve Türkiye’ de bilişim suçlarının artmasıyla birlikte bu suçların cezalandırılmasıyla ilgili yasal düzenlemelerin yapılması zorunluluğu ortaya çıkmıştır. Bilişim suçlarıyla ilgili cezalandırmalar ve hükümler 5237 sayılı TCK ile karara bağlanmıştır. 5237 sayılı TCK, Türk Hukuk sisteminin ceza sistemini belirlemekte ve toplumsal huzuru tesis ederek suçun işlenmesine karşı caydırıcı bir rol üstlenmektedir. Bu rolü bilişim sistemlerinde de yerine getirmek ve siber dünyada işlenecek suçların önüne geçmek için bir takım kararlar yer almaktadır. Bu kararlar 5237 sayılı TCK’nin 10. Bölümünde yer alan bilişim alanında suçlar başlığı altında karara bağlanmıştır ve bu bölümde bahsedilen temel maddeler sırasıyla Madde 243, 244 ve 245’tir. Madde 243 şu şekilde tanımlanmıştır. “Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir. Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir. Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.”. Bu madde kapsamında 5237 TCK bilişim teknolojisi sistemlerine yetkisiz erişimde bulunmak isteyen saldırganların ceza çerçevesini tanımlamıştır (TCK, 2019).

3.8.2. Bilgisayar Korsanlığı

“Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır. Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve 5000 güne kadar adli para cezasına hükmolunur”. Madde 244’ te bilgisayar korsanlığı kavramından bahsedilmiştir ve bu 5000 güne kadar cezalandırılmasını hükmetmiştir (TCK, 2019).

3.8.3. Dolandırıcılığın Nitelikli Hali: Bilişim Sistemlerini Yetkisiz Kullanma

“Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adli para cezası ile cezalandırılır. Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır” ifadesi ile Türkiye’de sık karşılan bilişim suçu kredi kartı dolandırıcılığının cezası belirtilmektedir. Bu sebepten dolayı Madde 245’de kredi kartının dolandırıcılığıyla ilgili cezai işlemleri tanımlamaktadır (TCK, 2019).

5237 Sayılı Türk Ceza Kanunu’nun 246. maddesi “bilişim sistemlerine girme”, “sistemi engelleme, bozma verileri yok etme veya değiştirme”, “banka veya kredi kartlarının kötüye kullanılması” suçlarının işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur şeklinde ifade edilmiştir.

Bilişim vasıtasıyla başka bir suç işlenirse TCK’nın ilgili maddesine göre hüküm verilir. Örneğin, ticari bir yazılımın izinsiz kullanılması, fikri mülkiyet hakları kanuna göre değerlendirilmektedir. Bu durum hukuksal açıdan bir problemlidir. Burada meydana gelecek yasal boşlukları kullanan bilgisayar korsanları ve suçlular kötü niyetli eylemlerini sürdürmeye devam etmektedir (Avşar & Öngören, 2010).

Bunlarla birlikte günümüzde en fazla görülen suçlardan birisi de özel hayatın gizliliğini ihlal etmedir. Bu suç genel olarak sosyal medya kullanılarak gerçekleştirilmektedir. Bireylerin arkadaşlarıyla paylaştıkları bilgiler bireyin istemediği kişilerle paylaşılmakta veya bu paylaşımlardan elde edilen bilgiler kullanılarak bireyler tehdit edilmektedir. Sosyal medyaya has bir yasanın olmaması bu tür suçların cezalandırılmayacağı manasına gelmemektedir. Bu tür durumlarda TCK’nın özel hayatın ihlali ile ilgili yasaları kullanılarak cezai işlemler yapılmaktadır.

Ayrıca 5237 sayılı TCK’nın 157. Maddesinde bilişim sistemlerini kullanarak dolandırıcılık suçunun nitelikli bir hali TCK’nın 158/1-f maddesinde düzenlenmiştir. BT kullanılarak işlenen dolandırıcılık suçlarında 5237 sayılı TCK’ da 3 yıldan 10 yıla kadar hapis ve 5000 güne kadar adli para cezası öngörülmektedir.

e-Devlet sistemleri bir devletin sahip olduđu en önemli biliřim sistemi olarak tanımlanmaktadır. Çünkü e-Devlet’ e yapılacak bir saldırı durumunda, devlet sistemi çöker ve vatandaşların özel bilgileri saldırganların eline geçer. Böyle bir durumda vergi sistemi, eğitim sistemi, nüfus sistemi gibi sistemler zarara uğrar. Hem bireysel hem de devlet olarak büyük mağduriyetler gerçekleşir. Ancak, bu tür kritik altyapılara yapılacak saldırılar ve bunların cezai hükümleriyle ilgili özel maddeler TCK’ da bulunmamaktadır. Yalnızca doğrudan e-Devlet’ e yapılacak saldırılar tüzel kişiler için oluşturulmuş güvenlik önlemlerini yasaları içermektedir çünkü e-Devlet tüzel bir kişiliktir. e-Devlet’ e doğrudan saldırı yapılması durumunda 5237 sayılı TCK’nın 246. Maddesi uyarınca cezalandırılmanın gerçekleştirilmesine karar verilir. Bu maddenin tam metni řu şekildedir. “ Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.” (TCK, 2019).

Geliřmiş ölkelerde bu tür suçlar ve bunların cezaları tanımlıyken, Türkiye’ de bu konuyla ilgili ciddi bir çalışma yapılmamaktadır (Sınar, 2001).

Biliřim suçları açısından 5237 sayılı TCK’nın temel problemi yeterince kapsamlı olmaması ve tüm biliřim suçları için sadece 3 maddenin tanımlı olmasıdır. Ayrıca, 5237 sayılı TCK’nın 2. Maddesinde yer alan “Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez ve güvenlik tedbiri uygulanamaz. Kanunda yazılı cezalardan ve güvenlik tedbirlerinden başka bir ceza ve güvenlik tedbirine hükmolunamaz.” ibaresi bilgisayar korsanlarının işin kolaylařtırmaktadır. Çünkü biliřim sistemlerine müdahale edebilmek, bu sistemleri bozabilmek için birçok saldırı tipi vardır ve bu saldırı tiplerinin çoğunda 5237 sayılı TCK’ da bahsedilmemiřtir. Örneğın, bir saldırgan e-Devlet için ayrılmış veri iletim bandını kendi verilerini iletmek için de kullanabilir. Sadece veri iletim bandını kullanmakla ilgili net bir madde bulunmadığı için saldırgan ceza almadan yaptığı işlemlere devam edebilir. Bu açıdan biliřim hukuku sistemi ele alınırsa, hukukçular, bilgisayar bilimciler ve bilgisayar korsanlarından oluşturulacak bir heyetin tüm suçları net olarak belirleyip, 5237 sayılı TCK’nın 10. Bölümünü güncellemeleri gerekmektedir. Hatta bu alanda yeni bir kanun kitapçığının çıkarılması elzem olarak yapılması gereken faaliyetler arasında yer almaktadır. Yalnızca yeni yapılan düzenlemelerle biliřim suçlarının caydırıcılığını arttırmak için cezalar ağırlaştırılmıştır. Özellikle son zamanlarda sıklıkla karşılan biliřim teknolojileri

kullanılarak dolandırıcılık eylemleri 5237 sayılı TCK'nın 158 1-f maddesine göre arttırılmıştır ve bu madde yukarıda verilmiştir.

3.9. e-Devlet Uygulamalarının Bilgi Güvenliği Alt Yapısını Güçlendirmek için Yapılması Gereken Süreçler

Yapılan çalışmalar ışığında elde edilen bulgular ise şu şekildedir. Ülkeler e-Devlet hizmetlerini sağlıklı bir şekilde işletebilmek için bilgi güvenliği ofisleri ve siber olaylara müdahale ekipleri kurmalıdırlar. Bu ofisler ve ekipler iyi bir eğitimden geçirilmelidir. Ardından, kanun koyucularla bir araya gelerek bir siber güvenlik politikası belirlemelidirler. Bu güvenlik politikası aşağıdaki süreçler zorunlu bir hale getirmelidir.

- Risk yönetiminin sürekli bir hale getirilmesi için çalışmalar yapmak.
- Gizlilik ve veri güvenliği sağlamak için sürekli çalışmaların yapılmasını teşvik etmek ve bu alanda yerli ve milli şifreleme sistemlerinin oluşturulmasını sağlayacak kararlar almak.
- Siber esneklik sağlayarak sistemlerin yeni teknolojilere adapte olmasını sağlamak.
- Güvenlik mimarisini kalıcı bir hale getirmek ve bu mimariyi yaygınlaştırmak.
- Siber güvenlik farkındalık eğitimlerini toplumun tabanına yaymak.
- e-İmza teknolojileriyle ilgili çalışmaları sürekli hale getirmek.
- Bulut ve mobil güvenlikle ilgili önlemleri arttırmak, hafif sıklet şifreleme algoritmalarının geliştirilmesini desteklemek.
- Bilgi güvenliği tatbikatlarını yurt geneline yaymak ve zayıf halkaları tespit etmek.
- Penetrasyon (sızma) testlerini yaygınlaştırmak ve sürekli hale getirmek.
- Siber felaket senaryolar oluşturmak ve senaryolar ışığında tedbirler almak.
- e-Devlet uygulamalarının daha şeffaf ve güvenilir bir hale getirilmesi için blok zinciri altyapısının entegrasyonunun uygulama bazlı sağlanmasıyla ilgili çalışmalar yapmak. Özellikle tapu kaydı gibi işlemlerde, blok zinciri kullanarak verimliliğin arttırılacağı ön görülmektedir. Ayrıca sağlık hizmetlerinde ve raporlu ilaç yazma gibi durumlarda, bu yapının sosyal güvenlik kurumunu (SGK) daha işlevsel bir yapıya dönüştüreceği ve kaçakların önlenebileceği görülmektedir.

- Bilişim suçlarının çerçevesini ve kapsamını arttırmayla ilgili çalışmalar yapmak.

Yukarıda sayılan süreçler standart haline getirilmeli ve bu standartlar Türkiye genelinde yaygınlaştırılarak, e-Devlet'in güvenliği sağlanmalıdır. Ayrıca, bu standarda tüm kamu ve özel kurumların uymasını zorunlu hale getirilmelidir.

Gelecekte e-Devlet kullanımının artacağı öngörülmektedir. Bu öngörünün en temel sebebi hızla yaygınlaşan internet ve akıllı cihaz kullanımı olarak görülmektedir. Çünkü gelecek neslin bilgisayar veya bilişim teknolojileri kullanma oryantasyon problemi bulunmamaktadır.



SONUÇ VE TARTIŞMALAR

Yerel otoritelerin sürdürülebilir kalkınmadaki rolü, en savunmasız kişilere ulaşmak için önemli olacaktır. Bu nedenle, yenilikçi katılımcı mekanizmalar aracılığıyla tüm toplumlarla yerel olarak çalışmak şarttır. Vatandaşların etkili, adaletli ve vatandaş merkezli hizmetler için beklentilerindeki artış, hizmetlerin sorunsuz bir şekilde sunulması ve gelişmiş kalkınma etkisi süreç odaklı organizasyon yapılarından yüksek işbirliğine dayanan çerçevelere geçişi gerektirmektedir. Kamu hizmetinde teknoloji kullanımı ve iyi yönetim için güvenilir, kapsayıcı ve etkili bir ortam sağlamak için açık ve uzun vadeli politika ve stratejik çerçevelere ihtiyaç vardır. Bu çerçeveler, sürdürülebilir kalkınmanın temel ilkelerinin uygulanmasını destekleyen kamu hizmeti için plan olmalıdır. Güvenilir kurumların performans beklentilerini karşılama kapasitesi, yeterlilik algıları ve herkes için etkin kamu hizmeti sunumu, kamu sorumluluğunun yanı sıra, kamu yönetiminde ve kamu sektörü reformunun altında yatan hedeflerin başında gelmelidir. Cinsiyet eşitsizliği, özellikle katılımcı toplumsal cinsiyete duyarlı bütçeler yoluyla, çok sayıda kamu politikası ile aşılmalıdır. Yeni vatandaşlar ve işletmeler, daha açık, şeffaf, hesap verebilir ve etkili bir yönetim talep ederken, yeni teknolojiler, herkes arasında etkili bilgi yönetimi, paylaşım ve işbirliği sağlar. Sektörler ve hükümetin her seviyesinde şeffaflık, katılım ve işbirliği ilkeleriyle vatandaşlar ve hükümetleri arasında güven inşa edilmesine özel önem verilmelidir. Hükümetler artık tek taraflı olarak hizmet sağlayamıyor ve hizmet entegrasyonundan kaynaklanabilecek daha etkin ve hesap verebilir kamu fonlarının kullanımına yönelik talepleri göz ardı ediyor (e Devlet, 2019). Bilgi ve İletişim Teknolojileri, bilgiye erişimi sağlayarak şeffaflığı artırabilir; bu aynı zamanda hesap verebilirliği de artırır ve hükümetin ne yaptığını ve ne kadar iyi yaptığını kontrol edebilir. Bilgi ve İletişim Teknolojileri ayrıca, hükümetler ve vatandaşları arasında iki yönlü bilgi ve deneyim paylaşımı yoluyla katılımı da teşvik eder. Bu, hem ulusal hükümet siloları arasında hem de sınır ötesi bölgelerde kamu hizmetlerini birlikte oluşturmayı ve kanıta dayalı karar ve politika oluşturma konusunda işbirliğini mümkün kılar. Kısacası, BİT'ler oyun değiştiren bir etkileştiricidir. Aynı zamanda, düzenleme eksikliği kamu hizmeti tasarımı ve sunumunda BİT kullanımını engelleyebilir. BİT'ler için uzun vadeli bir strateji geliştirmek ve bunu gerekli kaynaklarla, düzenleyici çerçeveye ve siyasi iradeyle desteklemek, sürdürülebilir kalkınmayı sağlamak için benzersiz bir güçlü potansiyele sahiptir. Kamu görevlilerinin

davranışlarının izlenmesi için genel bir açık Ülke stratejisi, sağlıklı insan kaynakları ve kapsamlı açıklama prosedürleri uygulanmalıdır. Etkili koordinasyon, işbirliği ve hesap verebilirlik için yeni kurumsal çerçeveler biçimleri, hükümetler arasında ve devletlerarasında ve kamuoyu değeri yaratmaya katkıda bulunabilecek kamuya açık olmayan aktörlerle birlikte uygulanmalıdır.

Gelecekte e-Devlet kullanımının artacağı öngörülmektedir. Ayrıca e-Devlet'in ilerleyen zamanlarda devlet teorisini derinden sarsacağı ve kendine has bir teorinin geliştirileceği ön görülmektedir. Özellikle devlet yönetimi için bürokratlara ve yöneticilere ödenen aşırı maaşlar ve onlara sağlanan imkânların halka dağıtılması fikri ön plana çıkmaktadır. Bu fikrin ortaya çıkmasının en önemli nedeni derin öğrenme yöntemlerinin yaygınlaşmasıdır. Derin öğrenme insan beynine en yakın model olarak ortaya çıkmaktadır. Bu yöntemler çok fazla veriyi tekrarlamalı olarak kullanarak öğrenme işlemini yapar. Evrimsel ve tekrarlayan sinir ağlarının yüksek performansı, bu sistemlerin yaygın kullanımına neden olmaktadır. Bu sistemlerle birlikte pekiştirmeli öğrenme teoremleri, çevredeki verileri toplayarak kendi kendine öğrenen sistemlerin sunulmasına neden olmuştur. Temel teorem, sosyal kabullerin, yasaların, kuralların ve kabullerin yapay zekâya öğretilerek, e-Devlet sistemlerinin karar alıcı olmasını desteklemektir. Bu sayede yasaları bir yapay zekâ yapacak ve birçok karar alıcıya gerek kalmayacaktır. Bu sistem kayırmacılık ve rüşveti engelleyerek sosyal adaleti tesis edecektir fikri ön plana çıkmaktadır. Tabii ki bu kuram günümüzde destek görmemektedir ancak günümüzdeki durum gelecekte de bu teoremin kabul görmeyeceği manasına gelmemektedir. Bu teoremle birlikte asistanlarla e-Devlet hizmetleri verilecektir. Bu asistanlar sayesinde vatandaşlar devlet hizmetlerinden daha efektif bir şekilde faydalanacaktır.

e-Devlet ile ilgili en önemli hususlardan birisi de güvenlidir. Günümüzde bilgisayarlarda kullanılan temel malzemeler silikon, bakır ve altındır. İşlem hızları da bu malzemelerin kapasiteleriyle doğru orantılıdır. Günümüz de geline nokta bu malzemelerin limitine yaklaşıldığı bilinmektedir ancak insanlık gelecek yıllarda daha yüksek işlem kapasitesine ihtiyaç duyacaktır. Bu nedenle bilgisayarlarda kullanılan malzemenin değiştirilmesi fikri ön plana çıkmıştır. Bu nedenle kuantum bilgisayarların gelecekte kullanıma sunulması planlanmaktadır ve hali hazırda kuantum bilgisayarlar mevcuttur. Kuantum bilgisayarlarla birlikte depolama ve işlem hızları muazzam bir şekilde artacaktır. Çünkü bizim bildiğimiz 0-1 değerini alan bitler yok olacak ve tek

başına büyük bir aralıkta değerler ifade edebilen qu-bit kavramı hayatımıza girecektir. Bu değişikliklerle birlikte bilinen güvenlik yöntemleri de yetersiz kalacaktır. Bundan dolayı kuantum sonrası güvenlik yöntemleri geliştirilmektedir. Bu tezde elde edilen bulgular ışığında sunulan temel öneri şu şekildedir. e-Devlet uygulamalarının devamlılığının sağlanması için güvenlik faktörünün ön planda tutulması gerekmektedir. Önümüzdeki yıllarda kuantum bilgisayarların hayatımıza gireceği muhtemeldir. Bu sebepten dolayı geliştiricilerin kuantum oryantasyonunun şimdiden yapılması gerekmektedir. Çünkü kuantum devrimiyle birlikte bilgi güvenliği protokolleri değişecektir. Bu değişime hızlı entegre olabilmek için kuantum çalışmalarının yapılması hayati önem taşımaktadır. Kuantum devrimine oryantasyonun yanı sıra, hali hazırda kullanılan blok zinciri yöntemlerinin de e-Devlet uygulamalarına entegre edilmesi gerekmektedir. Bildiğimiz kadarıyla, güvenilir bir sertifikatör kullanılırsa, blok zinciri uygulamaları mükemmel şeffaflık ve güvenlik sağlamaktadır. Özellikle e-Devlet uygulamalarının böylesi bir alt yapıya ihtiyacı olduğu bilinmektedir. Yapılan araştırmalar sonucunda, en kısa sürede blok zinciri alt yapısının e-Devlet uygulamalarına entegre edilmesiyle gizlilik ve şeffaflık konularının daha da güçlü hale getirileceği ve e-Devlet güvenlik problemlerinin büyük bir kısmının çözülebileceği görülmektedir. Blok zincir alt yapısıyla e-Devlet olan güven artacaktır. Blok zinciri yapısı ilk olarak kripto para kavramıyla karşımıza çıksa bile, bazı uygulamalarda daha efektif olarak kullanılabileceği görülmektedir. e-Devlet bunlardan birisidir. Çünkü e-Devlet sistemlerinde güvenlik ve şeffaflıktan bahsedebilmek için blok zincirinin efektif ve aktif bir şekilde kullanılması gerekmektedir. Bu kavramı somutlaştırmak için tapu kayıtları örnek olarak verilebilir. Miras yoluyla devrolan malların etiketlenmesi ve bireylerin haklarının korunması için tapu kayıtlarının sağlıklı olarak tutulması gerekmektedir. Eğer blok zinciri yapısıyla tapu kayıtları kaydedilirse, bu kayıtları manipüle etmek matematiksel olarak imkânsız hale gelecektir. Aynı zamanda tapu kayıtlarındaki şeffaflık üst düzeyde sağlanacaktır.

Sonuç olarak bu tezde e-Devletin dünü, bugünü ve geleceği bilgi güvenliği ekseninde tartışılmaya çalışılmıştır. Bu tartışmanın sonucu olarak; e-Devlet'in teorisinin devlet derinden sarsacağı, yapay zekâyla e-Devlet uygulamalarının değişebileceği ve kuantum sonrası şifreleme ile blok zinciri altyapısı kullanılarak mükemmel güvenilirlik ve şeffaflığın sağlanabileceği gösterilmiştir. Bilgi güvenliğinin e-Devlet portallarında hayati öneme sahip olduğu gösterilmiştir. Güvenin olduğu yerde e-Devlet

uygulamalarının yaygın ve efektif olarak kullanıldığı görülmüştür. e-Devlet sistemlerinde güvenliğin sağlanması için tüm dünyada yaygın olarak kullanılarak GSK protokolü kullanılmaktadır. Bu protokolün yanı sıra kamu çalışanları ve bireyler e-İmza cihazları kullanarak güvenliğini maksimum seviyeye çıkarabilmektedirler. Bilgi güvenliğindeki trendlerin e-Devlet geliştiricileri tarafından yakından takip edilmesi ve bu sayede e-Devletin yaşam döngüsünün sağlanabileceği gösterilmiştir. Özellikle yeni nesil güvenlik protokolleri kullanılarak e-Devletin yaşamının daha efektif bir şekilde sürdürülebileceği sonucuna ulaşılmaktadır.



KAYNAKÇA

- Abdelsatar, S. A. (2018). Electronic government and its role in administrative development applied study on the directorate general of education in Arbil. *Yayımlanmamış Yüksek Lisans Tezi. Bingöl Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı, Bingöl*
- Abdulrahman, B. A. (2014). e-Devlet ve CBS teknolojisinin eğitim hizmetlerinin gelişmesinde etkileri üzerine bir çalışma: Kerkük Merkezdeki okullar. *Yayımlanmamış Yüksek Lisans Tezi. Çankaya Üniversitesi Fen Bilimleri Enstitüsü Matematik ve Bilgisayar Bilimleri Anabilim Dalı, Ankara.*
- Abed, A. (2015). Genel bütçe verimliliği performansının artırılmasında e-Devletin rolü. *Yayımlanmış Yüksek Lisans Tezi. Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı, Gaziantep.*
- Abu-Shanab, E., & Al-Azzam, A. (2012). Trust Dimensions and the adoption of e-Government in Jordan. *International Journal of Information Communication Technologies and Human Development (IJICTHD)*, 4(1), 39-51.
- Abunadi, I. (2015). Characteristics of electronic integrated system and trust in the provider of service. *International Journal of Computer Applications*, 132(4), 23-31.
- Access Control Security Features, <https://www.securitycommunity.tcs.com/infos/ecsoapbox/articles/2016/07/21/access-control-security-features>, 04.03.2019.
- Adams Dr Carl., (2015), Proceedings of the 15th European Conference on e-Government 2015: ECEG 2015, Academic Conferences Limited, p. 398
- Akman, M. K. (2019). Bilgi Sosyolojisi Açısından İstihbarat Kaynaklarının Tasnifi ve Değerlendirilmesi. *Ankara Üniversitesi Sosyal Bilimler Dergisi*, 10(1), 24-42.
- Alshboul, R., (2012), Security and Vulnerability in the e-Government Society, *Contemporary Engineering Sciences*
- Al-adawi, Z., Yousafzai, S., & Pallister, J. (2005). *Conceptual model of citizen adoption of e-Government*. Paper presented at the The Second International Conference on Innovations in Information Technology IIT'05.
- Al-Ameri, M. A. A. (2017). e-Devlet servislerinin yönetim ve personel açısından ihtiyaç analizi ve modüler tasarım ile yaygınlaştırmanın önceliklendirilmesi: Irak

- tutuklu hizmetleri durum çalışması. *Yayımlanmamış Yüksek Lisans Tezi. Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Yeni Türk Dili Anabilim Dalı, Kayseri.*
- Al-Baiaty, S. H. H. (2017). Pasaport hizmetlerinde e-Devlet uygulamalarındaki zorluklar. *Yayımlanmamış Yüksek Lisans Tezi. Çankaya Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı, Ankara.*
- Al-Jamal, N. Q., & Abu-Shanab, E. A. (2015). *e-Government adoption in Jordan: The influence of age*. Paper presented at the ICIT 2015 the 7th International Conference on Information Technology.
- AlKalbani, A., Deng, H., & Kam, B. (2015). *Organisational Security Culture and Information Security Compliance for e-Government Development: The Moderating Effect of Social Pressure*. Paper presented at the PACIS.
- Almarabeh, T., & AbuAli, A. (2010). A general framework for e-Government: definition maturity challenges, opportunities, and success. *European Journal of Scientific Research*, 39(1), 29-42.
- Alrashedi, R., Persaud, A., & Kindra, G. (2015). Drivers of eParticipation: Case of Saudi Arabia. *The Journal of Business Inquiry*, 14(1), 1-22.
- Alshehri, M., Drew, S., & Alfarraj, O. (2012). A Comprehensive Analysis of e-Government services adoption in Saudi Arabia: Obstacles and Challenges. *International Journal of Advanced Computer Science and Applications*, 3(2), 1-6.
- Ataman, S. (2002). Küçük ve Orta Ölçekli İşletmelerde Bilgi Yönetimi ve Bir Uygulama. *Yayımlanmamış Yüksek Lisans Tezi. Marmara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, İstanbul*
- Atılğan, D. (2009). Bilgi yönetimi kavramı ve gelişimi. *Türk Kütüphaneciliği*, 23(1), 201-212.
- Ayyash, M. M., Ahmad, K., & Singh, D. (2013). Investigating the effect of information systems factors on trust in e-Government initiative adoption in Palestinian public sector. *Research Journal of Applied Sciences, Engineering and Technology*, 5(15), 3865-3875.
- Avşar, Z., & Öngören, G. (2010). *Bilişim hukuku*. Türkiye Bankalar Birliği.
- Arifoğlu, A.; Körnes A.; Yazıcı A.; Akgül K.; Ayvalı A., (2002), e-Devlet Yolunda Türkiye, Türkiye Bilişim Derneği (TBD) Yayınları, Ankara.

- Backus, M. (2001). e-Governance and developing countries, introduction and examples. *International Institute for Communication and Development (IICD)*.
- Baeza-Yates, R., & Ribeiro, B. d. A. N. (2011). *Modern information retrieval*: New York: ACM Press; Harlow, England: Addison-Wesley.
- Balcı, A. (2008). “e-Devlet: Kamu Yönetiminde Yeni Perspektifler, Fırsatlar ve Zorluklar”, Seçkin Yayınları, Ankara.
- Balay, R. (2000). *Yönetici ve öğretmenlerde: örgütsel bağlılık*: Nobe Yayıncılık, Ankara.
- Balay, R. (2004). Küreselleşme, bilgi toplumu ve eğitim. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi*, 37(2), 61-82.
- Baştan, S., & Gökbnar, R. (2004). Kamu hizmetlerinin sunumunda e-Devletle ilgili yeni gelişmeler: Tümüleşik e-Devlet sistemlerine doğru. *Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 19(1).
- Bell, D. (1972). The cultural contradictions of capitalism. *Journal of Aesthetic Education*, 6(1/2), 11-38.
- Beynon-Davies, P., & Williams, M. D. (2003). Evaluating electronic local government in the UK. *Journal of Information Technology*, 18(2), 137-149.
- Bhatnagar, S. (2004). *e-Government: From vision to implementation-A practical guide with case studies* SAGE Publications Pvt. Ltd.
- BM, B. M. (2019). <https://publicadministration.un.org>. Erişim Tarihi:01.12.2018.
- Bojang, M. B. S. (2017). A comparative study of e-Government policies: An alternative model proposal for e-Government success in Africa. *Yayımlanmamış Yüksek Lisans Tezi. Sakarya Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı, Sakarya*.
- Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: a socio-technical perspective, part II: the application of socio-technical theory. *MIS quarterly*, 11-28.
- Botterman, M., Schindler, H. R., & Van Dijk, L. V. (2010). Trend Analysis (D3) Smart n 2009/0069.
- Burn, J., & Robins, G. (2003). Moving towards e-Government: a case study of organisational change processes. *Logistics Information Management*, 16(1), 25-35.

- Carroll, J. M., & Campbell, R. L. (1989). Artifacts as psychological theories: The case of human-computer interaction. *Behaviour & Information Technology*, 8(4), 247-256.
- Castells, M., & Cardoso, G. (2006). *The network society: From knowledge to policy*: Johns Hopkins Center for Transatlantic Relations Washington, DC.
- Celep, C. (2003). Halk egitimi. *Ankara: Ani Yayincilik*.
- Chaligava, N. (2018). e-Government Implementation in Public Administration of Georgia, Yayınlanmamış Yüksek Lisans Tezi, Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Yönetimi Anabilim Dalı, Ankara.
- Chang, H. H., & Chen, S. W. (2009). Consumer perception of interface quality, security, and loyalty in electronic commerce. *Information & management*, 46(7), 411-417.
- Coleman, S. (1994). Quantum sine-Gordon equation as the massive Thirring model. In *Bosonization* (pp. 128-137): World Scientific.
- Cover, T. M., & Thomas, J. A. (2012). *Elements of information theory*: John Wiley & Sons, Wiley-Blackwell; 2nd edition.
- Cruz, F. A., Tan, J. C., & Yonaha, Y. Y. (2015). Assisting the reintegration of Philippine return migrants through mobile technology. A Submission to the Geneva Challenge.
- Curran, K., Carlin, S., & Adams, M. (2012). Security issues cloud computing. *Cloud Computing for Teaching and Learning: Strategies for Design and Implementation* (pp. 200-208): IGI Global.
- Çapar, B. (2005). Bilgi: Yönetimi, Üretimi ve Pazarlanması. Bilgi Yayınevi.
- Çelen, F. K., Çelik, A., & Seferoğlu, S. S. (2011). Türkiye'deki e-Devlet Uygulamalarının Değerlendirilmesi. *Akademik Bilişim Dergisi, İnönü Üniversitesi, Malatya, Türkiye (9-1): (2011)*.
- Çiftçi, H. (2013). Her Yönüyle Siber Savaş, Tübitak Popüler Bilim Kitapları, Ankara.
- Erdal, M. (2004). Elektronik Devlet e-Türkiye ve Kurumsal Dönüşüm. Filiz Kitabevi. İstanbul
- Dawes, S. S. (2009). Governance in the digital age: A research and action framework for an uncertain future. *Government Information Quarterly*, 26(2), 257-264.
- Delibaş, Kayhan ve YİĞİT, *Emin 2005 Siyaset Kurumu*, Birey Yayıncılık, İstanbul.

- Demir, Önder (2000), “İnternet Servis Sağlayıcısının Cezai Sorumluluğu”, İzmir Barosu Dergisi, 66(3): 36-43.
- Demirel, D. (2006). e-Devlet ve Dünya Örnekleri. *Sayıştay Dergisi*, 61(6), 83-118.
- Desa, D. (2019). United Nations; The Division for Public Institutions and Digital Government (Dpidg) is a division of the United Nations Department of Economic and Social Affairs (Desa). It provides secretariat support to the United Nations Programme in Public Administration (GA resolution 723 (VIII)[1] of 23 October 1953 and ECOSOC resolution 1199 (XLII)[2] of 24 May 1967).
- Devopedia, <https://devopedia.org/information-security-principles>, 14.04.2019.
- Duffany, J. L. (2012). Cloud computing security and privacy. Paper presented at the 10th Latin American and Caribbean Conference for Engineering and Technology.
- Durankaya, İ., Gökşen, Y., & Eminağaoğlu, M. (2018). ISO27001 Bilgi Güvenliği Yönetim Sisteminde Risk Analizi, IMISC 2018 Conference Proceedings, 29-33.
- Dwivedi, Y. K., Wastell, D., Laumer, S., Henriksen, H. Z., Myers, M. D., Bunker, D., . . . Srivastava, S. C. (2015). Research on information systems failures and successes: Status update and future directions. *Information Systems Frontiers*, 17(1), 143-157.
- Eker, S., Cömertpay, G., Konuşkan, Ö., Ülger, A. C., Öztürk, L., & Çakmak, İ. (2006). Effect of salinity stress on dry matter production and ion accumulation in hybrid maize varieties. *Turkish journal of agriculture and forestry*, 30(5), 365-373.
- Elazığ Belediyesi. (2019). <https://www.elazig.bel.tr/>. Erişim Tarihi: 11.02.2019
- Elazığ Valiliği. (2019). <http://www.elazig.gov.tr/>. Erişim Tarihi: 11.02.2019
- Elsheikh, Y., & Azzeh, M. (2014). What Facilitates the delivery of citizen-centric e-Government services in developing countries: model development and validation through structural equation modeling. *International Journal of Computer Science & Information Technology*, 6(1), 77.
- Elsteel, N. O. S. (2017). e-Devlet servislerinin gerçekleştirilmesindeki engeller: Libya için bir empirik çalışma. *Yayımlanmamış Yüksek Lisans Tezi. Atılım Üniversitesi Fen Bilimleri Enstitüsü Yazılım Mühendisliği Anabilim Dalı, Ankara.*
- European Commission. (2013). ‘Digital by default, or by Detour? *Assessing User Centric eGovernment performance in Europe -2012 Benchmark*

- Evans, D., & Yen, D. C. (2006). e-Government: Evolving relationship of citizens and government, domestic, and international development. *Government Information Quarterly*, 23(2), 207-235.
- Fırat, G. (2013). Kurumsal Bilgi Yönetimi. *Yayımlanmamış Yüksek Lisans Tezi. Beykent Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi Anabilim Dalı, İstanbul.*
- Firstgov. (2018). www.firstgov.gov. Erişim Tarihi:05.11.2018.
- Folstein, M. F., Folstein, S. E., & McHugh, P. R. (1975). "Mini-mental state": a practical method for grading the cognitive state of patients for the clinician. *Journal of psychiatric research*, 12(3), 189-198.
- Gaule, E., & Zilinskas, G. (2013). e-Governance in Lithuanian municipalities: external factors analysis of the websites development. *Viesoji Politika ir Administravimas*, 12(1).
- Gharehchopogh, F. S., & Hashemi, S. (2012). Security challenges in cloud computing with more emphasis on trust and privacy. *International Journal of Scientific & Technology Research*, 1(6), 49-54.
- Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS quarterly*, 213-236.
- Gökçe, Ş. (2006). Bilgi çağının iş organizasyonlarında stratejik bilgi yönetimi: Teori ve bir uygulama. *Yayımlanmamış Yüksek Lisans Tezi. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi Anabilim Dalı, Konya.*
- Gulliksen, J. (2014). *Human computer interaction and societal impact: can HCI influence public policy making IT politics.*
- Gülbahar, Y., Kalelioğlu, F., & Madran, O. (2010). Sosyal ağların eğitim amaçlı kullanımı. *XV. Türkiye’de internet konferansı, İstanbul, 10, 2016.*
- Gürsu, M. (2003). Bilgi yönetiminde bilgi haritaları *Yayımlanmamış Yüksek Lisans Tezi. Marmara Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi Anabilim Dalı, İstanbul.*
- Haider, Z., Shuwen, C., & Burdey, M. B. (2016). e-Government Project Obstacles in Pakistan. *International Journal of Computer Theory and Engineering*, 8(5), 362.
- Hashim, H. S., Hassan, Z. B., & Hashim, A. S. (2015). Factors influence the adoption of cloud computing: A comprehensive review. *International Journal of Education and Research*, 3(7), 295-306.

- Hazlett, S.-A., & Hill, F. (2003). e-Government: the realities of using IT to transform the public sector. *Managing Service Quality: An International Journal*, 13(6), 445-452.
- Heeks, R. (2003). Causes of e-Government success and failure: Factor model. *Institute for Development Policy and Management, University of Manchester*.
- Heeks, R. (2003). *Most e-Government-for-development projects fail: how can risks be reduced?* (Vol. 14): Institute for Development Policy and Management, University of Manchester
- Hingorani, N. G., Gyugyi, L., & El-Hawary, M. (2000). *Understanding FACTS: concepts and technology of flexible AC transmission systems* (Vol. 1): IEEE press New York.
- Iachello, G., & Hong, J. (2007). End-user privacy in human-computer interaction. *Foundations and Trends® in Human-Computer Interaction*, 1(1), 1-137.
- IBM. (2015). <http://www.redbooks.ibm.com/redpapers/pdfs/redp5179.pdf> ,Cloud Computing Simplified: The Thoughts on Cloud Way. Eriřim Tarihi: 22.01.2019
- Ibraheem, O. M. (2017). E - devlet: Sosyal etkileri, zorluklar, engeller ve çözüm önerileri. *Yayımlanmamış Yüksek Lisans Tezi. Erciyes Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Kayseri*.
- Irani, Z., Love, P. E., & Jones, S. (2008). Learning lessons from evaluating eGovernment: Reflective case experiences that support transformational government. *The Journal of Strategic Information Systems*, 17(2), 155-164.
- Irvine, C. E. (2000). Security issues for automated information systems. *Public Administration And Public Policy*, 77, 231-246.
- Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information technology and management*, 1(1-2), 45-71.
- Jones, P. D., Briffa, K., Osborn, T., Lough, J., Van Ommen, T., Vinther, B., . . . Mann, M. (2009). High-resolution palaeoclimatology of the last millennium: a review of current status and future prospects. *The Holocene*, 19(1), 3-49.
- Joshi, J., Ghafoor, A., Aref, W. G., & Spafford, E. H. (2001). Digital government security infrastructure design challenges. *Computer*, 34(2), 66-72.
- Karakoçak, K. (2007). Bilgi yönetimi ve verimliliğe etkisi: Türkiye Büyük Millet Meclisi uygulaması. *Yayımlanmamış Doktora Tezi. Ankara Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı, Ankara*.

- Karakuş, T., Çağıltay, K., Kaşıkçı, D., Kurşun, E., & Ogan, C. (2014). Türkiye ve Avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim ve Bilim*, 39(171).
- Kayrouz, A., & Atala, I. (2014). e-Government in Lebanon. *European Scientific Journal* Esj February 2014 ,Special, Edition Vol.1.
- Kızıldağ, D. (2011). ISO 31000 Risk Yönetimi. Ankara: Seçkin Yayıncılık.
- Koçak, H., & Memiş, K. (2018). Bilgi Toplumunda Korku: Bilgi Güvenliği ve Risk Toplumu. *Afyon Kocatepe University Journal of Social Sciences*, 20(3).
- Koçak, J. (2004). Küçük ve orta boy işletmelerde bilgi yönetimi *Yayımlanmamış Yüksek Lisans Tezi. Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü Strateji Bilimi Anabilim Dalı, Gebze.*
- Konuşkan, Ö. (2015). Bilgi yönetimi ve bilgi yönetimi anlayışında insan kaynakları yönetimi. *Yayımlanmamış Yüksek Lisans Tezi. Karabük Üniversitesi Fen Bilimleri Enstitüsü Endüstri Mühendisliği Anabilim Dalı, Karabük.*
- Kuran, N. H., (2005) Türkiye İçin e-Devlet Modeli, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.
- Kurttepe, B. G. (2008). Bilgi yönetimi açısından e-Dönüşüm ve bir uygulama. *Yayımlanmamış Yüksek Lisans Tezi. Haliç Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı, İstanbul.*
- Lee, G., & Lin, H. (2005). Customer perceptions of e-Service quality in online shopping. *International Journal of Retail & Distribution Management*, 33(2), 161-176.
- Lee, J., Kim, H. J., & Ahn, M. J. (2011). The willingness of e-Government service adoption by business users: The role of offline service quality and trust in technology. *Government Information Quarterly*, 28(2), 222-230.
- Lim, N., Grönlund, Å., & Andersson, A. (2015). Cloud computing: The beliefs and perceptions of Swedish school principals. *Computers & Education*, 84, 90-100.
- Lum, D. J., Howell, J. C., Allman, M., Gerrits, T., Verma, V. B., Nam, S. W., . . . Lloyd, S. (2016). Quantum enigma machine: Experimentally demonstrating quantum data locking. *Physical Review A*, 94(2), 022315.
- Martini, A., & Pellegrini, L. (2005). Barriers and levers towards knowledge management configurations: A case study-based approach. *Journal of Manufacturing Technology Management*, 16(6), 670-681.

- Mauss, M. (2002). *The gift: The form and reason for exchange in archaic societies*: Routledge.
- McLuhan, M., Powers, B. R., & Düzgören, B. Ö. (2001). *Global köy: 21. yüzyılda yeryüzü yaşamında ve medyada meydana gelecek dönüşümler*: Scala.
- Metaxiotis, K., & Psarras, J. (2004). e-Government: new concept, big challenge, success stories. *Electronic Government, an International Journal*, 1(2), 141-151.
- Equation of state calculations by fast computing machines. *The journal of chemical physics*, 21(6), 1087-1092.
- Meydanlı, M. (2010). e-Devlet ve Türkiye’de e-Devlet Uygularının Kamu Hizmetleri Üzerindeki Etkisi: İçişleri Bakanlığı MERNİS Uygulaması, *Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara*.
- Milner, E. (2002). *Managing information and knowledge in the public sector*: Routledge.
- Morad, H. (2014). Irak e-Devlet hükümetinin yüz tanıma sisteminin geliştirilmesi. *Yayınlanmamış Yüksek Lisans Tezi. Çankaya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Ankara*.
- Nacar, M. (2008). Türk Kamu Yönetiminde e-Devlet Uygulamaları: Emniyet Teşkilatı’nın e-Devlet Yapılanmasındaki Yeri. *Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara*.
- Nations, U. (2012). "United Nations e-Government Survey 2014." United Nations.
- Nawafleh, S., Obiedat, R., & Harfoushi, O. (2012). e-Government between developed and developing countries. *International Journal of Advanced Corporate Learning (iJAC)*, 5(1), 8-13.
- Ndou, V. (2004). E-Government for developing countries: opportunities and challenges. *The electronic journal of information systems in developing countries*, 18(1), 1-24.
- Ong, C.-S., & Wang, S.-W. (2009). Managing citizen-initiated email contacts. *Government Information Quarterly*, 26(3), 498-504.
- Otubu, A. K. (2009). e-Government and Land Administration in Nigeria-A Recipe for Lagos State. *The electronic journal of information systems in developing countries*, 18(1), 1-24.

- Papadomichelaki, X., & Mentzas, G. (2012). e-GovQual: A multiple-item scale for assessing e-Government service quality. *Government Information Quarterly*, 29(1), 98-109.
- Ramadhan, A. A. M. (2017). Irak'taki e-Devlet projesinin değerlendirilmesi: Trafik Genel Müdürlüğü. *Yayımlanmamış Yüksek Lisans Tezi. İstanbul Kemerburgaz Üniversitesi Fen Bilimleri Enstitüsü Elektrik ve Bilgisayar Mühendisliği Anabilim Dalı, İstanbul.*
- Razzaqi, H. A. (2013). Factors Determining e-Government Security *Brunel University, School of Information Systems, Computing and Mathematics Department of Information Systems and Computing, London.*
- Ribbink, D., Van Riel, A. C., Liljander, V., & Streukens, S. (2004). Comfort your online customer: quality, trust and loyalty on the internet. *Managing Service Quality: An International Journal*, 14(6), 446-456.
- Riley, S., Fraser, C., Donnelly, C. A., Ghani, A. C., Abu-Raddad, L. J., Hedley, A. J., . . . Thach, T. Q. (2003). Transmission dynamics of the etiological agent of SARS in Hong Kong: impact of public health interventions. *Science*, 300(5627), 1961-1966.
- Saadi, M., & Almahjoub, A. (2012). e-Governance in Libya—Where we are and Where to Go. In *Proceedings of Libyan Conference on International e-Government* (pp.14-15).
- Sancaktutar, M. (2013). e-Devlet yeniliklerinin benimsenme ve yayılımını etkileyen faktörler: Türk e-Devlet bağlamından bazı kanıtlar. *Yayımlanmamış, Yüksek Lisans Tezi, Maltepe Üniversitesi Sosyal Bilimler Enstitüsü Sosyoloji Anabilim Dalı. İstanbul.*
- Sarabdeen, J., & Ishak, M. M. M. (2015). Impediment of privacy in the use of clouds by educational institutions. *International Journal of Information Management*, 34(1), 48-57.
- Selimoğlu, N. (2005). Süreç Yönetimi ve Süreç İyileştirmede Bilgi Yönetiminin Rolü ve Uygulamaya İlişkin Bir Araştırma, *Eğitim ve Bilim*, 39(171).
- Shah, M. H., Peikari, H. R., & Yasin, N. M. (2014). The determinants of individuals' perceived e-Security: evidence from Malaysia. *International Journal of Information Management*, 34(1), 48-57.

- Shareef, M. A., Kumar, U., Kumar, V., & Dwivedi, Y. K. (2009). Identifying critical factors for adoption of e-Government. *Electronic Government, an International Journal*, 6(1), 70-96.
- Shareef, M. A., Kumar, V., Kumar, U., & Dwivedi, Y. K. (2011). e-Government Adoption Model (GAM): Differing service maturity levels. *Government Information Quarterly*, 28(1), 17-35.
- Shbair, K. F. K. (2015). e-Devlet metodolojileri temelli uzaktan öğrenme mimarisinin tasarımı ve gerçekleştirimi. *Yayımlanmamış Yüksek Lisans Tezi. Anadolu Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Eskişehir.*
- Shipp, B. (2013). Social networks, interactivity and satisfaction: assessing socio-technical behavioral factors as an extension to technology acceptance. *Journal of theoretical and applied electronic commerce research*, 8(1), 35-52.
- Sinar, H. (2001), *Internet ve Ceza Hukuku*, Beta Yayınevi, İstanbul.
- Srivastava, S. C., & Teo, T. (2005). Citizen trust development for e-Government adoption: Case of Singapore. *PACIS 2005 Proceedings*, 59.
- Stephen H, H., Norris, D. F., & Fletcher, P. D. (2003). Electronic government at the local level: Progress to date and future issues. *Public Performance & Management Review*, 26(4), 325-344.
- Suleiman, A.-H. A. M. (2016). e-Devlet hizmet kalitesinin ölçülmesi-Ürdün vaka analizi. *Yayımlanmamış Yüksek Lisans Tezi. Okan Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı, İstanbul.*
- Suriye Portalı: http://portal.egov.sy/eservices_guid.ar_guid/en/0/0/module.page.html
Erişim Tarihi: 28.05.2019
- Sze, S. M. (2008). *Semiconductor devices: physics and technology*: John Wiley & Sons. 2nd Edition
- Şahin, A., & Örselli, E. (2003). e-Devlet Anlayışı Sürecinde Türkiye. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*(9), 343-356.
- Şahin, A. (2008). *Türk Kamu Yönetiminde Yapısal Dönüşüm ve e-Devlet*, Çizgi Kitabevi, Konya.
- Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS quarterly*, 561-570.
- TCK, Ülgen, C. (2019). *Türk Ceza Kanunu*. Beta Yayınları. İstanbul.

- Teo, T. S., Srivastava, S. C., & Jiang, L. (2008). Trust and electronic government success: An empirical study. *Journal of management information systems*, 25(3), 99-132.
- Topaloglu, N., Calp, M. H., & Turk, B. (2019). A Novel Data Encryption Algorithm Design and Implementation in Information Security Scope. *arXiv preprint arXiv:1902.04418*.
- Tweneboah-Koduah, S., Endicott-Popovsky, B., & Tsetse, A. (2014). Barriers to government cloud adoption. *International Journal of Managing Information Technology*, 6(3), 1-16.
- Uçkan, Ö. (2003). *e-Devlet, e-Demokrasi ve Türkiye* (Vol.1):Literatür Yayıncılık. İstanbul
- Unpan, (2014). Un e-Government Survey 2014. e-Government for the Future We Want. *New York: Unpan. Retrieved June 25, 2014*.
- Van der Molen, P., & Wubbe, M. (2007). *e-Government and e-Land Administration-As an example: The Netherlands*. Paper presented at the 6th FIG Regional Conference, San Jose, Costa Rica.
- Van Dijk, J. A. (2005). *The deepening divide: Inequality in the information society*: Sage Publications.
- Van Greunen, D., Herselman, M., & Van Niekerk, J. (2010). Implementation of regulation-based e-Procurement in the Eastern Cape provincial administration. *African Journal of Business Management*, 4(17), 3655-3665.
- Vassilakis, C., Lepouras, G., & Halatsis, C. (2007). A knowledge-based approach for developing multi-channel e-Government services. *Electronic Commerce Research and Applications*, 6(1), 113-124.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478.
- Vural, Z., & Bat, M. (2010). Yeni Bir İletişim Ortamı Olarak Sosyal Medya: Ege Üniversitesi İletişim Fakültesine Yönelik Bir Araştırma. *Journal of Yasar University*, 5(20).
- Wei, X., & Zhao, J. (2005). *Citizens' requirement analysis in Chinese e-Government*. Paper presented at the Proceedings of the 7th international conference on Electronic commerce.

- Welchman, G. (1982). *The Hut Six story: breaking the Enigma codes*: McGraw-Hill New York.
- Werhahn, K., Brown, P., Thompson, P., & Marsden, C. (1997). The clinical features and prognosis of chronic posthypoxic myoclonus. *Movement disorders*, 12(2), 216-220.
- Williams, R. (2004). *Television: Technology and cultural form*: Routledge.
- Wyld, D. C. (2010). The cloudy future of government IT: Cloud computing and the public sector around the world. *International Journal of Web & Semantic Technology*, 1(1), 1-20.
- Yablonovitch, E. (1987). Inhibited spontaneous emission in solid-state physics and electronics. *Physical review letters*, 58(20), 2059.
- Yıldırım, E. (2012). Müşteri ilişkileri yönetiminde bilgi yönetimi ve teknoloji desteği ile CRM analizi. *Yayınlanmış Yüksek Lisans Tezi. Haliç Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi Anabilim Dalı, İstanbul*.
- Yıldırım, H., Kaplan, V., Çakmak, T., Üstün, C. C. (2003) Her Şeyi e-Eleştirdik, Macar Yayıncılık, 2. Baskı, Ankara.
- Yıldız, A. (2018). Endüstri 4.0 ve akıllı fabrikalar. *Sakarya University Journal of Science*, 22(2).
- Yıldız, M. (2003). “Elektronik (e)- Devlet Kuramı ve Uygulamasına Genel Bir Bakış ve Değerlendirme”, Nobel Yayıncılık, Ankara.
- Yürük, E. (2017). e-Devlet Ana Kapılarında Sunulan Hizmetler Üzerine Bir İnceleme: Türkiye Ve Seçilmiş Ülke Örnekleri. *Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Yönetimi Anabilim Dalı, Ankara*.
- Zhang, P., Galletta, D., Sun, H., & Li, N. (2009). Human-computer interaction. *Management Information Systems, Tsinghua University Press, Beijing, China*.
- Zheng, L., Shen, C., Tang, L., Zeng, C., Li, T., Luis, S., & Chen, S.-C. (2013). Data mining meets the needs of disaster information management. *IEEE Transactions on Human-Machine Systems*, 43(5).
- Zürcher, E. J., & Gönen, Y. S. (1999). *Modernleşen Türkiye'nin tarihi: İletişim Yayınları*.
- 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı (Taslak), <http://www.edevlet.gov.tr/wp-content/uploads/2016/07/2016-2019-Ulusal-e-Devlet-Stratejisi-ve-Eylem-Plani.pdf> Erişim Tarihi:28.05.2019

e-Nabız, <https://enabiz.gov.tr/> Eriřim Tarihi: 28.05.2019

Uyap, <https://www.uyap.gov.tr/> Eriřim Tarihi: 28.05.2019

Mernis, <https://www.icisleri.gov.tr/merkez-nufus-idare-sistemi-mernis> Eriřim Tarihi: 28.05.2019

e-Eđitim, http://idealms.eba.gov.tr/lms/login_main.aspx Eriřim Tarihi: 28.05.2019

e-Vergi, <https://intvrg.gib.gov.tr/> Eriřim Tarihi: 28.05.2019

e-Devlet, <https://giris.turkiye.gov.tr/Giris/> Eriřim Tarihi: 28.05.2019



EKLER

Ek 1. Orjinallik Raporu



SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORJİNALLİK RAPORU

ÖĞRENCİ BİLGİLERİ	
Adı-Soyadı	İlknur TUNCER
Öğrenci Numarası	161217106
Enstitü Anabilim Dalı	Teknoloji ve Bilgi Yönetimi Ana Bilim Dalı
Programı	Teknoloji ve Bilgi Yönetimi
Danışmanın Unvanı, Adı-Soyadı	Dr. Öğr. Üyesi İlke Bezen TOZKOPARAN
Tez Başlığı (Türkçe)	Bilgi Güvenliği Açısından Bir Değerlendirme: e-Devlet Uygulamaları

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE

Yukarıda başlığı belirtilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 112 sayfalık kısmına ilişkin, 04/09/2019 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezin benzerlik oranı % 7'dir.

Uygulanan filtrelemeler:

- 1- Kabul/Onay ve Bildirim sayfaları hariç,
- 2- Kaynakça hariç
- 3- Alıntılar hariç/dâhil
- 4- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Yukarıda bilgileri verilen öğrencinin doktora tezi Sosyal Bilimler Enstitüsü Yönetim Kurulu tarafından belirlenen azami benzerlik oranlarını aşmadığını ve tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Dr. Öğr. Üyesi İlke Bezen TOZKOPARAN
 Danışmanın Adı-Soyadı

(İmzası)

Cem AYDEN
 Anabilim Dalı Başkanı

(İmzası)

Lisansüstü tezler, savunma öncesinde **intihal program raporu** ile birlikte enstitüye teslim edilir.

İntihal raporu ile ilgili olarak etik kurallar dâhilindeki benzerlik oranları ilgili Enstitü Yönetim Kurulu tarafından belirlenir. (Enstitü Yönetim Kurulu tarafından tezin, intihal kapsamı dışında değerlendirilmesi için TURNITIN'den alınan raporda "benzerlik oranı"nın, "alıntılar hariç" en fazla %10, "alıntılar dâhil" % 30'u geçmemesi şeklinde kabul edilmiştir).

ÖZGEÇMİŞ

Doğum Tarihi ve Yeri: 08 Aralık 1988 - Elazığ

Ehliyet: B sınıfı

Öğrenim Bilgileri:

Derece	Alan	Üniversite	Fakülte/Enstitü	Yıl
Ön Lisans	Bilgisayar Programcılığı	Fırat Üniversitesi	Tek. Bil. MYO	2010
Lisans	Bilgisayar Öğretmenliği	Fırat Üniversitesi	Fen Fakültesi	2012
Yüksek Lisans	Tek. ve Bil. Yön.	Fırat Üniversitesi	Sosyal Bilimler Enstitüsü	-

İş Bilgileri:

Kurum	Pozisyon	Sektör	Yıl
Malatya Adliyesi	Teknisyen	Kamu Kurumu	2011 - 2011
Elazığ Valiliği	Bilgisayar işletmeni	Kamu Kurumu	2011- 2015
Elazığ Valiliği	Teknisyen	Kamu Kurumu	2015 - Halen