FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ PROGRAMI

KİŞİSEL VERİLERİN KORUNMASI KAPSAMINDA BİLGİ GÜVENLİĞİ FARKINDALIĞI ANALİZİ VE E-DEVLET YAPISININ İNCELENMESİ

YÜKSEK LİSANS TEZİ

CAN GENÇ

Nisan 2019

Program: Bilişim Sistemleri

KİŞİSEL VERİLERİN KORUNMASI KAPSAMINDA BİLGİ GÜVENLİĞİ FARKINDALIĞI ANALİZİ VE E-DEVLET YAPISININ İNCELENMESİ

CAN GENÇ

tarafından

İSTANBUL OKAN ÜNİVERSİTESİ

Bilişim Sistemleri Programı

YÜKSEK LİSANS

derecesi şartını sağlamak için sunulmuştur.

Onaylayan:

Dr.Öğr.Üyesi
Feridun C. ÖZÇAKIR
Danışman

Dr.Öğr.Üyesi
Nurşen TOPÇUBAŞI
Üye

Dr.Öğr.Üyesi
Erkan KIYAK
Üye

Nisan 2019

Bölümü: Bilişim Sistemleri Programı

ÖZET

Bu çalışmada bilgi toplumu ve dijital dönüşüm çerçevesinde kişilerin bilgi güvenliği açısından bilgi ve iletişim teknolojileri ve internet kullanımlarına ilişkin alışkanlıkları ve davranışları araştırma konusu olarak seçilmiştir. Temel olarak kişilerin bilgi güvenliğine yönelik tehditler ve risklerle ilgili farkındalık düzeyleri incelenirken, bilgi ve iletişim teknolojileri ile ilgili tehlike algıları, bilişim suçlarına maruz kalma durumları ve kendilerini bu durumlarda nasıl korudukları tespit edilmeye çalışılmıştır.

Araştırma kapsamında kullanılan ölçekler anket formu şeklinde Eğitim, Sağlık, Finans, Kamu sektörü alanlarında farklı kurum ya da mesleki pozisyonlarda çalışan kişilere ve üniversite öğrencilerine uygulanmıştır. Anket formları üzerinden örneklem grubu olarak seçilen kişilere ait yaş, cinsiyet, eğitim durumu gibi demografik veriler, internet ve bilgi teknolojileri kullanımı alışkanlıkları ile riskli ve korumacı davranışlarına, suça maruz kalma durumlarına ve tehlike algılarına ilişkin veriler toplanarak bir araya getirildikten sonra değerlendirilmiş ve yorumlanmıştır.

Ölçekler aracılığıyla elde edilen verilerin istatiksel araştırma sonuçlarına göre, örneklem grubundaki kişiler kullanım, alışkanlık, davranış ve bilgi güvenliği farkındalığı açısından farklı özellikler göstermektedirler.

Anahtar Kelimeler: E-Devlet, Kişisel Verilerin Korunması, Bilgi Güvenliği,
Kişisel Bilgi Güvenliği Farkındalığı,

ABSTRACT

In this study, information and communication technologies and internet usage habits and behaviors of people, in the frame of information society and digital transformation in terms of information security were selected as the research subject. While examining the level of awareness of the threats and risks related to information security, it has been aimed to determine the perceptions of danger related to information and communication technologies, exposure to cyber crimes and how they protect themselves in these situations.

The scales used within the scope of the research have been applied as a questionnaire to the people working in different institutions or professional positions in the fields of Education, Health, Finance, Public sector and university students. Data regarding demographic data such as age, gender, education, along with internet and information technologies usage habits and risky and protective behaviors, exposure to crime and danger perception have been collected with questionnaires, gathered together and interpreted statistically.

According to the statistical research results of the data obtained by the scales, the people in the sample group show dissimilarities in terms of usage, habit, behavior and information security awareness.

Keywords: E-Goverment, Protection of Personal Data, İnformation Security, Personal Information Security Awareness

İÇİNDEKİLER

ÖZET……..ii

ABSTRACT……..iii

İÇİNDEKİLER……..iv

ŞEKİL TABLOSU…….....viii

TABLO LİSTESİ……..……ix

I. GİRİŞ…….....1

II. BİLGİ TOPLUMU…… 4

2.1. Bilgi Toplumu Kavramı……..4

2.1.1. Teknoloji……4

2.1.2. Bilgi ve İletişim Teknolojileri – BİT…….. 5

2.2. Bilgi Toplumunun Gelişim Süreci……..5

III. E-DEVLET…….10

3.1. E-Dönüşüm……...10

3.2. E-Devlet Nedir?.....10

3.3. E-Devletin Etkileşim Alanları…….. 11

3.4. Geleneksel Devlet E-Devlet Karşılaştırması…… 13

3.5. E-Devlet Türkiye……..15

3.5.1. E-Devlet Uygulamalarının Tarihçesi ve Yürütülen Çalışmalar……15

3.5.2. E-Devlet Kapısı…….18

3.5.3. E-Devlet İdari Yapılanma……19

3.5.4. Türkiye Kamu BİT Yatırımları ve E-Devlet İstatistikleri…….21

3.5.5. E-Devlet Kullanıcı-Hizmet-Kurum İstatistikleri…….. 22

3.5.6. Avrupa Birliği E-Devlet Endeksinde Türkiye…….. 25

3.5.7. Birleşmiş Milletler E-Devlet Gelişmişlik Endeksinde Türkiye……26

IV. VERİ KAVRAMI……..27

4.1. Verinin Tanımsal Çerçevesi……27

4.1.1. Veri, Enformasyon, Bilgi…….……27

4.2. Büyük Veri (Bıg Data)……32

4.2.1. Büyük Verinin Yapısal Özellikleri……...32

4.2.2. Büyük Veri Uygulamalarının Kullanıldığı Alanlar……..34

4.3. Kişisel Veri (Personal Data)……40

4.3.1. Kişisel Verinin Tanımı ve Kapsamı……..40

4.3.2. Kişisel Veri Türleri……...42

4.3.3. Kişisel Verilerin Korunması……43

4.3.4. Kişisel Verilerin Korunması Uluslararası Düzenlemeler……46

4.3.5. Kişisel Verilerin Korunması Ulusal Düzenlemeler……..55

4.3.6. Kişisel Verilerin İşlenmesi……61

V. KİŞİSEL BİLGİ GÜVENLİĞİ FARKINDALIĞI……..65

5.1. Bilgi Güvenliği……65

5.2. Bilgi Güvenliği Kavramının Gelişimi……..66

5.3. Bilgi Güvenliğinin Unsurları……... 71

5.3.1. Gizlilik (Confidentiality)…….. 72

5.3.2. Bütünlük (Integrity)…….. 72

5.3.3. Erişilebilirlik (Availability)…….. 73

5.3.4. Güvenilirlik (Reliability-Consistency)……..73

5.3.5. İnkâr Edememe (Non-Repudiation)……... 74

5.3.6. Kimlik Doğrulaması (Authentication)……..74

5.3.7. Yetkilendirme (Authorization)……..75

5.3.8. İzlenebilirlik/Kayıt Tutma (Accountability)……75

5.4. Bilgi Güvenliği Yönetimi……76

5.5. Bilgi Güvenliği Sınıflandırması……77

5.5.1. Ağ Güvenliği (Network Security)……78

5.5.2. Uç/Son Nokta Güvenliği (Network Security)……...79

5.5.3. Veri Güvenliği (Data Security)……80

5.5.4. Uygulama Güvenliği (Application Security)……82

5.5.5. Kimlik Doğrulama ve Erişim (Identity and Access Management)……...82
5.5.6. Güvenlik Yönetimi (Security Management)…….83
5.5.7. Sanallaştırma Yönetimi ve Bulut Bilişim (Virtualization and Cloud)…..83
5.5.8. Siber Güvenlik……... 87
5.6. Bilgi Güvenliğine Yönelik Tehditler……93
5.6.1. Gelişmiş Hedef Odaklı Saldırılar (Advanced Persistent Threats)…… 93
5.6.2. Zararlı Yazılımlar (Maliciosus Software - Malware)……... 94
5.6.3. Virüsler…… 95
5.6.4. Oltalama/Kimlik Avı (Phishing)…… 99
5.6.5. Zombi Makineler/Botnet (Botnets)…… 100
5.6.6. Dağıtılmış Ağ Saldırıları (Distributed Denial Of Service (Ddos))……. 101
5.6.7. Fidye Yazılımları (Ransomware)……102
5.6.8. Silici/Yokedici Zararlı Yazılımlar (Wiper Attacks)……... 103
5.6.9. Ortadaki Adam Saldırısı (Man In The Middle (MITM))……104
5.6.10. Otomatik Olarak Yüklenen Zararlılar (Drive By Downloads)……. 105
5.6.11. Antivirüs Olarak Görünen Yazılımlar (Scareware, Rogue Software).. 105
5.6.12. Fikri Mülkiyet Hırsızlığı (Intellectual Property Theft)……106
5.6.13. Sosyal Mühendislik (Social Engineering)…… 107
VI. BİLGİ GÜVENLİĞİ FARKINDALIĞI ANALİZİ……108
6.1. Yöntem……... 108
6.2. Amaç Ve Kapsam……...108
6.3. Veri Toplama Araçları……108
6.3.1. Riskli Davranışlar Ölçeği……109
6.3.2. Korumacı Davranışlar Ölçeği……110
6.3.3. Suça Maruziyet Ölçeğ……111
6.3.4. Tehlike Algısı Ölçeği……..112
6.3.5. Kişisel Bilgi Formu……113
6.4. Araştırma Hipotezleri……114
6.5. Araştırma Modeli……115
6.6. Veri Analizi…… 115
6.7. Bulgular……... 117

6.7.1. Tanımlayıcı Bulgular……..117
6.8. Hipotezlerin İstatiksel Sonuçları…… 119
VII. DEĞERLENDİRME…….. 130
KAYNAKÇA…….134
ÖZGEÇMİŞ……158

ŞEKİL TABLOSU

Şekil 2.1 Bilgisayar İletişim Devrimi ve Toplumsal Etkileri (Ünal Y. , 2009) 8
Şekil 3.1 E-Devlet Etkileşim Alanları (Özçelik, 2010) 12
Şekil 3.2 Geleneksel Devlet E-Devlet Çalışma Prensibi (Bilişim Şurası, 2002) 13
Şekil 3.3 Geleneksel Devlet E-Devlet Karşılaştırması (Uçkan, 2003) 15
Şekil 3.4 E-Devlet Çalışmaları Tarihçe (B.İ.T. D. Bşk., 2018) 18
Şekil 3.5 E-Devlet Kapısının İşleyişi (E-Devlet, 2018) 19
Şekil 3.6 E-Devlet İdari Yapılanma (Afyonluoğlu M. , 2018) 21
Şekil 3.7 Kamu BİT yatırımları 2002-2018 (BTD, 2018) 22
Şekil 4.1 Anlam Şeması Laszlo ve Laszlo (Aktan C. C., 2005) 30
Şekil 4.2 Dünya'da Büyük Veri Hacminde Öngörülen Büyüme Grafiği 40
Şekil 4.3 Hassas (Özel Nitelikli) Kişisel Veriler 42
Şekil 4.4 Genel Nitelikli Kişisel Veriler 43
Şekil 5.1 Bilgi Güvenliği Yönetimi Başlıca Unsurlar (Henkoğlu, 2017) 77
Şekil 6.1 Kişisel Bilgi Formu 113
Şekil 6.2 Araştırma Modeli 115

TABLO LİSTESİ

Tablo 3.1 E-Devlet Kullanıcı İstatistikleri (AA, 2019) 23
Tablo 3.2 E-Devlet Hizmet-Kurum İstatistikleri (TUİK, 2018) (AA, 2019).....23
Tablo 3.3 E-Devlet Kapısı En Çok Kullanılan Hizmetler (E-Devlet, 2019) 24
Tablo 3.4 AB - Türkiye E-Devlet Performans Karşılaştırması (EU TR, 2016) 25
Tablo 3.5 Birleşmiş Milletler E-Devlet Gelişmişlik Endeksi (BM, TR, 2016) 26
Tablo 4.1 Veri, Enformasyon, Bilgiye Kavramsal Bakış (Durna & Demirel, 2008) ..31
Tablo 4.2 Büyük Verinin Kaynakları (Eyüpoğlu, 2017) 33
Tablo 4.3 İnternet'te 60 Saniyede Neler Oluyor? (Go Globe, 2017).....39
Tablo 4.4 Sınır Ötesi Veri Akışlarına İlişkin Yönlendirici İlkeler (OECD, 2015).....48
Tablo 4.5 Kişisel Verilerin İşlenmesi Genel İlkeler; (KVVK İlkeler, 2017).....62
Tablo 4.6 Kişisel Verilerin İşlenme Şartları; (KVKK İşlenme Şartları, 2017) 63
Tablo 5.1 Siber Saldırı ve Veri Sızıntısı Olayları (Bus. Ins., 2018) (Gb, 2018).....90
Tablo 6.1 Riskli Davranışlar Ölçeği 109
Tablo 6.2 Korumacı Davranışlar Ölçeği.....110
Tablo 6.3 Suça Maruziyet Ölçeği 111
Tablo 6.4 Tehlike Algısı Ölçeği.....112
Tablo 6.5 Tanımlayıcı İstatistikler.....117
Tablo 6.6 İnternet Kullanım Süresi.....118
Tablo 6.7 İnternet Erişim Şekli.....118
Tablo 6.8 Bilgi Güvenliği ile İlgili Eğitim Alma Durumu 118
Tablo 6.9 Ölçek Betimsel İstatistikleri 118
Tablo 6.10 Spearman Korelasyon Matrisi 119
Tablo 6.11 Kadın ve Erkek İnternet Kullanıcıları (MWU) Test İstatistikleri.....121
Tablo 6.12 Yaş Grupları (MWU) Test İstatistikleri.....122
Tablo 6.13 Eğitim Seviyeleri (KWH) Test İstatistikleri.....124
Tablo 6.14 İnternet Kullanım Süreleri (KWH) Test İstatistikleri.....126
Tablo 6.15 Güvenlik Eğitimi Mann Whitney U Test İstatistikleri 128

I. GİRİŞ

20. Yüzyılın ikinci yarısıyla birlikte bilgi ve iletişim teknolojilerinde yaşanan gelişmeler toplumsal yapıların sosyal, kültürel, ekonomik ve siyasal açıdan büyük bir değişim yaşamasına neden olmuştur. Elektronik devreli, programlanabilir bilgisayarların ortaya çıkışı insan yaşamına ait tüm olguların bilgi tabanlı sistemlerle yeniden düzenlendiği, kurum, devlet ve organizasyonların küresel bir endüstri ve üretim yapısı içerisinde, teknolojiyi bütüncül olarak iş ve çalışma süreçlerine dâhil ettiği, yeni dijital dünya düzenini yaratmıştır. İnternet ve ağ sistemleri, geniş bağlantı protokolleri, akıllı mobil cihazlar gibi iletişimin boyutunu farklılaştıran ileri teknolojilerin etkisindeki yeni dijital dünya, insanlar ve makineler arasında etkileşimin sağlandığı, bir varlık olarak bilgiye ulaşma, bilgiden yararlanma ve bilgiyi üretme odaklı bir yaşam modelini de beraberinde getirmiştir. Belirli bir fiziksel ortama bağlı olmaksızın sistematik bir şekilde üretilebilen, saklanabilen, bir noktadan diğerine kolaylıkla aktarılabilen ve gerektiğinde yeniden kullanılabilen bilgi dijital dünyadaki temel güç ve kaynak haline gelmiştir.

Bilgi ve iletişim teknolojilerinin etkisindeki dijital dünyada değişen sosyal, kültürel ve ekonomik yapı, eğitim, sağlık, finans, tarım, endüstri gibi toplumsal yaşamın bütün dinamiklerinin düzenlenmesini, yenilenmesini zorunlu kılmıştır. Bu zorunlu dijital dönüşümün kendisini gösterdiği önemli alanlardan bir tanesi de günlük yaşamda bireylerin sıklıkla kullanmak durumunda olduğu kamu yönetimi kapsamında sunulan hizmetlere yönelik uygulamalardır. 1990'lı yıllardan itibaren teknolojinin kamu disiplini içerisinde temel yönetim işlevlerinden biri olarak görülmeye başlanmasıyla birlikte, dünya genelinde gelişmiş ülkeler kamu hizmetlerinin sunulmasında maliyet ve zaman

tasarrufu sağlanması ve hizmet kalitesinin artırılması amacıyla geleneksel devlet anlayışlarını değiştirerek, uygulama ve hizmetlerin sağlanmasında çevrimiçi elektronik ortamların kullanıldığı dijital E-Devlet modeline geçiş yapmışlardır. Ülkemizde de 2000'li yıllarda başlayan E-Devlet ile ilgili dönüşüm çalışmaları vatandaşların kamu hizmetlerinden daha hızlı ve kolay biçimde faydalanabilmelerini sağlayacak şekilde dünyadaki bilgi teknolojileri ile paralel sürdürülmektedir. E-Devlet modeli çerçevesinde sistem altyapısını tamamlayan 512 kurumun internet üzerinden 4280 tane farklı hizmeti sunduğu E-Devlet Kapısı 2019 yılı Şubat ayı itibariyle yaklaşık 42 milyon kullanıcıya ulaşmış durumdadır (AA, 2019).

Değişen teknolojik kültürle birlikte E-Devlet uygulamalarında olduğu gibi fiziksel ortamlardan taşınan ya da başta İnternet olmak üzere farklı çevrimiçi iletişim kanalları kullanılarak eşzamanlı üretilen içerisinde farklı veri seti kümeleri barındıran elektronik ortamlardaki bilgi her geçen gün çoğalarak artmaktadır. Dijital ekosistem içerisinde sahip olduğu değerden dolayı çeşitli veri işleme teknolojileri ile sınıflandırılan, analizi yapılan büyük miktardaki bu bilgilerin veri madenciliği yöntemleriyle birleştirilmesi sonucu kişilere ait sosyal, ekonomik ve kültürel durumu, ilişkileri hakkında nesnel ya da öznel bilgiler veren verilere ulaşılabilmektedir. Kişisel veri olarak tanımlanan bu bilgilerin üçüncü kişiler tarafından öğrenilmesi veya ele geçirilmesi bilgi erişimiyle ilgili güvenliğe yönelik önemli derecede risk ve tehdit oluşturmaktadır. Özel hayatın gizliliği ve temel hak ve özgürlükler kapsamında kişisel verilerin korunması kavramı önemli bir hukuksal ve yapısal sorun olarak dikkat çekmektedir.

2018 Nisan ayında Hootsuite ve we are social'ın birlikte yayınladığı İnternet ve Sosyal Medya Kullanım raporunda ortaya çıkan istatistiklere göre; 2018 yılı itibariyle tüm

dünyada 4.08 milyar kişi internete aktif olarak bağlı durumdayken, 5.06 milyar kişi de mobil teknolojileri kullanmaktadır. Dijital dünyada bütün bu hareketlilik içerisinde bir varlık türü olan bilginin bulunduğu her ortamda güvenliğinin sağlanması, karşılaşılan risk ve tehditler incelendiğinde her geçen gün biraz daha zor ve karmaşık hale gelmektedir.

Dijital dönüşümün endüstriyel veri hırsızları ve bilgisayar korsanları iletişim/üretim ağlarına sızarak (Micro, 2018), makine sistemlerine müdehale etme, ticari faaliyetleri engelleme, verilerin çalınması, kritik altyapılara zarar verme gibi farklı tür ve nitelikte yöntemlerle bankacılık, finans, enerji, bilişim gibi sektörlerin, kurum, uluslararası örgüt, devletlerin ve elbette kişilerin güvenliğini küresel boyutta tehdit etmektedirler. Gelişmiş teknolojiler, otomasyon, iletişim ve küreselleşme ile şekillenen siber dijital dünya düzeninde, bir varlık olarak bilginin korunmasına yönelik mevcut güvenlik sistemlerinin geliştirilmesi, stratejilerin oluşturulması ve farkındalık bilgi güvenliğinin en önemli konusu haline gelmiştir.

Bu çalışmada bilginin yapısı, bilgi toplumu, e-dönüşüm süreci, bilgi güvenliğini tehdit eden unsurlar ve hukuksal çerçevede kişisel verilerin korunması kavramı incelenmiştir. Kişilerin internet ve bilgi teknolojileri kullanımı ile alışkanlıkları doğrultusunda bilgi güvenliği farkındalıkları araştırılmış ve genel hatlarıyla istatiksel olarak değerlendirilmiştir.

II. BİLGİ TOPLUMU

2.1. **Bilgi Toplumu Kavramı**

Bilgi toplumu; varlık olarak temel değer haline dönüşen bilginin bireylerin ve kuruluşların, sosyal ve kültürel hayatın bütün alanlarında yarattığı değişimi ifade eden, farklı boyutlara sahip toplumsal bir olgudur. Temel ekonomik faaliyetlerin bilgi üzerine kurulduğu ve nitelikli insan faktörünün önem kazandığı bu yeni toplum yapısında bilgiyi topluma hâkim kılmaya aracılık eden başlıca unsur ise; teknoloji, özellikle bilgi ve iletişim teknolojileridir. (Yeşilorman, 2016)

Bilgi toplumu sosyal, kültürel, ekonomik ve siyasi hayatın bütün alanlarında ve yönetim, karar alma, Ar-Ge, üretim, satış pazarlama, lojistik vb. iş süreçlerinin her aşamasında bilgi ve iletişim teknolojileri hizmetleri kullanılarak, internet vb. iletişim ağları üzerinden ihtiyaç duyulan her türlü bilgiye erişilebildiği endüstriyel bir toplum düzeninin ifadesidir.

2.1.1. **Teknoloji**

Teknoloji sözcüğünün kökeni Antik Yunan'a kadar uzanmaktadır. Yunanca teknik, sanat, zanaat anlamında kullanılan *techne kelimesi* ile bilgi, sözcük söz gibi karşılıkları bulunan logos-logia kelimelerinin birleşiminden "bilgiden gelen teknik/zanaat" anlamında kullanılmıştır. (Yeşilorman & Koç, 2018)

Türk Dil Kurumu sözlüğünde ise teknoloji kelimesi şu şekilde karşımıza çıkmaktadır**;** (TDK, 2018)

1. Bir sanayi dalı ile ilgili yapım yöntemlerini, kullanılan araç, gereç ve aletleri, bunların kullanım biçimlerini kapsayan uygulama bilgisi, uygulayım bilimi;
2. İnsanın maddi çevresini denetlemek ve değiştirmek amacıyla geliştirdiği araç gereçlerle bunlara ilişkin bilgilerin tümü.

Woods ve Woods'un tanımına göre ise; çok çeşitli araçlar kullanılarak bir süreç içerisinde yönetilen araştırma ve çalışmalar neticesinde elde edilen somut, anlaşılır ve yararlı sonuçların tümüdür.

2.1.2. **Bilgi ve İletişim Teknolojileri - BİT**

Bilgi iletişim teknolojileri (BİT) çok çeşitli kaynaklarda bulunan bilginin üretilmesi, sistemsel olarak analiz edilmesi, depolama ortamlarında saklanması, istenildiğinde ilişkisel yönden kolaylıkla, hızlı ve doğru bir şekilde erişilebilmesi, ağ yapıları kullanılarak kullanıcılara yönlendirilmesi ve iletilmesi ile ilgili süreçlerin tamamında faydalanılan iletişim ve bilgisayar teknolojilerini içinde barındıran bütünsel yapıdır. (Atılgan, 2006)

2.2. **Bilgi Toplumunun Gelişim Süreci**

Toffler, ünlü eseri Üçüncü Dalga'da (The Third Way) toplumsal gelişim dönemlerine yönelik yaptığı analizde insanoğlunun sosyal, kültürel ve ekonomik anlamda geçirdiği iki büyük değişim dalgasından söz etmiştir. Avcılık ve toplayıcılıkla yaşamlarını sürdüren ilkel toplulukların, toprağı işlemeyi öğrenmesi, ateşin bulunması ve tekerleğin icadı gibi gelişmeler sonucunda yerleşik hayata geçmeleri ile başlayıp binlerce yıl süren tarım devrimi birinci büyük değişim dalgasıdır. 16. Yüzyılda yaşanan teknik buluşlar ve özellikle deniz yollarının keşfedilmesiyle başlayan ikinci dalga sanayi devriminin

doğuşu ve gelişimi sadece üç yüzyıl almıştır. Bugün ise, bilgi toplumu olarak adlandırılan, bilgi ve iletişim teknolojilerinin ortaya çıkışıyla çok daha hızlı bir dönüşümle yaşanmakta olan üçüncü dalga tamamlandığında insanlık tarihi açısından çok farklı bir noktaya ulaşılacağı öngörülebilmektedir.

1763'te James Watt'ın, İskoçya'da buharla çalışan makineyi bulması ve İngiltere'de kömürün hammadde ve enerji kaynağı olarak kullanılmasıyla başlayan sanayi devrimi (Oliveira, 2014), büyük bir bilgi birikiminin sonucu, modern üretim anlayışıyla, insanların yaşam biçimlerinin değiştiği, rönesans ve reform gibi sosyo-ekonomik ve kültürel yenilik hareketlerinin tetiklendiği, insanlık tarihinin en önemli değişim ve dönüşüm sürecinin temeli olmuştur.

Alcorta'nın "İlerleme ve Değişimin Evreleri" olarak tanımladığı toplumsal değişim sürecinde, makinelerin kullanıldığı seri üretime dayalı bu dönem sanayi devrimi olarak adlandırılmıştır. Hammadde ve ürün çeşitliliğiyle birlikte makinelere dayalı üretimin gücü gelişirken, demiryolları, buharlı trenler ve gemiler sayesinde düşen ulaşım ve nakliye maliyetleri, başta tekstil ve demir-çelik olmak üzere çok miktarda üretilen ürünlerin daha uzak yerlere taşınmasını sağlamış, satıcı ve alıcıların sayısının artmasıyla birlikte de ticaretin gelişmesinin önü açılmıştır. (Kent, 2018)

20. Yüzyılın başlarında çeliğin üretimde kullanılmaya başlamasıyla temel hammadde ve enerji kaynaklarında yaşanan değişim sanayi devriminin ikinci aşaması olarak kabul edilmektedir. Elektriğin keşfi ile birlikte gelişen seri üretim modeli ve işlenmiş petrolle çalışan motorlar, otomotiv sektörünün ortaya çıkmasını sağlamıştır. Telefon, radyo, gramofon, fotoğraf, sinema gibi yeni tüketim biçimlerinin sosyal yaşama dâhil

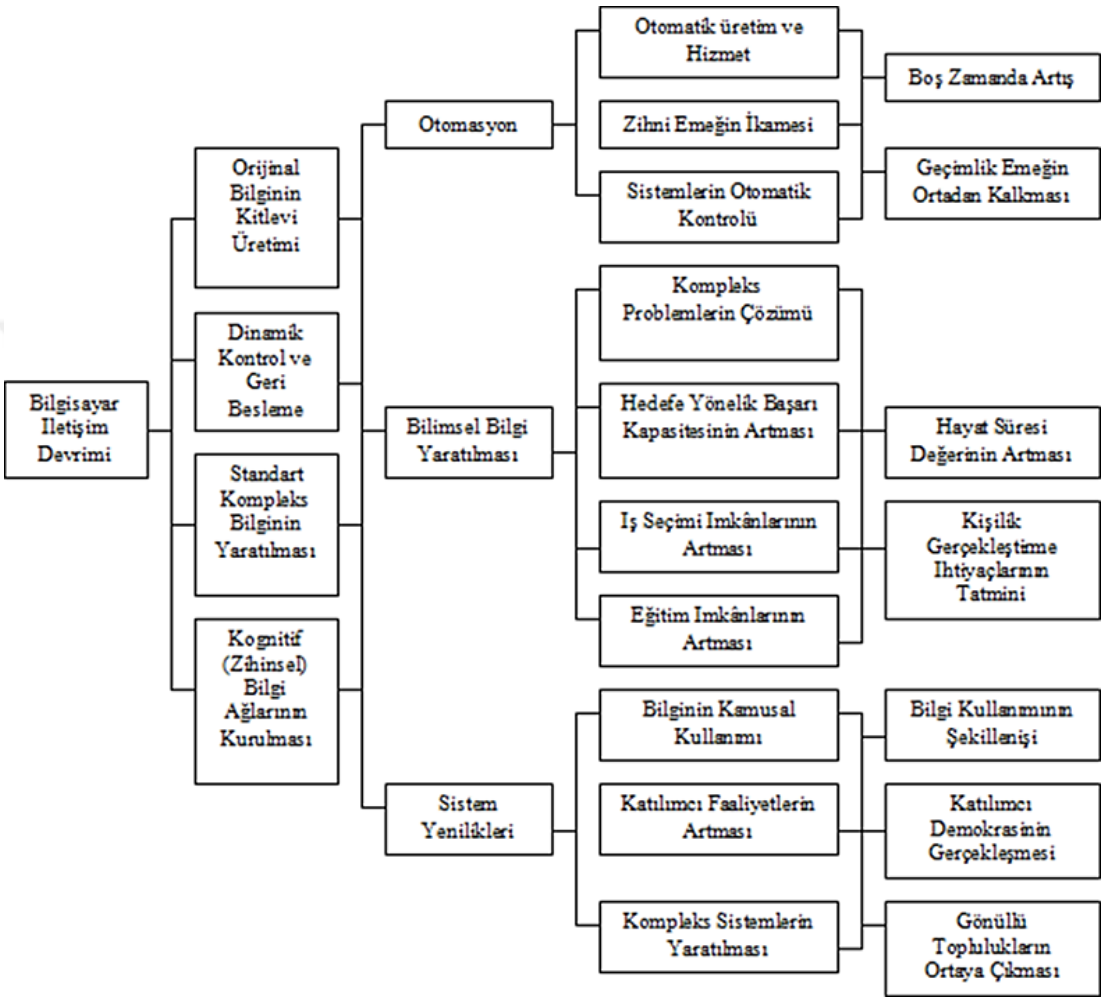
olmasıyla bilgi ve iletişim kavramlarının toplumsal dönüşümün en önemli araçları olması yolunda büyük bir adım atılmıştır. (Kavrakoğlu, 2018)

İki büyük dünya savaşının ardından 20. Yüzyılın ikinci yarısında, bilgi ve iletişim teknolojilerinde yaşanan gelişmeler, elektronik tabanlı ve programlanabilir makinelerin üretimde kullanılmaya başlaması ile birlikte sanayi devriminin üçüncü aşamasına geçilmiştir. (Tahgizadeh & Keser, 2015)

Bilgisayar, internet, telekomünikasyon, mikroelektronik, fiber optik, lazer vb. teknolojilerin ticari, sosyal ve toplumsal hayatın içerisinde yerini alması, hem bilgi süreçlerini etkin bir yapıya kavuşturmuş, hem de üretimin yönü ve biçimini farklılaştırmıştır (Siemens, 2018). Belirli bir yer ve fiziki ortama bağlı olmaksızın elektronik ortamlarda yürütülebilen iş, tasarım ve üretim modelleri ile ekonomi ve ticaret küreselleşen bir endüstriyel yapıya dönüşürken, bilgi ve iletişim teknolojileri ile sistematik olarak saklanabilmesi, düzenlenebilmesi ve gerektiğinde yeniden kullanılabilmesi bilginin tüm insanlar ve toplumlar için temel güç ve kaynak olmasını sağlamıştır. (Çalık, 2009)

Sanayi devriminin birinci aşamasına geçiş buhar makinesinin icadıyla üretimin makineleşmesi, ikinci aşama petrol ve elektriğin kullanımı ile birlikte üretimin serileşmesi, üçüncü aşama ise üretimin otomasyonu ve bilginin sayısallaşması olarak tanımlanmıştır. 20. Yüzyılla birlikte toplumsal değişimin son durağı, küresel çapta teknolojinin gelişimi sonrasında yaşanan enformasyon devrimi ile ortaya çıkan dijital bilgi toplumu olmuştur. Bilgi toplumu kavramıyla birlikte küresel çapta her alanda yaşanılan teknolojik ve bilimsel ilerleme, değişimin hızının artık öngörülemediği, bir toplumsal yapı ve bir uygarlığın kapılarını açmıştır. (Fortune, 2018)

Japon toplumbilimci Yoneji Masuda, bilgi toplumunun etkilerini "Bilgi Toplumunda Yönetim" adlı kitabında şu şekilde göstermektedir. (Ünal Y. , 2009)



Şekil 2.1 Bilgisayar İletişim Devrimi ve Toplumsal Etkileri (Ünal Y. , 2009)

Dijital dönüşüm, teknolojinin etkileşim alanı içerisinde, ticari ve ekonomik bütün faaliyetlerde küresel standartların belirleyici olduğu, daha düşük maliyetli ve daha kaliteli ürünlerin üretildiği bir üretim endüstrisini oluşturmuştur. (Özsoylu, 2017)

Enformasyon devriminin endüstri dünyasında talepten, ürün/hizmet geliştirmeye, hammaddenin tedarik edilmesinden, tasarım ve üretim verimliliğini artırmaya kadar olan bütün süreçler, siber fiziksel sistemler, nesnelerin interneti (IoT), otonom araçlar,

robotlar, artırılmış gerçeklik, büyük veri gibi gelişmiş teknolojilerle yürütülmektedir. (TÜSİAD, 2016)

Bilginin varlığı, temelleri, kaynağı gibi niceliksel problemlerin yerini bilgiyi kullanarak yine bilgiye ulaşmanın, bilgiden yararlanmanın ve bilgiyi üretmenin olabilecek en hızlı ve pratik yönlerinin bulunması odaklı, gelişmiş teknoloji altyapılı insan makine etkileşiminin sağlandığı yeni dijital dünyada yaşanan değişim ve gelişmeler, kamu yönetimi ve kamu hizmetlerinde de kendisini göstermektedir. 1990'lı yıllarla birlikte gelişmiş ülkelerde başlayıp bütün dünyaya yayılan geleneksel devlet modelinden, uygulama ve hizmetlerin çevrimiçi elektronik ortama taşındığı vatandaşların 7 gün ve 24 saat kesintisiz bir şekilde kamu hizmetlerinden yararlanabildiği elektronik devlet (E-Devlet) modeline yönelen hızlı bir dönüşüm süreci yaşanmaktadır.

III. E-DEVLET

3.1. **E-Dönüşüm**

E-dönüşüm kavramı 2000'li yılların başında dijital teknolojilerin kullanımının yaygınlaşmasıyla kurumlar ve örgütler üzerindeki etkisinin kavramsallaştırılması için ortaya çıkmıştır. Ekonomik ve sosyal hayatta iş ve işlemlerin dijital teknolojiler kullanılarak elektronik ortama aktarıldığı, izlendiği, kayıt altına alındığı ve herhangi bir zamanda ibraz edilebildiği sistemlerin genel ifadesidir.

E-dönüşüm; bir kurum, yapı ya da örgütün sahip olduğu varlık ve değerlerin, etkileşimde bulunduğu her türlü organizasyon ortamında bilgi ve iletişim teknolojilerinin etkin biçimde kullanılarak, çalışan, müşteri, iş ortakları ve diğer tüm sosyal paydaşlarının yararını gözeterek, bir bütünlük içerisinde, değiştirilmesidir. (Erkul, 2004)

Kısaca bir kurum, şirket veya yapının, iş modelleri ve organizasyon ile ilgili mevcut süreç ve hizmetlerini dijital bir altyapı üzerinden üretme ve sunmasına olanak sağlayacak şekilde yasal, yönetsel, örgütsel ve kültürel olarak düzenlemesi e-dönüşüm kavramını ifade etmektedir. (Bengshir, 2011)

3.2. **E-Devlet Nedir?**

Dijitalleşme ve teknolojinin gelişimi etkisinde üretim faktörlerinde yaşanan değişim, organizasyon, örgüt ve kurumların kendilerini yeniden yapılandırmasını zorunlu kıldığı bir ortamı da beraberinde getirmiştir. Sosyal, kültürel ve siyasal açıdan dijital süreçlerin

etkin olduğu, standartlaşma ve merkezileşmenin ötesinde bilgi üretimi/paylaşımı temelli, bir toplum ve devlet yapısının gerçekleştirilmesi artık bir zorunluluk haline gelmiştir. (Rukancı, 2004)

"Geleceğin Devleti", "Akıllı Devlet", "Dijital Devlet", (Demirel, 2006) gibi tanımlamaları bulunan e-Devlet; kamu yönetiminde hizmetlerin sunulmasında bilgi ve iletişim teknolojileri altyapısının kullanıldığı, elektronik çevrimiçi uygulamalar ile erişim hızı, kolaylığı ve zaman tasarrufu sağlayan, şeffaf, güvenilir bir yönetim yapısı olarak tanımlanabilir. (İnce, 2001)

Kamu hizmetlerinin elektronik ortama taşınarak sunulmasının bir sonucu olarak "devletin elektronikleşmesi"nin temel hedefi, teknolojinin gerçek anlamda yalnızca araç olarak kullanıldığı, bilgi işleme ve saklama kapasitesi genişletilmiş organizasyon ve uygulamalarla, çok hızlı karar alabilen ve vatandaşların ihtiyaçlarına aynı hızda cevap verebilen bir devlet yapısının oluşturulmasıdır. (Ünal F. , 2016)

3.3. **E-Devletin Etkileşim Alanları**

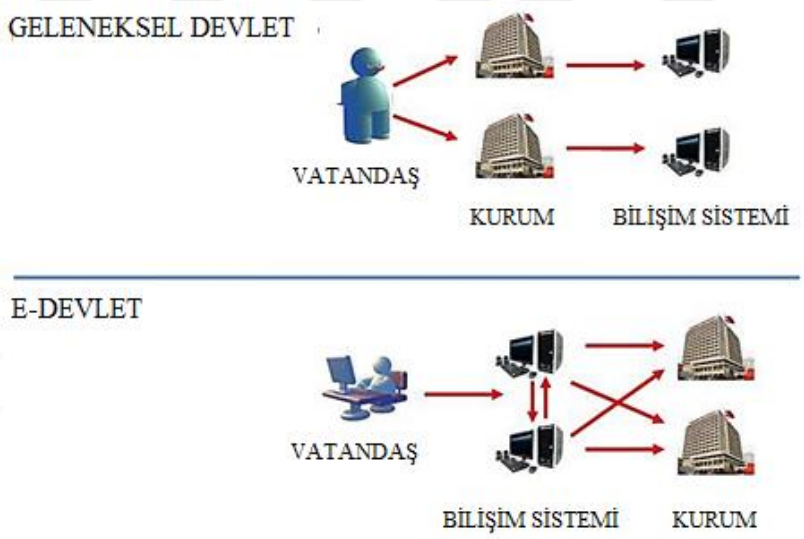
Kamusal alan ekonomik, sosyal ve idari anlamda bilgi üretiminin, kullanımının ve saklanmasının en yoğun olduğu bileşendir. Gelişen yeni teknolojik kültürle birlikte kamu yönetiminde vatandaş, kurumlar, çalışanlar ve diğer devlet birimlerinin birbirleriyle olan etkileşimleri de artmaktadır. E-Devletin etkileşim alanı içerisinde 4 temel yapı bulunmaktadır. (Özçelik, 2010)

Devlet – Devlet **Government to Government** **G2G**	Kurumlar arası bilgi akışı ve entegrasyonu sağlamak
Devlet – Vatandaş **Government to Citizen** **G2C**	Bilgi sağlama/verme amacıyla sunulan hizmetler: • Haberler, dokümanlar, raporlar, • Kamu bilgileri, • Hava-yol durumu, meteoroloji hizmetleri ve ulaşım bilgileri, • Döviz kurlan, İstatistiksel bilgiler, • Resmi gazete, mevzuat ve kanunlar, • Sanatsal ve kültürel etkinlikler. Sorgulama ve yanıt alma alma şeklinde sunulan hizmetler: • Eğitim, sosyal yardımlar, sağlık, aile ve çocuk, • Yerel yönetimler, • Kurumlara dilekçe vermek, • Ehliyet, pasaport vb. talepler, • Telefon başvurusu, nakil ve kapama, • İş/eleman arama, • Güvenlik ve askerlik, • Yargı işlemleri, Çevrimiçi işlemler olarak sunulan hizmetler: • Vergi beyannamesi ve tahakkuk işlemleri, • Bankacılık ve Sigorta işlemleri, • Kamu alımları, • Hastane randevu sistemi, dispanser ve sağlık ocakları, • Acil yardım, itfaiye ve ambulans hizmetleri, • Hazine bonolan, devlet tahvili işlemleri, • Standart, Marka, patent başvurusu, Sertifikasyon, • Bilimsel araştırma formlarına başvuru, • Öğrenci kredisi başvurusu, okullara başvuru ve kayıt, • Demokratik yönetim ve seçim, • Askerlik başvurusu, • Ulaşım, rezervasyon ve bilet alma.
Devlet – İş dünyası **Government to Business** **G2B**	Tedarikçiler, aracılar, servis sağlayıcılar, üreticiler, tüketiciler • İletişimi ve iş süreçlerini hızlandırma, verimliliği artırma, • Finansal kaynaklardan tasarruf edilmesi, • Bürokratik işleyişin ortadan kalkması, • E Ticaretin gerçekleştirilmesi, • Gümrük, vergi ve ihalelerle ilgili her türlü iş ve işlem
Devlet – Çalışanları **Government to Employee** **G2E**	Kamu Personeli için • Bilgi erişimi, paylaşımı • E-Öğrenme • Şeffaflık

Şekil 3.1 E-Devlet Etkileşim Alanları (Özçelik, 2010)

3.4. **Geleneksel Devlet E-Devlet Karşılaştırması**

E-Devlet, hiyerarşik, tek yönlü geleneksel devlet yapısı içerisinde kamu tarafından verilen hizmetlerin sunuş biçiminde karşılıklı etkileşime dayanan değişiklikler yapan bütünler şeklinde değerlendirilebilir. E-Devlet, sadece kamu hizmetlerinin sunumunu değil aynı zamanda devlet ile vatandaş arasındaki organizasyonel ilişkilerin de değişmesini sağlamıştır. E-Devlet modeli geleneksel devlet yapısının karşısında bir alternatif olarak değil, kamu kurum ve kuruluşları tarafından hizmetlerin sağlanması, üretilmesi, sunulması, işlemlerin tamamlanması ve devlete ait birimlerin planlama/karar süreçlerinin modern bilgi teknolojilerine dayalı olarak uygulanması konusunda yapılan değişiklikler şeklinde ele alınmaktadır. (Karagülmez, 2010)



Şekil 3.2 Geleneksel Devlet E-Devlet Çalışma Prensibi (Bilişim Şurası, 2002)

Şekil 3.2'de görüldüğü gibi geleneksel devlet modelinde, vatandaşın ihtiyacı olan bilginin sağlandığı bilişim sistemine erişimi olan, yöneten ana yapı kamu kurumunun kendisidir. Vatandaşın bilgiye doğrudan erişim sağlaması mümkün değildir. Vatandaştan herhangi bir bilgi talebi geldiğinde kamu kurumu gerekli bilgiye, ilgili

bilişim sisteminden erişerek aktarımını gerçekleştirmektedir. Bilgi sağlayıcı durumdaki kamu kurumlarnın bilişim sistemleri ile aralarındaki iletişim tek yönlü ve yetersizdir. Vatandaş talep ettiği bilgiye ulaşabilmek için, kamu kurumuna ulaşmak ve yüzyüze görüşmek durumundadır. Geleneksel devlet modelinde kamu hizmetlerinde bürokrasi olarak adlandırılan bu tek yönlü hizmet zorunluluğu zaman ve para kaybına yol açmaktadır. E-Devlet yapısında bilgi sistemi hizmet veren kamu kurumu ile vatandaş arasında yer almaktadır. Sunulacak tüm hizmetler vatandaşların bilgi talepleri öngörülerek sistem içerisinde ulaşılabilir bir halde, bürokratik işlemler olmaksızın hazır hale getirilmiştir. (Özçelik, 2010)

Kamu hizmetlerinin sağlanmasında gelişmiş bilgi ve iletişim teknolojileri altyapısının kullanılmasıyla birlikte kamu kurum ve kuruluşlarının faaliyetlerinde verimlilik artışı, azalan maliyetlerle bütçeden tasarruf edilmesi, güvenliği sağlanmış tek merkezden yönetilen bilgi kaynakları, daha etkin, şeffaf, denetime açık devlet yönetiminin ve yerel yönetim anlayışının sağlanması, e-Devletin yönetimsel açıdan avantajlarıdır. Devlet kurumlarıyla olan fiziksel iletişimin azalması, herkesin eşit şekilde kamu hizmetlerine erişebilmesi ve bilgi alma konusunda esneklik, kolaylık sağlaması, aktif katılım ve güvenilirlik de vatandaşlar açısından avantajlarını oluşturmaktadır. Devlete ait kamu kurum ve kuruluşları ile açık ve hızlı şekilde bağlantı kurulması, ekonomik olarak maliyetlerdeki azalma, üretim faaliyetlerindeki esneklik ve hareketlilikle rekabet gücünün ve dış pazarlara açılma olanaklarının artması da e-Devletin işletmeler açısından avantajları olarak söylenebilir. (Fadhıl, 2014)

GELENEKSEL DEVLET	E-DEVLET
Pasif Yurttaş	Aktif-Müşteri-Yurttaş
Kâğıt Temelli İletişim	Elektronik İletişim
Dikey/Hiyerarşik Yapılanma	Yatay/Koordineli Ağ Yapılanması
Yönetimimi Veri Yüklemesi	Yurttaşın Veri Yüklemesi
Eleman Yanıtı	Otomatik Sesli Posta, Çağrı Merkezi vb.
Eleman Yardımı	Kendi Kendine Yardım/Uzman Yardımı
Eleman Temelli Denetim Mekanizması	Otomatik Veri Güncellemesiyle Denetim
Nakit Akışı/Çek	Elektronik Fon Transferi (EFT)
Tek Tip Hizmet	Kişiselleştirilmiş/Farklılaştırılmış Hizmet
Bölümlenmiş/Kesintili Hizmet	Bütünsel/Sürekli/Farklılaştırılmış Hizmet
Yüksek İşlem Maliyetleri	Düşük işlem Maliyetleri
Verimsiz Büyüme	Verimlilik Yönetimi
Tek Yönlü İletişim	Etkileşim
Uyruk İlişkisi	Katılım İlişkisi
Kapalı Devlet	Açık Devlet

Şekil 3.3 Geleneksel Devlet E-Devlet Karşılaştırması (Uçkan, 2003)

3.5. **E-Devlet Türkiye**

3.5.1. **E-Devlet Uygulamalarının Tarihçesi ve Yürütülen Çalışmalar**

Türkiye'de e-Devlet uygulamaları ile ilgili ilk çalışmalar 1990'lı yıllarda başlamıştır. Ülkemizde bu dönemde, bilgi toplumuna geçiş yönünde ortaya koyulan çabalar, organizasyon seviyesinde hazırlanan rapor ve araştırma geliştirme faaliyetlerinin yanı sıra e-Devlet'in belli unsurlarını kapsayan toplumsal koordinasyona yönelik çalışmalar ön planda olmuştur.

12 Nisan 1993'de Orta Doğu Teknik Üniversitesine bağlı sunucular üzerinden TCP/IP protokolü kullanılarak ülkemizdeki ilk internet bağlantısı gerçekleştirilmiştir (ODTÜ, 2018). İnternetin kavramsal olmaktan çıkıp teknik bir kaynak haline dönüşmesi, bilginin sayısallaşması ve bilgisayarlar arasında paylaşılabilir hale gelmesi ile kamu kurum ve idareleri bilgi verme düzeyinde e-Devlet uygulamalarına başlamışlardır. Bilgi iletişim teknolojierinde yaşanan hızlı değişimin de etkisiyle 2000'li yıllardan itibaren, e-Devlet uygulamaları bütün kamu idarelerini kapsayan büyük projeler haline dönüşmüştür. Ülkemizde e-Devlet Uygulamaları ile ilgili yapılan çalışmalar kronolojik olarak şu şekilde sıralanabilir. (B.İ.T. D. Bşk., 2018)

1993 Bilişim ve Ekonomik Modernizasyon Raporu Türkiye ile Dünya Bankası işbirliğinde hazırlanarak 1993 yılında yayınlanan raporda Türkiye'de bilgi toplumuna yönelik bilgisayar kullanımı, yazılım pazarı, bilgi ekonomisinde insan kaynağı, iletişim ağları ve yasal altyapı alanında tespitlere yer verilerek bir eylem planı önerisi getirilmiştir.
1996 Türkiye Ulusal Enformasyon Altyapısı Anaplanı (TUENA) 1996 yılında Başbakanlığın görevlendirmesi ile Ulaştırma Bakanlığı tarafından Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA)'nın hazırlanması için çalışmalar başlatılmıştır.

2001 E Türkiye Girişimi

Rekabetçi, dinamik ve bilgiye dayalı ekonomiye sahip olunması ve bilgi toplumuna dönüşümün sağlanması ve E Avrupa+ Eylem Planının ülkemize uyarlanması hedeflerinin gerçekleştirilmesine yönelik olarak Başbakanlığın 9.10.2001 tarihli ve 352 sayılı Genelgesi ile E Türkiye Girişimi başlatılmıştır.

2003 E-Dönüşüm Türkiye Projesi

2003 yılında 2003/12 sayılı Başbakanlık Genelgesi ile o güne kadar farklı kurum/kuruluşlar tarafından yürütülen bilgi ve iletişim teknolojileri ile ilgili çalışmaların Devlet Planlama Teşkilatı sorumluluğunda E-Dönüşüm Türkiye Projesi adı altında birleştirilmesi kararlaştırılmıştır.

1998 E Ticaret Koordinasyon Kurulu

1998 yılında Bilim ve Teknoloji Yüksek Kurulu kararıyla, Dış Ticaret Müsteşarlığının başkanlığında ülkemizde elektronik ticaretin yaygınlaştırılması amacıyla Elektronik Ticaret Koordinasyon Kurulu oluşturulmuştur.

1998 KamuNET

1998 yılında 1998/13 sayılı Başbakanlık Genelgesi ile kamu ağları konusunda yapılan faaliyetlerin değerlendirilmesi, koordinasyonu, izlenmesi ve finansmanı amacıyla KamuNet Teknik Kurulu oluşturulmuştur. 2002 yılında eAvrupa+ ve E-Türkiye çalışmaları E-Devlet'e Geçiş Eylem Planı hazırlanmıştır.

Bilişim ve Ekonomik Modernizasyon Raporu

2006 yılında E-Dönüşüm Türkiye Projesi kapsamında bilgi toplumuna yönelik 2006-2010 Bilgi Toplumu Stratejisi ve Eylem Planı hazırlanmış ve uygulamaya konulmuştur.

2011 E-Devlet Hizmetleri Dairesi Başkanlığı

2011 yılında yürürlüğe giren 655 sayılı Kanun Hükmünde Kararname ile Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü çatısı altında e-Devlet çalışmalarının yapılması için E-Devlet Hizmetleri Dairesi Başkanlığı kurulmuştur.

2003 E-Dönüşüm Türkiye Projesi

2003 yılında 2003/12 sayılı Başbakanlık Genelgesi ile o güne kadar farklı kurum/kuruluşlar tarafından yürütülen bilgi ve iletişim teknolojileri ile ilgili çalışmaların Devlet Planlama Teşkilatı sorumluluğunda E-Dönüşüm Türkiye Projesi adı altında birleştirilmesi kararlaştırılmıştır.

2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı (BTS)

2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı

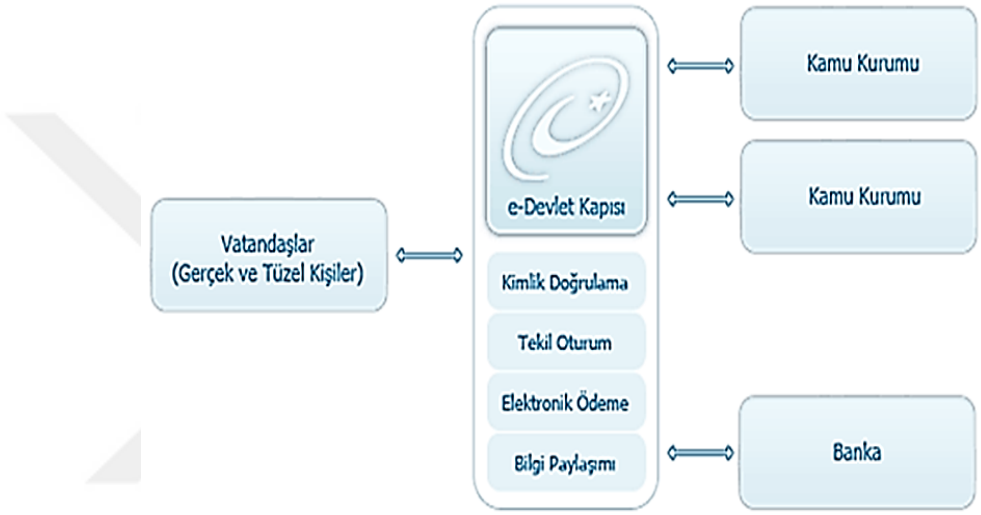
Şekil 3.4 E-Devlet Çalışmaları Tarihçe (B.İ.T. D. Bşk., 2018)

3.5.2. **E-Devlet Kapısı**

E-Devlet Kapısı, kamu kurumlarına ait hizmetlerin internet altyapısı üzerinden bilgi iletişim teknolojisi araçları kullanılarak istenilen zamanda hızlı, kolay ve güvenli biçimde vatandaşlara sunulduğu sistemsel yapıdır.

E-Devlet Kapısının İşleyişi

E-Devlet altyapısını tamamlayarak sisteme dâhil olan bütün kurumlar, www.türkiye.gov.tr adresi üzerinden kendilerine ait hizmetleri sunmaktadır. Vatandaşlar E-Devlet şifresi, elektronik ya da mobil imza, internet bankacılığı ve elektronik kimlik kullanarak sisteme giriş yaptıktan sonra bilgilerine erişebilmektedir.



Şekil 3.5 E-Devlet Kapısının İşleyişi (E-Devlet, 2018)

E-Devlet Kapısı içerisinde sisteme giriş yapan kullanıcıların profil bilgileri dışında hiçbir bilgi depolanmamaktadır. Kullanıcılar sistem üzerinden giriş yaptıktan sonra kullanmak istedikleri kamuya ait tüm hizmetlere yeniden giriş ya da kayıt yapmadan tek oturum üzerinden ulaşabilmektedir. E-Devlet Kapısı ödeme sistemi ile de hizmet alınan kurumlara ait ödemeler gerçekleştirilebilmektedir. (E-Devlet, 2018)

3.5.3. **E-Devlet İdari Yapılanma**

2011 yılında Bakanlıkların yeniden yapılandırılması ile Başbakanlık denetimi ve yönetiminde üç Bakanlık kendilerine bağlı kurumlarla E-Devlet kapsamında yapılan çalışmaları yürütmektedirler. (E-Devlet, 2018)

BAŞBAKANLIK

3056 Sayılı Kanun kapsamında

Bilim ve Teknoloji Yüksek Kurulu

Bilim ve teknoloji politikalarının tespit etmek, hedeflerin saptanması, öncelikli alanların belirlenmesi, plan ve programların hazırlanması, kamu kuruluşlarının görevlendirilmesi, özel kuruluşlarla işbirliği sağlanması, gerekli yasa tasarıları ve mevzuatın hazırlanması, araştırıcı insan gücünün yetiştirilmesi, sektörler ve kuruluşlar arasında koordinasyonun sağlanması.

Kişisel Verileri Koruma Kurulu

Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak, şikâyetleri karara bağlamak, veri sorumlularının sicilini tutmak, veri güvenliğine ilişkin yükümlülükleri belirlemek.

Müsteşarlık - İdareyi Geliştirme Başkanlığı

Kamu yönetiminin geliştirilmesi, idari usul ve işlemlerin kolaylaştırılması ve mevzuat ile ilgili çalışmaların koordine edilmesinden sorumludur.

E-Devlet Danışma Grubu

E-Devletin amaçları doğrultusunda, kamu kurum ve kuruluşlarının iş ve işlemlerinin yürütülmesiyle ilgili faaliyetlerde bulunur.

ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI

655 Sayılı Kanun Hükmünde Kararneme kapsamında

Haberleşme Genel Müdürlüğü

İnternet ve BİT altyapılarının geliştirilmesi, regülasyonun ve siber güvenliğinin sağlanması ile E-Devlet eylem planının, usul ve esaslarının belirlenmesi ve ilgili faaliyetlerin koordine edilmesinden sorumludur.

TÜRKSAT

Uydu teknolojilerindeki faaliyetlerinin yanı sıra, bilişim hizmetleri kapsamında E-Devlet Kapısı'nı işletmekte ve kamu hizmetlerinin elektronik ortamdan sunumuna yönelik projeler yürütmektedir.

Bilgi Teknolojileri ve İletişim Kurumu

Genişbant, e-imza, bilgi güvenliği ve posta hizmetleri gibi bilgi ve iletişim teknolojileri sektörüne yönelik regülasyon ve diğer tedbirlerin alınmasını, elektronik haberleşme hizmetlerinin ve altyapı şebekesinin sunulmasını sağlamaktır.

BİLİM, SANAYİ VE TEKNOLOJİ BAKANLIĞI

635 Sayılı Kanun Hükmünde Kararneme kapsamında

Bilim ve Teknoloji Genel Müdürlüğü

BİT sektörü dâhil Ar-Ge'ye yönelik politikalar, teşvikler ve standartlardan sorumludur.

TÜBİTAK

Bilim, teknoloji politikaları ve eylemleri ile bilgi toplumu ve e-Devlet için gerekli kapasite, yetkinlik ve teknolojilerin oluşturulmasına destek olmaktadır.

- TÜBİTAK-BİLGEM Bilişim Teknolojileri Enstitüsü (BTE)
- TÜBİTAK-BİLGEM Kamu Sertifikasyon Merkezi (KSM)
- TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü (SGE)
- TÜBİTAK-BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)
- TÜBİTAK-BİLGEM Yazılım Teknolojileri Araştırma Enstitüsü (YTE)

Bilim ve Teknoloji Yüksek Kurulu Sekreteryası

Bilim ve Teknoloji Yüksek Kurulu adına verilen görevleri yapmak.

KALKINMA BAKANLIĞI

641 Sayılı Kanun Hükmünde Kararneme kapsamında

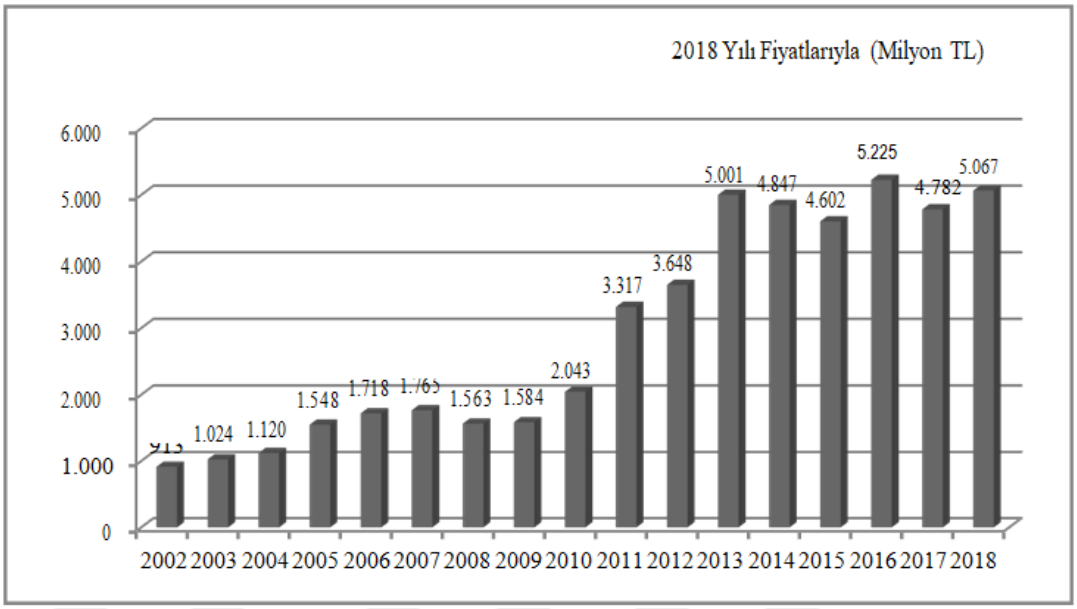
Bilgi Toplumu Daire Başkanlığı

Ulusal hedefler ile uyumlu bilgi toplumu ve bilgi ekonomisi politikalarının hazırlanması ve kamu BİT yatırımları dâhil kamu yatırımlarının planlanmasından sorumludur.

Şekil 3.6 E-Devlet İdari Yapılanma (Afyonluoğlu M. , 2018)

3.5.4. **Türkiye Kamu BİT Yatırımları ve E-Devlet İstatistikleri**

E-Devlet hizmetleri ve uygulamaları kamu tarafından finanse edilen BİT yatırımlarıyla yürütülmektedir. T.C. Kalkınma Bakanlığı (Kalkınma, 2018) ve Türkiye İstatistik Kurumu'nun (TUİK, 2018) istatistiki ölçümleme çalışmaları açısından bakıldığında ülkemizde e-Devlet'in bilgi ve iletişim teknolojisi yatırım ve tercihleri, kullanıcı-hizmet-kurum analizlerinin, ulusal düzeydeki görünümü aşağıdaki gibidir.



Şekil 3.7 Kamu BİT yatırımları 2002-2018 (BTD, 2018)

2002-2018 yılları arasında yatırım programları kapsamında kamu sektöründe bilgi ve iletişim teknolojilerine yapılan yatırımlara bakıldığında 2013 yılından itibaren e-Devlet uygulamalarının yaygınlaşmasına paralel bir artış gerçekleşmiştir. 2018 yılında 255 proje için Kamu BİT yatırımları toplam miktarı 5 milyar 67 milyon TL olarak gerçekleşmiştir. (Kalkınma, 2018)

3.5.5. **E-Devlet Kullanıcı-Hizmet-Kurum İstatistikleri**

Türkiye'de bilgi toplumu kapsamında vatandaş ve tüzel kişilerin e-Devlet kullanımı ile ilgili tercihlerini ortaya koyan istatistiki çalışmalar TÜİK tarafından yapılmaktadır. TÜİK tarafından son olarak 2018 yılı içerisinde yapılan araştırmaya ait istatistiki veriler ve e-Devlet hizmetleri kapsamında yayınlanan resmi veriler aşağıda özetlenmiştir.

Tablo 3.1 E-Devlet Kullanıcı İstatistikleri (AA, 2019)

E-Devlet Kayıtlı Kullanıcı Sayısı - Şubat 2019
41 Milyon 585 Bin Kişi
E-Devlet Kayıtlı Kullanıcıların Cinsiyete Göre Dağılımı - 2018
Kadın % 37
Erkek % 63
E-Devlet Kayıtlı Kullanıcıların Yaşa Göre Dağılımı - 2018

15-30 Yaş	31-46 Yaş	47-62 Yaş	63-78 Yaş	79- Üstü Yaş
%32,4	%35,4	%22,4	%8,3	%1,1

Tablo 3.2 E-Devlet Hizmet-Kurum İstatistikleri (TUİK, 2018) (AA, 2019)

E-Devlet Kapısı Üzerinden Hizmet Veren Kurum Sayısı - Şubat 2019
513
E-Devlet Kapısı Üzerinden Sunulan Hizmet Sayısı - Şubat 2019
4280
E-Devlet Kapısı Üzerinden Sunulan Mobil Hizmet Sayısı - Şubat 2019
1944
E-Devlet Hizmetleri Kullanımı Sayısı - 2018
2 Milyar 528 Milyon
Kişisel Amaçla Kamu Kurum / Kuruluşlarıyla İletişimde İnterneti Kullananlar - 2018
% 45,6

Tablo 3.3 E-Devlet Kapısı En Çok Kullanılan Hizmetler (E-Devlet, 2019)

1	Sosyal Güvenlik Kurumu 4A Hizmet Dökümü
2	Adalet Bakanlığı Dava Dosyası Sorgulama
3	Gelir İdaresi Başkanlığı Vergi Borcu Sorgulama
4	Sosyal Güvenlik Kurumu SGK Tescil ve Hizmet Dökümü
5	Emniyet Genel Müdürlüğü Araç Plakasına Yazılan Ceza Sorgulama
6	Sosyal Güvenlik Kurumu 4A Emekli Aylık Bilgisi
7	Tapu ve Kadastro Genel Müdürlüğü Tapu Bilgileri Sorgulama
8	Meteoroloji Genel Müdürlüğü 5 Günlük Hava Tahmini
9	Yüksek Seçim Kurulu Başkanlığı Yurt İçi Seçmen Kaydı Sorgulama
10	Sosyal Güvenlik Kurumu 4A Emekli Ödeme Bilgileri
11	Türkiye Cumhuriyet Merkez Bankası Günlük Döviz Kurları
12	Hazine ve Maliye Bakanlığı Maliye Bakanlığı e-Bordro Hizmeti
13	Adalet Bakanlığı İcra Dosyası Sorgulama
14	Bilgi Teknolojileri ve İletişim Kurumu Mobil Hat Sorgulama
15	Sosyal Güvenlik Kurumu 4A/4B İşgöremezlik Ödemesi Görme
16	Millî Savunma Bakanlığı Askerlik Durum Belgesi Sorgulama
17	Yargıtay Dava Dosya Sorgulama
18	Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü Alt-Üst Soy Bilgisi Sorgulama
19	Sosyal Güvenlik Kurumu 4C Emekli Aylık Bilgisi
20	PTT Genel Müdürlüğü Hızlı Geçiş Sistemi (HGS) Hesap Bilgileri Sorgulama

3.5.6. **Avrupa Birliği E-Devlet Endeksinde Türkiye**

2016 Ekim ayında yayınlanan rapora göre Türkiye, son ölçüm döneminde AB ülkelerine kıyasla orta üstü bir performans sergilemiştir. Aşağıdaki tabloda 2010, 2013, 2015 yılı ölçümlemeleri ile hazırlanan 2016 Avrupa Birliği E-Devlet Endeksi Raporunda yer alan karşılaştırmalı puanlar yer almaktadır.

Tablo 3.4 AB - Türkiye E-Devlet Performans Karşılaştırması (EU TR, 2016)

Ölçüm Başlığı	AB EU28+ Ortalaması %	Türkiye %
Kullanıcı Merkezlilik	77	86
Şeffaf Devlet	55	56
Sınırlar Ötesi Hizmet	56	35
Anahtar Altyapılar	54	49
Hizmet Sunumunda Şeffaflık	52	89
Kullanım Kolaylığı	80	94
Mahremiyet ve Bilgi Güvenliği	90	78

3.5.7. **Birleşmiş Milletler E-Devlet Gelişmişlik Endeksinde Türkiye**

193 ülkeyi kapsayan 2003 – 2016 yılları arasında 8 kez gerçekleştirilen e-Devlet gelişmişlik düzeyi, kullanılan çevrimiçi hizmetler, telekomünikasyon altyapısı, insan kaynağı ve kullanıcı katılımı ölçümlemelerini kapsayan Birleşmiş Milletler E-Devlet Gelişmişlik Endeksi'nin Türkiye değerlendirmeleri aşağıdaki tabloda yer almaktadır.

Tablo 3.5 Birleşmiş Milletler E-Devlet Gelişmişlik Endeksi (BM, TR, 2016)

Yıl	Ülke Sayısı	E-Devlet Gelişmişlik	Çevrimiçi Hizmetler	Telekomünikasyon Altyapısı	İnsan Kaynağı	E-Katılım
2016	193	68 (0,5900)	66 (0,6014)	88 (0,3775)	48 (0,7910)	60 (0,6271)
2014	193	71 (0,5442)	53 (0,5590)	86 (0,3604)	95 (0,7133)	65 (0,4901)
2012	193	80 (0,5281)	82 (0,4641)	80 (0,3478)	107 (0,7726)	123 (0,0526)
2010	192	69 (0,4780)	62 (0,3460)	68 (0,2581)	108 (0,8339)	55 (0,2143)
2008	192	76 (0,4834)	71 (0,4214)	68 (0,2191)	106 (0,8116)	78 (0,1364)
2005	191	60 (0,4960)	46 (0,5231)	68 (0,1648)	101 (0,8000)	34 (0,2857)
2004	191	57 (0,4892)	38 (0,5328)	69 (0,1648)	110 (0,7700)	26 (0,2951)
2003	191	49 (0,5060)	24 (0,5550)	59 (0,1920)	105 (0,7700)	48 (0,2070)

IV. VERİ KAVRAMI

Veri (data), dijital dünyada adını sıklıkla duyduğumuz, gün geçtikçe yapısal olarak kullanım alanı genişleyen ve önemi daha da artan bir kavramdır. Veri kavramı araştırma, deney, gözlem, internet, sosyal medya, sensörlerden vb. çok farklı ortamlardan elde edilen genel bir terimi ifade etmektedir (Arslantekin & Doğan, 2015).

4.1. **Verinin Tanımsal Çerçevesi**

4.1.1. **Veri, Enformasyon, Bilgi**

Veri, enformasyon ve bilgi kavramları tanım ve içerik olarak farklı olsa da birbirleriyle doğrudan ilişkisel olarak bağlı kavramlardır. Bilimsel çalışmalarda ve araştırmalarda, aralarındaki yapısal ilişki sebebiyle veri, bilgi ve enformasyon kavramlarının birlikte değerlendirildiği, yorumlandığı görülmektedir

Veri (Data)

İngilizce data ile ifade edilen, etimolojik olarak Latince'de vermek-çıkartmak anlamındaki dare sözcüğünden gelen veri, herhangi bir olgudan soyutlanarak (çıkartılarak) araştırma, bilgi edinme, tartışma, akıl yürütme yoluyla oluşturulan işlenmemiş, üzerinde yorum yapılacak düzeyde sistemleştirilmemiş, farklı yöntem ve teknikler kullanılarak ölçülen ve kayıtlanan ham bilgidir. (Binark, 2017)

Bilgi işleme süreci açısından veri, çeşitli semboller ve işaretlerle ifade edilen bilgisel gerçekliğin, düşüncelerin ve görüşlerin işlenmemiş ham halidir (Öğüt, 2003).

Özümlenmemiş ve yorumlanmamış gözlemler, işlenmemiş gerçekler, işlenmemiş bilgidir (Barutçugil, 2002).

Enformasyonun ve bilginin temelini oluşturan, ilişkilendirilme, gruplandırılma, yorumlanma, anlamlandırılma ve analiz edilmeye gereksinim duyulan ham bilgi olarak tanımlanan veri, tek başına anlam ifade etmez veya kullanılamaz (Yılmaz, 2009). Veri, bilişim teknolojileri açısından sayısal/dijital ortamlarda bulunan, işlenen veya taşınan sinyaller, anlamlı hale dönüştürülmemiş bitler veya birbiriyle bağlantısı henüz kurulmamış bilinenler olarak tanımlanabilir. (Sağıroğlu, 2017)

Veri, bir olguya ait fiziksel ve fiziksel olmayan sayı, ağırlık, uzaklık, yükseklik, hacim, başarı durumu, toplumsal sınıf, psikolojik durum vb. gibi nicel özellikli sayısal kayıtlardan ya da metin, elektromanyetik dalga, sembol, ses, resim, video vb. formundaki nitel yapıdaki sayısal olmayan kayıtlardan oluşur. (Kitchin, 2014)

Enformasyon (Information)

Enformasyon kelimesi Türkçe sözlükte İngilizce information kelimesinin karşılığı olarak kullanılan bilgi verme, haber verme, haberleşme (TDK Sözlüğü 2018) şeklinde ifade edilmektedir. Enformasyon verilerin belirli bir amaç doğrultusunda anlamlı bir şekilde bir araya getirilmesi, düzenlenmesi ile oluşur (Yılmaz, 2009).

Enformasyon, herhangi bir konu, düşünce ya da yapıyla ilgili bilinmeyenler hakkında varolan belirsizliğin giderilmesi, anlaşılması, yorumlanabilmesi konusunda organizasyonel olarak yardımcı olan tanımlayıcı, betimleyici, açıklayıcı ifadelerdir. Örneğin, bir şirketin bu yıl satışlardan en çok hangi üründen kar ettiğini, bilet satın almak istediğimiz filmin nerede gösterildiğini ya da bir tiyatro oyununun nerede

sergilendiğini veya satın almak istediğimiz bir ayakkabının hangi mağazada olduğunu bilmek, enformasyon sahibi olmaktır. (Çelebioğlu, 2018)

Bilgi (Knowledge)

Bilgi kavramı ilk ortaya çıktığı dönemlerde nesne ile içerik arasındaki ilişki olarak tanımlandığı felsefenin tartışma ortamı içerisinde yer alırken, zaman içerisinde farklı bilim alanlarının ortaya çıkışıyla geniş bir çerçevede bütün bilim dallarının ortak konusu haline gelmiştir. Değişen koşullarla birlikte önceleri sadece insanı geliştiren, sekillendiren haber değeri olan bir olgu olarak tanımlanan bilgi günümüzde üretilen, üzerinde işlem yapılabilen, alınıp satılabilen bir değere dönüşmüş durumdadır. Düşünme, karar verme, problem çözme değerlendirme, akıl yürütme, iletişim gibi zihinsel süreçlerin tamamında kendisine yer bulan bilgi kavramı birçok farklı tanımla ifade edilmeye çalışılmaktadır. (Uçak, 2010)

Bateson'a (1979) göre bilgi insan beyninde farklılık meydana getiren, bilişsel yapısında değişiklik yaratan herhangi bir şeydir.

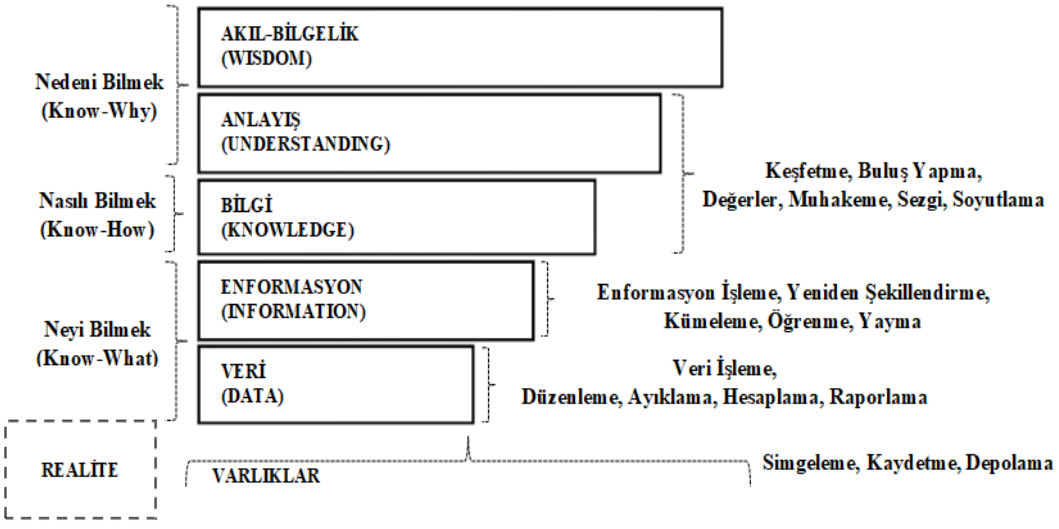
İnsanın olayları ve olguları tanıma, anlama ve açıklayabilmesine yönelik, eğitim, gözlem, araştırma yoluyla edindiği deneyimleri zihinsel değerledirme süreçlerinden geçirdikten sonra ortaya çıkan olgular veya fikirlerin bütünüdür. (Gürak, 2006)

Bilgi, duygu, deneyim, sezgi vb. farklı yollarla elde edilen veri ve enformasyonun düşünce ve akıl yoluyla yorumlanarak doğuştan getirilen kişisel özelliklerle birleştirilmesi ve planlama, değerlendirme, analiz etme, tahminde bulunma gibi süreçlerin yürütülmesinde kullanılan şeklidir. (Çapar, 2008)

Bilginin temelini veri ve enformasyon oluşturmaktadır. Üzerinde işlem yapılmamış veriler sınıflandırılma, düzenleme, hesaplama, aktarılma ya da düzeltilme gibi içeriksel işlemlerin sonucunda bir değer kazanarak enformasyona dönüşür (Kalseth & Sarah, 2001). Enformasyonun öğrenme, karar verme, planlama, keşfetme, karşılaştırma, değerlendirme, analiz, tahmin, tanı vb. (Çapar, 2005) gibi zihinsel süreçlerle içselleştirilmesi ve yorumlanmasıyla bilgiye ulaşılır. En açık haliyle bilgi, insanın yaşamın her alanında olup biten şeyleri tam ve doğru olarak kavramasını sağlayan düşünceler, fikirler, öngörüler ve deneyimlerdir (Barutçugil, 2002). Veri, enformasyon ve bilgi kavramlarını anlamak için şu örneği verebiliriz:

1 ABD Dolar'ının 2015 Aralık ayında 2,90 TL olması bir veridir.

1 ABD Dolar'ının Aralık 2015'den Aralık 2018'e kadar geçen sürede 2,90 TL'den 5,30 TL seviyelerine çıkması ise bir enformasyondur. Bu enformasyonu yorumlamamıza ve ekonomi yönetimi yaparken lehimize kullanmamıza yarayan herşey ise bilgidir.



Şekil 4.1 Anlam Şeması Laszlo ve Laszlo (Aktan C. C., 2005)

Tablo 4.1 Veri, Enformasyon, Bilgiye Kavramsal Bakış (Durna & Demirel, 2008)

Yazarlar	Veri	Enformasyon	Bilgi
Wiig	-	Bir durum veya koşulu betimlemek için organize edilmiş gerçekler.	Gerçekler ve inançlar, perspektifler ve kavramlar, yargılar, beklentiler, metodolojiler, Know-how.
Nonaka; Takeuchi	-	Anlamlı mesajların akışı	Mesajlardan üretilen bağlılıklar, inançlar.
Spek; Spijkervet	Henüz yorumlanmamış semboller	Anlamlı veriler	Anlam kazandırma yeteneği.
Davenport	Basit gözlemler	Alakası ve amacı olan veriler	İnsan aklından ortaya çıkan değerli enformasyon
Dovenport; Prusak	Birbirinden farklılaşmış olgulardan oluşan bir set	Alıcının ön kabulünü değiştirmek için gönderilen bir mesaj	Deneyimler, değerler, kavrayışlar ve bağlamla ilişkili enformasyon
Quigley; Debons	Özel durumlar için bir anlam ifade etmeyen metinler	Kim, ne zaman, ne, nerede gibi sorulara cevap veren metinler	Niçin ve nasıl sorularına cevap veren metinler
Choo, vd.	Olgular ve mesajlar	Anlam ifade eden veriler.	Haklılığı görülmüş gerçek kanaatler.
Hussain	Gerçekler, ölçümler ve istatistikî değerler toplamı.	Zamanlı ve kesin olan, düzenlenmiş işlenmiş veri	İçeriksel, anlamlı ve uygulanabilir enformasyon.
Tuomi	Enformasyona dönüştürülmek üzere biçimlendirilebilen ham gerçekler	Verilerin yorumlanarak içerik kazandırılmış hali	Enformasyonun yorumlanarak, içerik kazandırılması, bir anlam katılarak, bilgiye dönüştürülmesi.
Marchand	-	İfadeleri, görüşleri kullanarak duyma, toplama, düzenleme, işleme, iletme	Kişisel yorum ve anlayış üzerinde durur
Terra; Angeloni		Organize olmuş, yorumlanabilen veri.	İnsan beyninde oluşan deneyim ve tecrübeye dayanan inançlar
Hey	İşlenmemiş enformasyon, objektif olguların temsili.	Elektronik kanallarla akışı sağlanır, sınırlı bir şekilde anlamlandırılır.	Bireylerin deneyim ve tecrübeleriyle biçimlendirilen, genelleştirilebilen enformasyon.

İnternet, bilgi iletişim teknolojileri ve mobil teknolojilerdeki gelişmelerin sonucunda üretilen ve depolanan verinin çeşitliliği ve miktarı her geçen gün artmaktadır. Daha önce sadece yazılı metin biçiminde depolanabilen veri parçaları dijital teknolojiyle birlikte sesli görüntülü vb biçimlerde de depolanmayı desteklemektedir. Verilerin miktarı, büyüklüğü veya çeşitliliği artarken, veri boyutu Petabyte, Exabyte, Zettabyte, Brontobyte, Geopbyte gibi yeni kavramlarla tanımlanmaktadır.

İnsan, makine ve nesne tabanlı birçok farklı kaynaktan elde edilen verilerin toplanmasını, ayrıntılı biçimde değerlendirilmesini, karar verme süreçleriyle analizinin

yapılmasını ve tekrar kullanılmasını içeren teknolojileri kapsayan büyük veri kavramı günümüz dijital dünyasında önemli bir alanı teşkil etmektedir.

4.2. **Büyük Veri (Big Data)**

Büyük veri (big data) yüksek hacimdeki ve hızdaki veriler ile ilgili konularla birlikte, çeşitlilik içeren, yapısal olmayan nitelikli video, ses, metin vb. verilerin saklanması, yönetilmesi ve işlenmesi yoluyla bilgiye erişimin sağlanmasını ifade etmektedir.

Diğer bir ifadeyle, ilişkisel veri tabanı yönetim sistemleri ve yazılım kaynaklarının veriler üzerinde gerçekleştirdikleri analiz ve çözümleme yeteneklerini aşan (Karaca, 2015), depolama özellikleri gelişmiş, dağıtık paralel işlem kabiliyetine sahip sistemlerin kullanımını gerekli kılan büyüklükteki yüksek hacimli ve farklı konfigürasyonlara sahip verilere büyük veri (big data) denir. (Aktan E. , 2018)

Büyük veri hem farklı kaynaklardan toplanan devasa boyutlardaki verilerin çeşitliliğini hem de bu verilerin özel olarak toplanması, birleştirilmesi, işlenmesi ve analizi için kullanılan karakteristik uygulamaları ve teknolojileri kapsamaktadır. (Arslantekin & Doğan, 2015)

4.2.1. **Büyük Verinin Yapısal Özellikleri**

Büyük veri yapısal olarak beş temel dinamikle değerlendirilmektedir. Verilerin üretilmesi, toplanması, dönüştürülmesi, analiz edilmesi gibi bütün süreçleri kapsayan, Çeşitlilik (Variety), Hacim (Volume), Hız (Velocity), Doğrulama (Veracity), ve Değer (Value) kavramları büyük verinin yapısal bileşenlerini oluşturmaktadır.

Çeşitlilik (Variety): Verinin çeşitliliği farklı kaynaklar tarafından üretilen farklı özelliklere sahip verileri ifade etmektedir (Dokuz & Çelik, 2018). Sosyal ağ verileri, web platformlarının verileri, mobil uygulama verileri, konum verileri, kurum-devlet verileri, uzay, uydu, sonar vb. bilimsel veriler, makine ve sensör verileri gibi makineler ve bilgisayarlar tarafından üretilen veya bilgisayar aracılığıyla insanlar tarafından üretilen biçimsel olarak yapılandırılmamış veriler büyük verininin çeşitliliğini açıklamaktadır.

Tablo 4.2 Büyük Verinin Kaynakları (Eyüpoğlu, 2017)

• **Ağ ve Sistem Verileri**
Ağın durumu, yetkisiz erişimler, IP adresleri, web logları, internet arama kayıtları vb.
• **Mobil Cihaz Verileri**
GPS yer bildirimleri, arama, mesaj, uygulama kayıtları,
• **Sosyal Medya Verileri**
Facebook, Instagram, Twitter, Google Drive, vb.
• **Kimlik/ Kimlik Doğrulama Verileri**
Kullanıcı adı, şifresi vb., kimlik doğrulamada kullanılan dijital sertifikalar,
• **Sağlık ve Biyometrik Kimlik Tanıma Verileri**
Genetik, ilaç kullanımı, hastalık, parmak izi, iris, ses tanıma vb., kayıtlar,
• **OTP (One Time Passwords)**
Bankacılık işlemleri, e-Devlet gibi çevrimiçi erişimde kullanılan tek seferlik şifreler,
• **Sensör Verileri**
Üretim hatlarında kullanılan makine ve cihazlara entegre sensörler, trafik akışı vb.,
• **Bilimsel Veriler**
Uzay araştırmaları, uydu, sonar, takibi, hava tahminleri,

Hız (Velocity): Hız, büyük veri nesnelerinin oluşturulması ve eklenmesi sonrasında görülebilen farklı kavramları ele alan birleşik veri altyapısı ve veri yönetimi sürecidir (Techopedia, 2018). Dijital dünyada yüksek bant genişliği ve internet hızı ile sistemler üzerindeki bilgi akışı ve veri üretimi çok hızlı gerçekleşmektedir. Olağanüstü hızda üretilen ve büyüyen veri ile birlikte veri üzerinde yapılan işlem sayısı ve çeşitliliği de aynı hızda artmaktadır.

Hacim (Volume): Kısaca verinin fiziksel büyüklüğünün ifadesidir. Günümüzde petabytelar seviyesinde yüksek boyuttaki verilerin analiz edilmesi ve işlenmesi için kullanılacak sistemler ya da yapıların geliştirilmesiyle ilgili verilecek kararlarda ilk düşünülmesi gereken özelliktir. (Sağıroğlu, 2016)

Doğrulama (Veracity): Doğrulama, doğruluk genellikle toplanan verilerin kalitesi veya güvenilirliği olarak tanımlanır. Üretilen verinin kirli ve bozulmamış olması gerekir. Elde edilen verinin geçerliliğini yitrimemiş olması, anlamlı ve doğru olması gerekliliğini ifade eder. Büyük verinin yaratacağı değer ancak doğruluğuna bağlıdır.

Değer (Value): Değer, üretilen ve analizi yapılan verilerin değerini ifade eder. Sonsuz miktarda veriye sahip olmak, her zaman yüksek değerli verilere sahip olmak anlamına gelmez. Çevrimiçi araçlar genişledikçe ve İnternet'teki kullanıcı sayısı her geçen gün arttıkça, büyük veriden yararlanmak değer yaratmada kritik öneme sahip olmaktadır. (Shannon, 2018)

4.2.2. **Büyük Veri Uygulamalarının Kullanıldığı Alanlar**

Gelişmiş BT mimarileri ve çözümleriyle şekillenen büyük veri teknolojileri, imalat, enerji, lojistik, bankacılık, finans, telekomünikasyon, sağlık, perakende, tarım, ulaşım

gibi endüstriyel dünyada veri toplayan bütün sektörlere, iş-hizmet uygulamalarını ve üretim-yönetim süreçlerini iyileştirmek, yeni karar alma mekanizmaları ve stratejileri oluşturmak için fırsatlar sunmaktadır.

İmalat/Üretim

Büyük verinin sağladığı öngörüyle yapılan gelişmiş analizlerin, finansal ölçümlerle birleşmesi, endüstriyel üretime entegre büyük veri teknolojileri ile gerçek zamanlı süreç kontrolü takibi, tedarik zinciri analizi, kapasite kullanımı ve tahmini, makinelerin, sensörlerin, denetleyicilerin optimizasyonu vb. süreçlerde verimlilik ve kalite artışı sonucunu doğurmaktadır. (Columbus, 2014)

Enerji

Enerji sektöründe büyük veri, enerji verimliliğini artırmak, akıllı ölçüm cihazları ve hava durumu bilgi sistemleri, yenilenebilir enerji kaynaklarıyla (güneş, rüzgâr enerjisi) ilgili tahmin ve hesaplamalar, gerçek zamanlı görüntüleme, akıllı sayaç analizi, enerji dağıtım şebekelerinde iletim, cihaz ve ekipmanların uzaktan kontolü gibi uygulamalarıyla karşımıza çıkmaktadır.

Lojistik

Lojistik yönetim sürecinde büyük veri teknolojileri, otomatik tanıma, operasyonları gerçekleştirme, stratejik fayda için entegrasyon, gözlem, karar verme ve planlamada kullanılır. Fayda maliyet analizleri yapılarak seçilen büyük veri teknolojileri, farklı işletmelerin altyapılarına dahil olarak daha az kaynak kullanılarak iş süreçlerinin etkin biçimde yönetilmesini sağlamaktadır (MÜSİAD, 2017). Dağıtım ve lojistik optimizasyonu, GPS konum izleme, RFID okuyucular, araç iletişimi, analizi gibi

uygulamalar ile, araç bakımı, zaman, yakıt tüketimi gibi kaynaklardan önemli ölçülerde tasarruf edilebilmektedir.

Bankacılık, Finans

Büyük Veri; müşteri takibi yapabilen mobil teknolojilerle uyumlu veri görselleştirme araçları ve bulut ödeme sistemleri gibi uygulamalarla, bankacılık ve finans sektörüne; dolandırıcılık tespiti, kredi risk analizi, müşteri duyarlılığı ile ürün tekliflerini belirleme gibi fırsatlar sağlamaktadır. (Exastax, 2018)

Sağlık

Sağlık kurumlarındaki büyük veri uygulamaları, bireylerin kendi tıbbi verilerine erişmelerini ve sağlık durumları ile bilgilenmelerini sağlayan Kişisel Sağlık Kayıt Sistemleri (PHR) gibi çeşitli sistemlerde karşımıza çıkmaktadır. Bu sistemler ve sensörler üzerinden elde edilen veriler klinik araştırmalar, genetik tanılama, DNA analizi, kişiselleştirilmiş tıp, gerçek zamanlı hasta izleme, ilaç ve tıbbi malzeme kullanımı analizi gibi sağlık endüstrisindeki farklı hizmetlerin yürütülmesinde ve geliştirilmesinde kullanılmaktadır. (Gaitho, 2018)

Telekomünikasyon

Telekomünikasyon operatörleri/şirketleri, mobil telefonlar, çağrı detay kayıtları, web sunucusu günlükleri ve sosyal ağlardan çok miktarda müşteri verisini toplamaktadır. Operatörler/Şirketler, konum tabanlı hizmetler, cihaz verilerinin takibi, tıklama, satın alma, çağrı merkezi analizleri, abonelerin erişim sağladığı noktalarda şebeke kapasite ve altyapı planlaması, kullanıcıların DNS kayıtlarından en çok erişilen sitelerin tespit edilmesi gibi pek çok süreç için büyük veri uygulamalarını kullanmaktadır (Mc Donald,

2017). Operatörler/Şirketler gerçek zamanlı çağrı verilerini analiz ederek müşteri verilerinin korunması, yetkisiz cihazların tanımlanması, ödeme işlem takibi, hacking, dolandırıcılık, siber saldırı gibi güvenlikle ilgili riskleri tespit edip önleyebilmektedir (Exastax, 2017).

Pazarlama, Perakende

Müşterilerin web sitelerindeki hareketleri, konum/yer bilgileri, sosyal medya davranışları, alışveriş alışkanlıkları, kullanılan ödeme yöntemleri vb. verilerin şirketler/firmalar tarafından toplanıp analiz edilmesi ve varolan verilerle bütünleştirilmesiyle ayrıntılı müşteri analizleri yapılabilmesine olanak sağlamaktadır. (Dal, 2013)

Tarım

Tarım Endüstrisinde, günlük işlerin verimliliğini artırmak için sensör teknolojileri sayesinde çiftçiler bölgedeki topografya ve kaynakların yanı sıra toprak asitliği, hava koşulları tahmini gibi değişkenlerle ilgili bilgilere ayrıntılı bir şekilde sahip olabilmektedir. Mobil teknolojiler üzerinden çiftçiler ürünlerini, hayvanlarını uzaktan izleyip, takip ederek, besleme ve üretme konusunda istatisikleri derleyerek gelecek tahmininde bulunabilmekteler. (Meola, 2016)

Kamu Devlet

Büyük veri vatandaşlara sunulan kamu hizmetlerin kolaylaştırılmasında, güvenliğinin sağlanmasında veya verimlilik kapsamında daha etkin kullanım imkânları sağlamaktadır. Devletler savunma, ulusal güvenlik, enerji araştırmaları, ekonomi, çevre koruma, sosyal hizmetler, hava durumu tahminleri, su tüketim analizleri, trafik akışının

düzenlenmesi siber güvenlik, suç tahmini ve önleme gibi farklı uygulama alanlarında büyük veriyi kullanmaktadır. (Doğan, 2014)

Küresel öngörüler, Büyük Veri ile ilişkili teknolojilerin daha çok uygulama alanı bulacağını ve sürekli yükselen bir eğilim göstereceğini işaret etmektedir. Amazon, Google ve Microsoft, Oracle, SAP gibi dünyanın teknoloji devlerinin yaptıkları yatırımlarla büyük veri yönetiminde söz sahibi yazılım şirketlerini satın aldıkları görülmektedir (Grant, 2018). International Data Corporation (IDC) Uluslararası Büyük Veri ve Analiz Harcamaları raporunda 2017 yılı itibariyle, bilgi tabanlı ürünlerden elde edilen gelir artışının Fortune 500 şirketlerinin üçte biri için ürün/hizmet portföyünün geri kalanını ikiye katlayacağını öngörmüştür. Büyük veri teknolojileri ve iş analitiği uygulamaları için dünya çapındaki pazar gelirlerinin 2020 yılında 200 milyar doları aşacağı tahmin edilmektedir (IDC, 2017).

GO Globe'ın hazırladığı 10 dakika dergisi tarafından Türkçeleştirilen "İnternette 60 Saniye" isimli infografik büyük verinin çeşitli kaynaklardan ne kadar hızlı üretildiğini göstermektedir. (Go Globe, 2017)

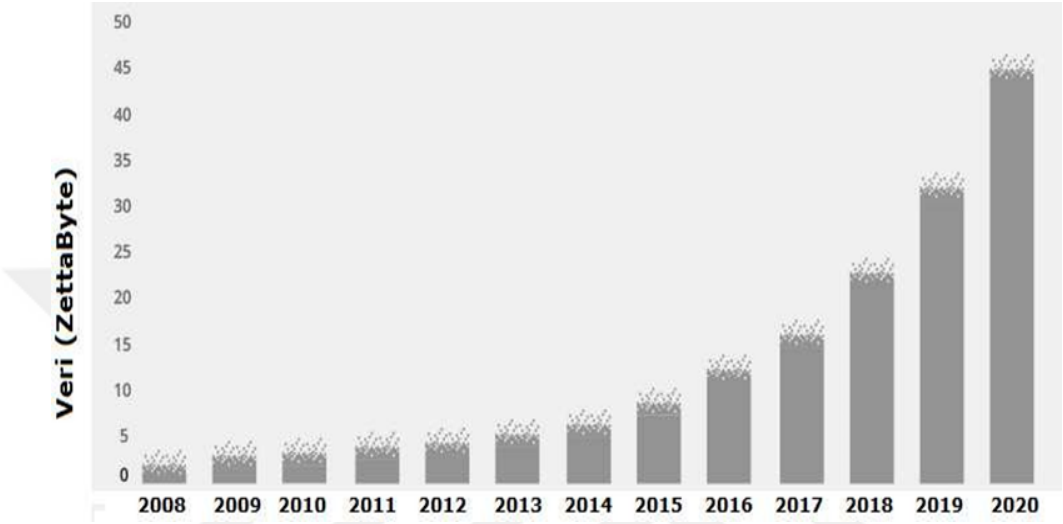
Tablo 4.3 İnternet'te 60 Saniyede Neler Oluyor? (Go Globe, 2017)

Apple Store'da 13.000 uygulama indiriliyor
Tumblr'da 20.000 gönderi giriliyor
Skype'e 2 milyon dakika telefon görüşmesi gerçekleştiriliyor
Whatsapp'ta 29 milyon mesaj, 1 milyon fotoğraf ve 175 bin video paylaşılıyor
Twitter'da 350 bin yeni tweet atılıyor
Instagram'a 65 bin yeni fotoğraf ve video yükleniyor
Facebook'da 695.000 durum güncellemesi, 510.040 yorum yapılıyor
Google'da 3,8 milyon arama işlemi gerçekleşiyor
Dropbox'a 800 bin yeni dosya transfer ediliyor
Foursquare'da 5500 yer bildiriminde bulunuluyor
Netflix'te 87 bin saat video izleniyor
168 milyondan fazla e-posta gönderiliyor
Youtube'a 400 saatlik yeni video ekleniyor, 700 saatlik video izleniyor

Dünyanın en büyük mağazalar zincirlerinden Wal-Mart'ta bir saat içinde 1 milyondan fazla müşteri işlemi gerçekleşiyor. Bu işlemler sonucu veri tabanlarına ulaşan günlük olarak yaklaşık 2.5 Petabyte'dan fazla bilgi Amerikan Kongre Kütüphanesi'ndeki bilginin 167 katı büyüklüğündedir. (Bernard, 2018)

Hootsuite ve we are social'ın 2017 Küresel Genel Bakış Raporuna göre geniş bant altyapılı internet ve akıllı telefonların kullanımı ile veri trafiği hacminde yıllık bazda %50 artış sağlanmıştır. Dünya genelinde yaklaşık 4 milyar internet kullanıcısı her ay 7 milyar Gigabyte'tan fazla veri trafiği oluşturmaktadır. Dijital dönüşümün önemli donanım yapılarına bakılacak olursa, yapılan tahminlere göre, 2020 yılı itibariyle, 200

milyardan fazla sensör, 50 milyar aygıt, 2,5 milyar insanın yüksek hızlı veri ağlarına erişimi, 4,5 milyar uygulama kullanıcısı ve 50 Exabyte büyüklüğünde veri trafiğinin oluşacağı ön görülmektedir. (Yıldız T. , 2017)



Şekil 4.2 Dünya'da Büyük Veri Hacminde Öngörülen Büyüme Grafiği (Tosun, 2017)

Elektronik ortamlarda yapılan işlemler sonucunda, kullanıcıların eş zamanlı olarak etkilişimde bulunduğu farklı kaynaklardan gelen verilerin sınıflandırılması ve analizinin yapılması veri örüntüleri açısından mahremiyet kavramını ortaya çıkarmıştır. Tek başına önemli olmayan, içerisinde farklı veri seti kümeleri barındıran verilerin, büyük veri işleme teknolojileri ile istatistiksel analizi ve veri madenciliği sonucunda birleştirilmesiyle paylaşılmamış durumdaki kişisel verilere erişilebilmektedir.

4.3. **Kişisel Veri (Personal Data)**

4.3.1. **Kişisel Verinin Tanımı ve Kapsamı**

Kişisel veri kavramı ile ilgili alanyazın incelendiğinde uluslararası kanun ve mevzuatlarda farklı tanımlarla ifade edildiği görülmektedir. 28 Ocak 1981 tarihli Kişisel

Verilerin Korunmasına İlişkin Avrupa Konseyi Sözleşmesinde (md. 2 a) ve 24.10.1995 tarihli, Kişisel Verilerin İşlenmesi Karşısında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği hakkındaki direktif metninde (95/46/EG) kişisel veri, kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgiler şeklinde tanımlanmıştır. (EC, 1981)

Kişisel veri yapısal olarak tanımlanırken genel anlamda bir verinin kişisel veri olmasını sağlayan iki temel unsur vardır. Bilginin gerçek bir kişiye ait olması ve bu kişinin belirli ya da belirlenebilir olması. Kişisel veri esas olarak, belirli veya belirlenebilir bir gerçek kişiye ait kişisel, sosyal, ekonomik ve kültürel durumu, ilişkileri hakkındaki nesnel ya da öznel nitelikteki tüm bilgileridir.

Ülkemizde kişisel verinin tanımı 24.03.2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanununda "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi" şeklinde yapılmıştır. (Resmi Gazete, 07.04.2016)

Anayasa Mahkemesi kişisel veriyi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan, bütün veriler olarak tanımlamıştır. Bu tanıma göre; kimlik ve aile bilgileri (Ad soyad, doğum yeri ve tarihi vb.), meslek, adres, telefon numarası, taşıt plakası, sosyal güvenlik numarası, sağlık ve genetikle ilgili kayıtlar (kan grubu, parmak izi, hastalık vb.), bilişim teknolojileri kullanımı (IP adresi, e-posta adresi, metin, görüntü, ses, video vb.), cinsel tercihler, siyasi görüş, düşünce ve faaliyetler, gibi kişiyi kesin olarak teşhis edip tanımlayan ya da kişi ile ilişkilendirilerek kişinin belirlenebilir olmasını, tanınmasını sağlayan verilerin tamamı kişisel veri olarak kabul edilebilir. (Anayasa Mahkemesi, 2014).

Kişisel veriler, belirli veya belirlenebilir bir gerçek kişiye ait kişinin öznel nitelikleri olabileceği gibi üçüncü kişiler ile yaptığı sesli-görüntülü her türlü iletişimin içeriği,

hareket, konum bilgileri gibi nesnel ilişkilerini de içermektedir. Kişisel veri, verinin toplanması, işlenmesi, analizi, iletilmesi ve saklanması süreçlerinde kullanılan teknolojik araç ve yöntemlerden bağımsız olarak farklı kaynaklardaki bilgiden türetilmiş kişiyi tanımlayan her türlü üründür. (Ayözger, 2016)

4.3.2. **Kişisel Veri Türleri**

Hassas (Özel Nitelikli) Kişisel Veriler

Hassas kişisel veriler, temel haklar ve özel yaşamın gizliliği kapsamında, ifşa edilmesi ve başkaları tarafından öğrenilmesi durumunda kişiyi sosyal açıdan zor duruma düşürecek, ayrımcılığa maruz bırakabilecek nitelikteki (etnik kökeni, ırkı, dini/felsefi inanışı, siyasi görüşleri, psikolojik durumu, genetik ve sağlık kayıtları, cinsel yaşamı ve ceza mahkûmiyeti vb.) bilgilerini ortaya çıkartabilecek, daha fazla koruma uygulanması gereken veri grubudur. (Kaya C. , 2011)

Hassas kişisel veriler, 1995/46/EC VKD ve Avrupa Konseyi'nin Ocak 1981 tarih ve 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme m.6 kapsamında özel koruma altındadır.

Siyasi Düşünce	Irk/Etnik Köken	Retina	Cinsel Hayat
Felsefi İnanç	Sağlık	Parmak İzi	Biyometrik Veri
Din	Ceza Mahkûmiyeti	Vakıf/Sendika	Kan Grubu
Mezhep	Güvenlik Tedbirleri	Dernek	Kılık, kıyafet

Şekil 4.3 Hassas (Özel Nitelikli) Kişisel Veriler

Hassas Olmayan (Genel Nitelikli) Kişisel Veriler

Kişinin tanınmasını, bilinirliğini sağlayan fakat öğrenilmeleri halinde özellikleri gereği tek başına veri sahibinin temel hak ve özgürlüklerini ve özel yaşamını tehdit etmeyen, mağduriyetine ve ayrımcılığa uğramasına sebep olmayacak veriler hassas nitelikte olmayan verilerdir.

Ad/Soyad	Fotoğraf	Taşıt Plakası	Kredi Kartı
DoğumYeri/Tarihi	E-mail Adresi	Maaşı, Ünvanı	Evlilik Durumu
Yaş, Cinsiyet	Ses Kayıtları	Askerlik Bilgisi	IP Adresi
Telefon Numarası	Pasaport Numarası	Anne Kızlık Soyadı	Login/Kullanıcı Adı

Şekil 4.4 Genel Nitelikli Kişisel Veriler

4.3.3. **Kişisel Verilerin Korunması**

Bilgisayarlar, mobil iletişim araçları, akıllı cihazlar vb. teknolojilerin sağladığı hız ve kolaylıkla çevrimiçi web siteleri, özellikle de Google, Facebook, Instagram, Linkedin vb. sosyal medya platformlarında kullanıcılar, yazılı materyaller, ses kayıtları, görsel dosyalar, videolar gibi kendilerine ait kişisel verilerini paylaşmaktadır. İnternet ağ yapısını kontrol eden şirketler, sosyal ağ etkileşimleri, tanıtım, reklam ve pazarlama stratejileri uygulamalarıyla paylaşılan bu verileri kendi veri işleme sistemleri içerisine aktarırken; devlet ve kurumlar ise kamu yönetimi alanındaki eğitim, sağlık, finans kayıtlarının tutulduğu e-dönüşüm sistemleri ve gelişmiş hareket sensörleriyle donatılmış görüntü/izleme teknolojilerini kullanarak, milyonlarca kişiye ait verileri toplamaktadırlar (Derinözlü, 2007).

Bağımsız ortamlarda bulunan kayıt altına alınıp, derlenen devasa boyutlardaki bu dağınık büyük veri yığınları, kimlik, eğitim, fiziksel özellik, beğeni, cinsel tercih, siyasi görüş ve düşünce, alışveriş alışkanlıkları, finansal durum gibi kişilere ait detayların kolaylıkla incelenmesine, ilişkisel olarak bir araya getirilerek, birbirleriyle bağlantı kurulmasına olanak sağlamaktadır (Kaya B. M., 2017). Özel hayatın gizliliği ve temel hak ve özgürlükler kapsamında kişiye ait olan ve kişisel veri olarak nitelendirilen bu verilerin mahremiyetinin korunması günümüzde önemli bir yapısal sorun olarak karşımıza çıkmaktadır.

İnternet ortamının dinamik yapısı içerisinde gelişmiş teknolojilerin kullanılması yolu ile toplanabilmesi, sınıflandırılabilmesi, saklanabilmesi ve istenen biçimde şekillendirilebilmesi imkânı, kişisel verilerin hukuki normlara aykırı biçimde kullanılması riskini arttırmıştır. (Kaya C. , 2005)

Ekonomik ve sosyal açıdan yüksek değeri olan farklı değişkenlere sahip kişisel verilere yönelik güvenlik, gizlilik ve mahremiyetin en çok tehdit altında bırakıldığı ilk on durum Kanada Veri Gizliliği Komitesi tarafından şu şekilde sıralanmıştır. (Canada, 2018)

1. Mahremiyet ve gizlilik, uluslararası kabul görmüş bir insan hakkı ve modern demokrasinin temelini oluşturan temel bir özgürlüktür. Kişisel olarak “korkacak bir şeyin yoksa, saklanacak hiçbir şeyin yok” düşüncesi veri mahremiyeti ve gizliliği karşısındaki en önemli tehditdir.

2. Bilginin, kişiden kişiye, yetki alanından yargıya, kamu sektöründen özel sektöre özgürce dolaştığı ve veri koruma yasalarının eşit olmadığı küresel dünya düzeni.

3. Aşırı miktarda kişisel bilgi toplanması ve korunamaması nedeniyle körüklenen

kimlik hırsızlığı.

4. Gelişmiş teknolojileri kullanarak hackleme, dolandırıcılık, sahtekarlık gibi yöntemlerle veri iletişim ağlarına sızan, sistemleri ele geçiren dijital dönüşümün endüstriyel veri hırsızları ve bilgisayar korsanları.

5. Hem kamusal alanda hem de özel sektörde yaşanan veri ihlalleri

6. Kullanıcıların, gizlilik politikalarını gözden geçirmeden, gizlilik ayarlarını değiştirmeden veya bu bilgilerin başkaları tarafından nasıl kullanılabileceğini düşünmeden, kendileriyle, aileleriyle ve arkadaşlarıyla ilgili her türlü kişisel bilgiyi sosyal paylaşım sitelerinde paylaşması.

7. Kişisel verilerin korunması veya kullanılmasında yeterli koruma tedbirlerine ve uygun araçlara sahip olmayan ancak gittikçe daha çok sayıda kişiye ait verileri toplayan şirketler ve ticari kuruluşlar

8. Kamu güvenliği ve ulusal güvenlik kapsamında birçok kişisel veriyi elde eden hükümetler

9. Kamera ve izleme teknolojileri, internet aramaları, pos cihazları ile elde edilen veri kayıtlarının kişilerin izni ve bilgisi olmadan toplanması, analiz edilmesi, satılması.

10. Çevrimiçi oyun platformları, elektronik alışveriş siteleri gibi web ortamlarında paylaşılan bilgiler.

4.3.4. **Kişisel Verilerin Korunması Uluslararası Düzenlemeler**

20. Yüzyılın ikinci yarısında bilgisayarların ve veri iletişim ağlarının yaygınlaşması ve tüm dünyada toplumsal yaşamın her alanında kullanılmaya başlaması, gelişmiş veri işleme teknolojileri sayesinde de kişisel verilerin üretilmesi, toplanması ve işlenmesinin kolaylaşması bilginin korunması temeline dayanan güvenlik risklerini de beraberinde getirmiştir.

1980'li yıllardan itibaren kişisel verilerin korunmasının hukuksal açıdan bir hak olarak kabul edilmesiyle birlikte uluslararası anlamda birçok düzenleme ve çalışmanın yapılmasına neden olmuştur (Oğuz, 2013). Bu çerçevede, bireylerin devlet ve özel sektör yapıları ve diğer kişiler karşısında özel yaşamlarındaki mahremiyetlerinin sağlanması ve kişisel verilerinin korunmasına ilişkin yeni bir hukuksal alan ortaya çıkmıştır.

Kişinin özel yaşamının korunması ve mahremiyet hakkı uluslararası bir sözleşmede ilk kez 1948 yılında İnsan Hakları Evrensel Beyannamesinde aşağıda belirtilen ifadeyle düzenlenmiştir. (TBMM, 1949)

"Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır"

"İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme" adıyla 1950 yılında Avrupa Konseyi tarafından İnsan Hakları Evrensel Beyannamesi paralelinde hazırlanan ve 1953 yılında yürürlüğe giren Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesi

1. Herkes, özel yaşamına ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamı tarafından, ulusal güvenliğin, kamu emniyetinin ya da ülkenin ekonomik refahının yararı, suçun ya da düzensizliğin önlenmesi, sağlığın ya da ahlakın korunması için, yahut başkalarının haklarının ve özgürlüklerinin korunması için, hukuka uygun olarak yapılan ve bir demokratik toplumda gerekli bulunanlar hariç, hiçbir müdahale olmayacaktır;

hükümleriyle de kişilerin özel yaşamı ve mahremiyet hakkı hukuksal açıdan güvence altına alınmıştır. (Keser, 2014)

Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD)

Kişisel verilerin korunması alanında yapılan ilk kapsamlı çalışma Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından 23 Eylül 1980 tarihinde yayımlanan bilginin serbest dolaşımının engellenmesi, gizlilik ve mahremiyetin muhafaza edilmesi amacıyla sekiz farklı ilkeden oluşan "Kişisel Verilerin Sınır Ötesi Trafiği ve Verilerin Korunmasına İlişkin Kılavuz İlkeler''idir. Tavsiye niteliğinde olan bu ilkelerin üye ülkelere kişisel verilerin korunmasına yönelik alacakları tedbir ve gerçekleştirecekleri yasal düzenlemelerde rehberlik etmesi öngörülmüştür.

Tablo 4.4 Sınır Ötesi Veri Akışlarına İlişkin Yönlendirici İlkeler (OECD, 2015)

• **Veri Toplamanın Sınırlandırılması** İşlemin tamamlanması için gerekli veriden fazlasının işlenmemesi, verilerin yasalara ve hukuki amaçlara uygun biçimde, kişilerin izni/bilgisi dâhilinde toplanması;
• **Veri Kalitesi** İşlenen verinin doğru, eksiksiz ve güncel olması;
• **Amacın Belirli Olması** Verinin işlenmesi ile ilgili belirtilen amaca uygun olarak değiştirilmeden işlenmesi
• **Veri Kullanımın Sınırlandırılması** Verinin, işlenme amacı dışında kullanılmaması, kişinin rızası ve hukuki otoriteye dayanmadan açıklanmaması.
• **Veri Toplamanın Sınırlandırılması** İşlemin tamamlanması için gerekli veriden fazlasının işlenmemesi, verilerin yasalara ve hukuki amaçlara uygun biçimde, kişilerin izni/bilgisi dâhilinde toplanması;
• **Koruyucu Tedbirler** Verinin, izinsiz erişim, kullanım ve değişikliklere karşı güvenliğinin sağlanması.
• **Açıklık** Verinin korunmasına ilişkin, politika uygulamalarında açık olunması; veri işleme yöntem ve araçlarının gizli olmaması.
• **Bireysel Katılım** Kişinin, kendisine ait işlenen ve kayıt altında tutulan verilere ulaşma, gerekli durumlarda bir kopyasını alma, silinmesi, düzeltilmesi ve tamamlanmasını isteme
• **HesapVerebilirlik** Kişisel verileri kontrol altında tutan kişilerin yukarıdaki ilkelerle uyumlu olmasını sağlayacak yasal mevzuat ve yaptırımların olması

Avrupa Konseyi

108 Sayılı Sözleşme

Avrupa Konseyi, Avrupa İnsan Hakları Sözleşmesinin 8. maddesine dayanarak, bilgi teknolojileri alanında yaşanan gelişmeler sonucunda, hukuki normlar çerçevesinde kişisel verilerin korunması ile ilgili çeşitli metinler kabul etmiştir. Avrupa Konseyi tarafından 28 Ocak 1981 yılında çıkarılan "108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Hakkındaki Avrupa Sözleşmesi" uluslararası kapsamda bağlayıcılığı olan ilk resmi düzenlemedir (Sevimli, 2006). Avrupa Konseyine üye devletleri bağlayıcı nitelikte olan bu sözleşme Türkiye tarafından 1985 yılında imzalanmıştır.

Zaman içerisinde yapılan bazı değişiklikler ve ek protokollerle son şeklini alan 108 sayılı Sözleşme ile üye ülke sınırları içerisinde yaşayan herkesin, özel hayatın gizliliği ve temel hak ve özgürlüklerin güvence altına alınması kapsamında kişisel verilerinin işlenmesi ile ilgili yasal norm oluşturulması amaçlanmıştır. Sözleşmede doğru, güncel nitelikteki kişisel verilerin adil biçimde, yasal yollardan izin alınarak elde edilmesi, belli ve meşru amaçlar için aşırıya kaçmadan kaydedilmesi, işlenmesi ve belirli bir zaman sonra yok edilmesi gerektiği gibi hususlara yer verilmiştir (Atak S. , 2010). Sınır ötesi veri taşıma çerçevesinde Avrupa Konseyine üye devletlerdeki uyrukları ya da ikametgâhları farketmeksizin gerçek kişilerin tamamını kapsayıcı bir anlayış sergilenerek konsey dışındaki ülkelerin de sözleşmeye taraf olmalarına imkân sağlanmıştır (Greenleaf, 2008).

181 Sayılı Ek Protokol

Avrupa Konseyi üye ülkelerde 108 sayılı sözleşmenin yürürlüğe girmesinin ardından

yeni teknolojilerle verilerin işlenmesi ve sınır ötesi transferi konusunda yaşanan gelişmeler, kişisel verilerin korunmasıyla ilgili uygulamalardan sorumlu bağımsız ve özerk bir denetleyici otoritenin (kurumun) ve sınır ötesi veri transfer standartlarının belirlenmesi ihtiyacını doğurmuştur. Bu kapsamda 108 sayılı Sözleşmeye eklenen hükümlerle Kişisel Verilerin Otomatik Yöntemlerle İşlenmesi, Denetleyici Otoriteler ve Sınır Ötesi Veri Akışları Hakkında Bireylerin Korunması Sözleşmesine Ek Protokol (181 sayılı Ek Protokol) 08.11.2001 tarihinde imzaya açılmış ve 01.07.2004 tarihinde yürürlüğe girmiştir.

181 sayılı Ek Protokolle birlikte kişisel verilerin korunması ve sınır ötesi transferi ile ilgili ulusal denetim ve kontrol mekanizmalarının oluşturulması zorunlu kılınarak, kişisel veri güvenliği konusunda yeterli korumayı sağlayamayan ülkelere veri trasnferi yapılamayacağı hukuki olarak karara bağlanmıştır. (Atak S. , 2010)

Birleşmiş Milletler

Birleşmiş Milletler'e üye ülkelerce 14 Aralık 1990 tarihinde "Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler" adını taşıyan bir belge kabul edilmiştir. Birleşmiş Milletlere üye ülkelerin kişisel verilerin korunması alanında yasal düzenleme yapmalarına teşvik edilmesi amacı taşıyan tavsiye niteliğindeki bu belgede, doğru verinin güvenli bir şekilde toplanması, amacın belirliliği, ayrımcılık yapmama, gereksiz verinin talep edilmemesi, verilerin sınır ötesi transferi ve yasal sorumluluk gibi hem OECD tarafından benimsenen rehber ilkeler hem de 108 sayılı sözleşmede kişisel verilerin korunmasına ilişkin hususlar ayrıntılandırılmıştır (La Rue, 2013).

Avrupa Birliği

II. dünya savaşı sırasında ve sonrasında Avrupa'da otoriter yönetimler kaynaklı, kişilerin özel hayatlarının gizliliği ve temel hak ve özgürlükleri ile ilgili yaşanan olumsuz tecrübelerin ardından, demokrasi anlayışının gelişmesiyle birlikte 1970'li yıllardan itibaren başta Fransa, Almanya ve İsviçre olmak üzere kişisel verilerin korunması alanında hukuksal düzenlemeler konusunda çalışmalar yapılmaya başlanmıştır. Kişisel verilerin korunması alanında Avrupa'da ilk veri koruma yasası 1970 yılında Almanya Hesse eyaletinde yürürlüğe koyulmuştur. Ulusal anlamda veri gizliliği konusunda kanun yapan ilk ülke ise 1973 yılında İsveç olmuştur. Özel hayatın gizliliği ve veri koruma ilişkisi temelinde ‘‘Law Concerning Data Processing, Files, and Liberty’’ adı verilen bir kanun da 1978 yılında Fransa'da çıkartılmıştır. (Kutlu, 2017)

Veri Koruma Direktifi (1995/46/EC)

24 Ekim 1995 tarihinde Avrupa Birliği'ne üye devletlerde kişisel verilerin farklı şekilde işlenmesinin ekonomi, rekabet ve hukuksal açısından olumsuz sonuçlar doğurabileceği gerekçesiyle (The European Parliament and The Council of The European Union, 1995) imzalanan, Avrupa Parlamentosu ve Konseyi tarafından da kabul edilen Veri Koruma Direktifi (1995/46/EC) kişisel verilerin korunmasının temel bir insan hakkı olduğunun net biçimde ifade edildiği Avrupa Birliği'ne ait ilk yasal düzenleme olmuştur.

Kişisel mahremiyet başta olmak üzere, bireylerin temel hak ve özgürlüklerinin korunması ve özel yaşamın gizliliğinin amaçlandığı Direktifte belirtilen esaslar, Kişisel Verilerin Otomatik İşlenmesine İlişkin Bireylerin Korunması Hakkındaki 28 Ocak 1981 tarihli 108 sayılı Avrupa Konseyi Sözleşmesinde belirtilen ilkeleri güçlendirici ve

genişletici niteliktedir. Direktifte kişi ve kişisel veri kavramlarının tanımları geniş bir biçimde yapılmış, veri kaynağının bilinmesi, hatalı, eksik verilerin düzeltilmesi, hukuki başvuru hakkı, verilerin ekonomik değerleri gereği pazarlanmasının engellenmesi, hassas verilerin durumu, serbest dolaşımı ve korunması konularında yürütülecek faaliyetler belirtilmiş ve koşullara bağlanmıştır. Kişisel veriler üzerinde gerçekleştirilecek toplama, kaydetme, değiştirme, düzenleme, depolama, yayma, silme yoketme gibi verilerin işlenmesine yönelik çalışmalara, özel yaşam faaliyetlerinde, ulusal güvenlik, kamu güvenliği alanlarında, etik ihlaller ya da ceza gerektiren suçların önlenmesinde, üye ülkelerin ekonomik veya mali menfaatiyle ilgili durumlarda Direktif'in uygulanması sınırlandırılmıştır (Bilgin, 2017).

Avrupa Birliği üyesi ülkeler Direktif'te belirtilen koşullara yasal olarak uymak zorunda olduğu gibi, Avrupa Birliği üyesi olmayan ülkelere de Avrupa Birliği ülkeleriyle karşılıklı veri transferi yapabilmeleri için Direktif ilkelerine uygun eşdeğer veri koruma sağlamaları (güvenli ülke) zorunluluğu getirilmiştir. (Mantelero, 2012)

Elektronik Veri Koruma Direktifi (2002/58/EC)

Teknolojik gelişmelerin hız kazanması, internet ve veri ağlarının genişlemesi ile verilerin toplanmasının ve paylaşımının kolaylaşması sonucunda Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu tarafından kişisel verilerin korunması alanında ortaya çıkan ihtiyaçları karşılamak üzere Avrupa Birliği 95/46/EC sayılı Direktifinin temel alındığı farklı hukuki düzenlemeler ve çalışmalar da yapılmıştır.

İnternet ve modern iletişim araçlarının (mobil telefon, SMS, e-posta, sohbet odaları) kullanımı sonucu ortaya çıkan verilerin (trafik, konum bilgisi vb.) işlenmesi kapsamında 2002 yılında yürürlüğe giren 2002/58/EC sayılı Elektronik Haberleşme Sektöründe

Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin Direktif, 1995/46/EC sayılı Veri Koruma Direktifini tamamlayıcı nitelikte hazırlanmıştır. Elektronik Veri Koruma Direktifi ile halka açık iletişim ağları üzerindeki elektronik haberleşme hizmetlerinden elde edilen kişisel verilerin 3. kişilere aktarımı konusunda sadece gerçek kişileri değil tüzel kişileri de kapsayan ve gizlilik hakkının eşit ölçüde korunduğu sistemli bir yapının kurulması amaçlanmıştır. (Kılınç, 2012)

Veri Saklama Direktifi (2006/24/EC)

Avrupa Birliği tarafından, organize suçlar ve terör saldırıları gibi ciddi tehditlerin önlenmesi, adli vakaların incelenmesi, suçlu takibi vb. cezai soruşturmalarda iletişim teknolojisi araçlarının kullanımı esnasında ortaya çıkan verilerin (internet IP adresleri, telefon numaraları, kimlik bilgisi, iletişim veya bağlantının zamansal ve konumsal bilgileri) elektronik haberleşme altyapı ve hizmet sağlayıcılar tarafından kayıtlarının tutulması ve yetkili mercilerle (üye ülkelerin emniyet güçleri) işbirliği yapılarak paylaşılması amacıyla 15 Mart 2006'da 2006/24/EC sayılı Halka Açık İletişim Hizmetleri veya İletişim Ağlarına İlişkin Olarak Üretilen veya İşlenen Verilerin Saklanmasına İlişkin Direktif yürürlüğe girmiştir. (ECJ, (C-293/12 ve C-594/12 Birleşik Davası) EU:C:2013:845EU:C:2014:238, 2014)

Avrupa Adalet Divanı (European Court of Justice) 8 Nisan 2014 tarihinde Direktif'in uygulanması süreçlerinde kurumların yetki alanlarını aşarak, özel hayatın gizliliği sınırlarını keyfi ve orantısız biçimde ihlal ettiği ve kişisel verilerin korunması alanındaki temel hak ve özgürlüklerin hukuksal açıdan zarar gördüğü gerekçesiyle 2006/24/EC sayılı Veri Saklama Direktifi'nin yürürlülüğünü iptal etmiştir. (ECJ, (C-293/12 ve C-594/12 Birleşik Davası) EU:C:2013:845EU:C:2014:238, 2014)

Avrupa Birliği Genel Veri Koruma Tüzüğü (2016/95/46)

2011 yılında, Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu tarafından AB üyesi ülkelerin kendi iç hukuk alanlarında kişisel verilerin korunması kapsamında işlerliği bulunan farklı yasal uygulamaların modernleştirilip birbirleri ile uyumlaştırılarak, bütün Avrupa Birliği'ni kapsayacak ortak bir veri koruma standartının oluşturulması konusunda bir reform kararı alınmıştır. (Akıncı N, 2017)

Bilgi ve iletişim teknojilerinin ve gelişmiş veri ağlarının hâkim olduğu dijital dünyada Avrupa Birliği'nin sosyal ve ekonomik sistemi içerisindeki kurumlar, şirketler ve bireyler arasında güvenin sağlandığı, üye ülkelerin veri koruması kapsamındaki yasal mevzuatlarının üst seviyede uyumla birleştirildiği tek bir veri koruma standartının kullanılması amacıyla hazırlanan Avrupa Birliği Genel Veri Koruma Tüzüğü (2016/95/46) 14 Nisan 2016 tarihinde Avrupa Parlamentosunda kabul edildikten sonra 24 Mayıs 2016 tarihinde yürürlüğe girmiştir. (Akıncı N, 2017)

Avrupa Birliği ülke vatandaşlarının google, apple, facebook vd., küresel veri aktörlerine karşı kişisel verilerinin korunması ve mahremiyetlerinin güvence altına alınması, Tek Pazar Stratejisi temeline dayanan dijital AB ekonomisine uluslararası rekabet avantajı sağlaması gibi, ekonomik gelişme, güvenlik ve bireysel hakların korunması alanlarında çok önemli sonuçları olacağı öngörülen Genel Veri Koruma Tüzüğü (2016/95/46) 25 Mayıs 2018 tarihinden itibaren Avrupa Birliği üye ülkelerin tamamında doğrudan uygulanmaya başlanmıştır. (Ayözger, 2016)

Genel Veri Koruma Tüzüğü (2016/95/46) ile verilerin işlenmesi, korunması ve mahremiyet hakkı alanında yapılan düzenlemeler şunlardır (Akıncı N., 2017);

- Veri koruma mevzuatları ve kullanıcı hakları açısından üst seviye uyumlaştırma
- Veri İşleyen kurum, şirket ve bireylerin veri işleme ile ilgili uygulamalardan sorumlu tutulması
- Veri korunması kapsamında verilerin hukuki güvence altına alınması
- Veri işlenmesi sonucu yaşanacak mahremiyet ve gizlilik ihlallerine karşı tazminat
- Kişisel verilerin sınır-ötesi aktarımında korunması ve denetiminin sağlanması
- Kişilere kendisine ait verilerin silinmesini isteyebilme hakkı (Unutulma Hakkı)
- Veri kontrolörlerine veri gizliliği konusunda kullanıcı haklarına ilişkin bilgilendirme yükümlülüğü getirmesi
- Veri ihlalleri karşısında denetim mekanizmalarıyla daha ağır yaptırımların uygulanması
- Kişisel verilerin işlenmesine ilişkin veri sahiplerinden özgür, bilinçli ve açık rıza alınması zorunluluğu
- Veri sahibinin verilerini istediği zaman, istediği veri kontrolörüne taşıyabilmesi
- Hassas verilerin işlenmesi ile ilgili faaliyetlerde Veri Koruma Görevlisi görevlendirilmesi.
- Hassas verilerin otomatik veri işleme sistemlerinde işlenmesi sırasında oluşacak riskli durumlara karşı Veri Koruma Etki Değerlendirmesi yapılması.
- Başlangıçtan ve tasarımdan itibaren veri koruması yaklaşımı
- Yüksek riskli veri ihlali durumlarının veri koruma otoritesine ve veri sahibine bildirilmesi

4.3.5. **Kişisel Verilerin Korunması Ulusal Düzenlemeler**

Kaynağını özel yaşamın gizliliğinden alan kişisel verilerin korunması kavramı alanında hukukumuzdaki yasal düzenleme çalışmaları Türkiye'nin gündemine Avrupa Konseyi

tarafından hazırlanan 28.01.1981 tarihinde imzalanan 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme ve 08.11.2001 tarihinde imzalanan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol (181 Sayılı Ek Protokol) ile girmiştir. Ülkemizde 1985 yılında yürürlüğe giren 108 sayılı sözleşme ile kişisel verilerin korunması kavramı anayasada karşılığını bulan özel hayatın gizliliği ile doğrudan ilişkilendirilmiş ve hukuksal düzenlemeler bu yönde geliştirilmiş ve sürdürülmüştür (BTK, 2016). Ancak yürürlüğe girmesine karşın hem 108 sayılı Sözleşme'nin (Resmi Gazete, 18.02.2016) hem de 181 Sayılı Ek Protokol'ün (Resmi Gazete, 05.05.2016) iç hukuka uyarlanması ve kanunlaşması süreci çok uzun zaman almıştır.

Türk Hukuk Mevzuatı içerisinde kişisel verilerin korunması alanında hem Anayasa'da hem de farklı Kanunlarda birçok düzenleme yapılmıştır.

Anayasa'da (1982) bulunan hükümler;

- Özel hayatın gizliliği (m. 20),
- Haberleşmenin gizliliği (m. 22),
- Düşünce ve kanaatleri açıklamaya zorlanamama (m. 25),

Türk Ceza Kanunu'nda (2004) yapılan düzenlemeler;

- Kişisel verilerin kaydedilmesi (m. 135),
- Verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi (m. 136),
- Verilerin yokedilmemesi (m. 138)

Ancak bu düzenlemelerin önleyici nitelikte olmamaları sebebiyle kişisel verilerin korunması kavramının özel bir kanun kapsamında değerledirilmesi zorunlu hale gelmiştir. (Henkoğlu, 2017)

Anayasa'da Kişisel Verilerin Korunması

Hukuksal uygulama alanında temel hak ve özgürlükler, mahremiyet hakkı ve kişisel verilerin korunması kavramları, nitelik olarak özel hayatının gizliliği ve korunması hakkı çerçevesinde değerlendirilmektedir. Bu kapsamda hazırlanan bütün Kanun, tüzük, yönetmelik ve düzenlemeler normlar hiyerarşisi gereği Anayasal hükümlere uygun ve uyumlu olmak durumundadır.

Anayasa Mahkemesi 6.1.1999 tarihli, 199/1 sayılı kararıyla kişisel verilerin korunmasını Anayasanın 20'nci maddesinde düzenlenen özel hayatın gizliliği kapsamında değerlendirmiştir. Yine 03.10.2001 tarih ve 4709/7 sayılı kararıyla Anayasa'da düzenlenen haberleşme hürriyeti, aile ve özel hayatın gizliliğinin kişisel veriler ile ilişkili olduğu belirtilmiş ve güvence altına alınmıştır. Bu kararlar doğrultusunda, kişisel verilerin işlenmesine ilişkin düzenlemelerin, Anayasada yer alan özel hayatın gizliliğinin sınırlandırılmasıyla ilgili esaslarla uygunluk göstermesi gerekmektedir. (Civelek Y., 2011)

Kişisel verilerin korunmasının hukuki açıdan en önemli ayağını bilişim teknolojileri özelinde internet kavramı oluşturmaktadır. 2000'li yıllarla birlikte ülkemizde bilişim teknolojileri ve internetin yaygınlaşması sonucu kişisel veriler ile ilgili en kapsamlı hukuki düzenleme 23.05.2007 tarihinde 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi kapsamındaki Kanun ile yapılmıştır. (BTK, 2016)

5651 sayılı Kanun ile ilk defa;

- İnternet ile ilişkili kavramların (içerik sağlayıcı, yer ve erişim sağlayıcı, toplu kullanım sağlayıcı) tanımı yapılmış ve bu kavramlara bağlı hak ve sorumluluklar belirlenmiştir.
- Yasa ile belirtilen suçlar kapsamında erişimin engellenmesi usul ve esasları düzenlenmiştir.
- İnternet ortamında yayınlanan içerik nedeniyle hak ihlaline uğrayan ya da maddi/manevi zarar gören kişilere ilişkin; içeriğin yayından çıkarılması ve cevap hakkı sağlanmasıyla ilgili usul ve esaslara yer verilmiştir.

12.09.2010 tarihinde Anayasa'nın 20. maddesinin 3. fıkrasında değişikliğe gidilmiş, yürürlüğe giren 5982 sayılı Kanun ile kişisel veri kavramı aşağıda belirtildiği haliyle Anayasa'da yerini almıştır; (Dğş., 12.09.2010)

"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Anayasa'ya eklenen bu maddeyle, bilgisi dışında kişisel verilerinin işlenmesi sonucunda meydana gelebilecek zararlara karşı veri sahiplerinin temel haklarının korunarak güvence altına alınması hedeflenmiştir.

6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)

Kişisel verilerin korunmasına ilişkin kanun hazırlanması ile ilgili çalışmalar Türkiye tarafından 1982 yılında imzalanan 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'nin 1985 yılında yürürlüğe girmesiyle başlamıştır.

Kişisel verilerin yetkisiz kişiler tarafından elde edilmesi, kullanılması ve ifşa edilmesinin gerek Türkiye'nin taraf olduğu sözleşmelere gerekse de Anayasa'da yer alan temel haklara aykırılık teşkil etmesi sonucu ortaya çıkan uyumsuzluk ve ihlaller Anayasa ve bazı sektörel bazlı yasal düzenlemelerle giderilmeye çalışılmıştır. Ancak zaman içerisinde uygulama alanında kişisel verileri işleme tabi tutulan kişiler ile bu verileri işleme tabi tutan kamu kurum ve kuruluşları ile gerçek ve özel hukuk tüzel kişileri arasında açık, net çizgilerle belirlenmiş tam uyum ve korumayı sağlayacak bir kanunun hazırlanması zorunluluk haline gelmiştir. (Anı, 2018)

2003 yılında kanun çalışmalarının yapılması oluşturulan komisyon tarafından 2005 yılında hazırlanan Kanun Tasarısı 2008'de ve 2012'de Adalet Bakanlığı tarafından tekrar düzenlenmiş, 26.12.2014 tarihinde son şeklini alarak TBMM'ye sunulmuş, 05.01.2015 tarihinde de ilgili komisyonda görüşülerek ve onaylanmıştır. 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'nin 18.02.2016 tarihinde onaylanarak iç hukuka dahil edilmesi ile AB Veri Koruma Direktifi (1995/46/EC) temel alınarak hazırlanan Kişisel Verilerin Korunması Kanun tasarısı 24.03.2016 tarihinde yasalaşmıştır. Yasalaşan 6698 sayılı Kişisel Verilerin Korunması Kanunu, 07.04.2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. (KVKK, 2016)

Kişisel Verilerin Korunması Kanunu Amaç ve Kapsamı

KVKK birinci maddesinde Kanunun amacı belirtilmiştir. (6698 KVKK m.1)

"Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."

Maddenin gerekçesinde de belirtildiği üzere Kanunun amacı, kişisel verilerin işlenmesi kapsamında yürütülecek uygulamaların denetim altına alınması ve Anayasa'da (m. 20) belirtilen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin korunmasıdır. KVKK ile kişinin mahremiyet ile bilgi güvenliği hakkının korunması, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esaslar düzenlenmiştir.

6698 sayılı Kanun'un "Kapsam" başlıklı 2. Maddesinde (6698 KVKK m. 2) kanunun kapsamı şu şekilde ifade edilmiştir:

"Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."

KVKK kapsamı dâhilindeki otomatik olmasa dahi bir veri kayıt sisteminin parçası olma durumu, fiziki olarak bir ortamda tutulan, saklanan verilere ulaşılabilirliğin bir takım kriter ve süreçlerle kolaylaştırılmasıdır. Örneğin, iş başvurusunda bulunan bir kişiye ait kişisel verilerinin yer aldığı iş başvuru formunun veya özgeçmiş örneğinin başvurulan şirket tarafından herhangi bir bilgisayar ortamına veya daha sonra nerede saklandığını bulmak amacıyla fiziken bir dosyalama sistemine kaydedilmeksizin şirket merkezinde diğer evraklarla birlikte herhangi bir yerde saklanması halinde bu saklama işlemi Kanun kapsamına girmeyecek, ancak iş başvuru formunun veya özgeçmiş örneğinin

bilgisayarlarda, sunucularda veya bir arşivleme sistemi ile fiziki olarak şirket içerisinde saklanması halinde Kanun'a tabi olunacaktır. (KVKK, 2017)

4.3.6. **Kişisel Verilerin İşlenmesi**

Veri Koruma Direktifi 1995/46/EC m. 2/b'ye göre otomatik ya da otomatik olmayan araçlar ile veriler üzerinde yapılan silme, tahrip etme, engelleme, birleştirme, sıralama, sağlama, dağıtma, iletme, açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon, değiştirme, kurtarma, danışma gibi her türlü faaliyet ya da faaliyet dizisi veri işleme kavramının tanımı içerisinde bulunmaktadır. Tanımda açıkça belirtildiği gibi verilerin işlenmesi sadece bilgisayar altyapılı otomasyon sistemleri aracılığıyla yapılan uygulamaları değil, otomatik sistemler kullanılmadan verilerin elden işlenmesi durumlarını da kapsamaktadır (Ayözger, 2016).

KVKK içerisinde verilerin işlenmesi, Veri Koruma Direktifi'nde belirtilen tanımsal çerçeveye benzer nitelikte "Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem" şeklinde ifade edilmiştir. (KVKK m. 3/e)

KVKK Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler ve Şartlar

KVKK'da kişisel verilerin toplanmasından, yokedilmesine kadar işlenmesi sürecine ilişkin usul ve esaslar 108 sayılı Sözleşme ve 95/46/EC sayılı AB Veri Koruma Direktifinde atıf yapılan ilkelerle aynı düzlemde oluşturulmuştur.

Tablo 4.5 Kişisel Verilerin İşlenmesi Genel İlkeler; (KVVK İlkeler, 2017)

M. 4/2 (a) Hukuka ve dürüstlük kurallarına uygun olma; Veri işleyenin kişisel verilerin işlenmesi sürecinin başından sonuna kadar, kanunlarda ve diğer hukuki düzenlemelerde belirtilen ilke ve yükümlülüklere uygun hareket etmesi gerekir. M. 4/2 (b) Doğru ve gerektiğinde güncel olma; Verilerin işlenmesi sürecinde veri sahibinin kişisel verilerinin doğruluğunu kontrol etme ve verilerinde meydana gelen değişikliklerin güncellenmesini talep etme hakkı vardır. M. 4/2 (c) Belirli, açık ve meşru amaçlar için işlenme; Kişisel verileri işlenen herkes, veri işleyen kurum ve kuruluşlardan verilerinin hukuksal çerçevede uygun amaçlarla toplanıp toplanmadığını ve bu amaca uygun işlenip işlenmediğini öğrenmek hakkına sahiptir. M. 4/2 (ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma; Kişisel verilerin ilk işlenmesi için gereken amaç sonradan değiştirilemez. İşlenen veriler başka amaçlar için kullanılmama konusunda güvence altında, rızası alınan amaç ile uyumlu, tamamlayıcı nitelikte olması gerekir. M. 4/2 (d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme; Kişisel veriler amaçla sınırlılık ilkesi gereği işlendikleri amaç doğrultusunda belirlenen süreye uygun olarak saklanabilir. Bu konuda idari ve teknik her türlü tedbirleri almak veri sorumlusuna aittir.

Tablo 4.6 Kişisel Verilerin İşlenme Şartları; (KVKK İşlenme Şartları, 2017)

M. 5/1 İlgili kişinin açık rızası olma;

Verisi işlenecek kişinin, belirli bir konuda veri işleme faaliyeti başalamadan önce, veri işleyen tarafından bilgilendirilerek hiç kimsenin etkisi altında kalmadan, kendi iradesi ile özgürce verilerinin işlenmesi konusunda rızasının alınması gerekir. Açık rıza üç temel şartın sağlanmasıyla oluşur.

- Belirli bir konuya ilişkin olma
- Bilgilendirmeye dayanma
- Özgür iradeyle açıklanmış olma

Aşağıdaki şartlardan herhangi birisinin oluşması durumunda açık rıza şartı aranmaz.

M. 5/2 (a) Kanunlarda açıkça öngörülmesi;

Kanunlarda verilerin işlenebileceği ile ilgili hüküm bulunduğu durumlarda.

Örnek: Adli soruşturma kapsamında parmak izinin alınması.

M. 5/2 (b) Fiili imkânsızlık;

Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

Örnek: Suç soruşturması kapsamında belirlenen faaliyetlerde ya da hürriyeti kısıtlanan bir kişinin kurtarılması amacıyla, teknik ve idari takip yapılması.

M. 5/2 (c) Sözleşmenin kurulması ve ifası için gerekli olması;

Herhangi bir sözleşmenin tamamlanması açısından taraflara ait kişisel verilerin işlenmesinin zorunlu olduğu durumlarda bu amaca uygun biçimde kişisel verilerin işlenmesi mümkündür.

Örnek: Banka sözleşmelerinde kullanılan maaş bordrosu, hesap numarası vb. veriler.

M. 5/2 (ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması;

Veri işlenmesinin veri sorumlusu açısından hukuken zorunlu olduğu hallerde ilgili kişinin kişisel verileri işlenebilecektir.

Örnek: Bir şirketin çalışanların maaşlarını yapabilmek için sigorta numarası, evlilik durumu, çocuk sayısı vb.gerekli olan bilgilerin elde edilmesi.

M. 5/2 (d) Kişisel verilerin ilgili kişi tarafından alenileştirilmiş olması;

Veri sahibi kişinin herhangi bir şekilde kendisi tarafından kamuoyuna açıklanmış verileri bu kapsamdadır.

Örnek: Kurumsal telefon numarasını, mail adresini paylaşmak

M. 5/2 (e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması;

Hukuki bir süreç sırasında ispat hakkı için ve sözleşmelerde belirtilen yasal süreler içerisinde evrak, belge saklanması gereken durumlarda veriler işlenebilir.

Örnek: Kendisine çalışanı tarafından dava açılan bir şirketin bazı verileri ispat hakkı için kullanması.

M. 5/2 (f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması;

Veri sorumlusu açısından veri işlemenin zorunlu olduğu fakat bu zorunluluğun veri sahibinin temel hak ve özgürlüklerini tehdit etmediği durumlarda veriler işlenebilir.

Örnek: Bir şirketin el değiştirmesi sürecinde görev ve rol dağılımının belirlenmesi sırasında çalışanların temel hal ve özgürlükleri gözetilerek verilerinin işlenmesi

V. BİLGİ GÜVENLİĞİ FARKINDALIĞI

Değişen teknolojik kültürle ortaya çıkan siber dijital dünyada, geniş bağlantı iletişim protokolleri ile fiziksel veya sanal ortamlarda yer alan bilginin miktarındaki sınırsız artış potansiyel güvenlik risk ve tehditlerini de beraberinde getirmiştir. (Öztemiz & Yılmaz, 2013)

Akıllı üretim endüstrisinin etkisinde fiziksel ve sanal varlıklarının birbirleri ile bütünleştiği bankacılık, finans, enerji, sağlık, eğitim gibi sektörlerin, kurum, uluslararası örgüt ve devletlerin dijital dönüşümüyle ortaya çıkan bilgi toplumunda bilginin güvenliği önemli gündem maddelerinden birisi haline gelmiştir.

Bilgi ve iletişim teknolojilerinin etkisinde gelişen sosyal ağlar, E-Ticaret, E-Bankacılık, E-imza, E-Devlet gibi yeni kavramlar ile birlikte yüksek derece de öneme sahip olan bilgiler internet ortamına aktarılmaya başlanmıştır. Sayısal teknolojiler aracılığıyla çevrimiçi ortama taşınan, geleneksel sunum tarzını terk edip bilgi teknolojilerinin sunmuş olduğu hız, basitlik, şeffaflık, maliyet gibi unsurlar ile kullanım kolaylığı ve alışkanlığı kazanan bilginin akışında hem kişisel hem de kurumsal bilgilerin güvenilirliği tehlike altına girmiştir. Bu durum da bilginin güvenirliliğinin sağlanmasını zorunlu kılmıştır. (Öğütçü, 2010)

5.1. **Bilgi Güvenliği**

Bilgi güvenliği; dijital veya dijital olmayan ortamlarda bulunan her türlü verinin/bilginin, göndericiler/alıcılar arasında taşınması sırasında, varlık olarak

bütünlüğünün bozulmaması, zarar görmemesi, değişikliklere uğramaması, yetkisiz-izinsiz erişimlerden korunması, istenmeyen kişilerce ele geçirilmesinin engellenmesi doğrultusunda teknolojinin uygun amaç ve biçimde kullanılması sürecidir. (Canbek & Sağıroğlu, 2006)

Bilgi güvenliği, doğru işleme yöntemleriyle bilginin bütünlüğünün sağlanması, herhangi bir değişikliğe uğramadan taşınması ve yalnızca erişim yetkisi verilmiş kullanıcıların ihtiyaç duyduğu zamanda, bilgi kaynaklarına erişimlerini sağlayan araç ve yöntemlerin tamamıdır. (ISO, 2005)

Bilgi güvenliği, bilgilerin izinsiz-yetkisiz erişimlerden, kullanılmasından, ortaya çıkarılmasından, silinmesinden, değiştirilmesinden veya zarar verilmesinden kısaca kişisel veya kurumsal mahremiyetin, gizliliğinin, bütünlüğünün ve ulaşılabilirliğinin korunması işlemidir. (Baykara, Daş, & Karadoğan, 2013)

5.2. **Bilgi Güvenliği Kavramının Gelişimi**

Bilgi ilkel toplumlardan günümüz bilgi toplumuna kadar yüzyıllardır kişiler, kurumlar ve ülkeler için hep önemli bir varlık olarak gelişimini sürdürmüştür. Tarih boyunca insanlar bilgiyi koruyarak güvenliğini sağlayabilmek için farklı yöntemleri kullanmışlardır. Yazının icadıyla niteliksel olarak yazılı bir form halini alan bilgi çalınmaya, zarar verilmeye, değiştirilmeye karşı güvenli bir şekilde korunması gereken bir meta haline gelmiştir. (Baykara, Daş, & Karadoğan, 2013)

Bilgi güvenliğinin bir kavram olarak günümüzdeki şeklini alması II. Dünya Savaşı sırasında iletişim kodu kırma hesaplamaları için geliştirilen ilk ana bilgisayarların ortaya çıkmasıyla başlamıştır. Elektromanyetik bir rotor makine olan ENIGMA Mors

alfabesi şeklinde kodlanan mesajların alıcıya gönderilmesi ve alıcının bu kodları çözmesi temelinde 1930'lu yıllarda Alman ordusu tarafından istihbarat ve gizli yazışmaların şifrelendiği bir sistem olarak kullanılmıştır. Bilgi güvenliğinin sağlanması bu ilk zamanlarda, ağırlıklı olarak sabotaj, fiziksel güvenlik, casusluk ve basit belge sınıflandırmalarına karşı alınan önlemlerden ibarettir.

1951 yılında üretilen UNIVAC adlı bilgisayarın manyetik bir teyp kullanarak verileri depolayabilmesi, gelecek kuşaklara aktarılması istenen bilgileri elektromanyetik saldırı gibi dış etkilere karşı daha duyarlı hale getirmiş, bu tarihten itibaren bilginin korunmasına yönelik yeni güvenlik önlemlerinin alınması konusu bilgi güvenliği ile ilgili önemli bir tarihsel dönüşüm noktası olmuştur. (Henkoğlu, 2017)

1960'lı yılların başında soğuk savaş döneminde daha karmaşık görevleri yerine getirmeye programlı bilgisayarların birbirleriyle uzaktan iletişim kurması için yapılan çalışmaların sonucunda internetin temelleri atılmış, bilgi güvenliği de internetin tarihsel gelişimine paralel bir yol izlemiştir. 1962 yılında Massachusetts Institute of Tecnology'den (MIT) J.C.R. Licklider, küresel olarak bağlanmış bir sistemde isteyen herkesin, herhangi bir anda, herhangi bir yerden veri ve programlara erişebilmesi olarak tanımladığı Galaktik Ağ kavramı ile İnternet bir düşünce olarak ilk defa ortaya çıkmıştır. (Gümüş, 2014)

1960'ların başında ABD Savunma Bakanlığı tarafından desteklenen çalışmalardan, İnternet Protokolü'nü (IP) kullanan ilk fiziksel ağ olan ARPANET, 1969 yılında NCP ağ protokolü ile 50 Kbps'lik bağlantı hızıyla ABD'de dört ayrı üniversitedeki merkezi bilgisayarlar arasında kurulmuştur. Böylelikle farklı ağların daha büyük ağlara bağlanmasını mümkün kılan ARPANET, internet konusundaki gelişmelerin de önünü

açmıştır. ARPANET çalışmaları devam ederken 1970'li yıllarda farklı iletişim protokollerinin kullanıldığı, NPL network, CYCLADES, Merit Network, Tymnet ve Telenet gibi benzer özellikli ağlar geliştirilmiştir. (Wikipedia, 2018)

1972 yılında bilgisayarlar arasında ağ üzerinde dosya aktarımı için kullanılan Dosya Transfer Protokolünün (FTP - File Transfer Protocol) çekirdek teknolojisi geliştirilmiştir. Yine bu yıl içerisinde ilk elektronik posta (e-mail) ARPANET bağlantısı üzerinden gönderilmiştir. Ocak 1973 yılında sağladığı farklı olanaklar ile bugün varolan internet ağının ana halkasını oluşturan, TCP/IP protokolü ARPANET içerisinde NCP'nin yerini almıştır. (Gümüş, 2014)

1970 yılında yayınlanan "RAND Report R-609-1" (Ware, 1979) raporunda bağımsız bir şekilde çalışırken görünürde güvenli oldukları düşünülen ağ sistemleri ve bilgisayarların birbirleriyle entegre edilerek bütünleşik bir duruma geçmesi sonucu ortaya çıkan tehdit ve riskler tüm yönleriyle kavramsal olarak bilgi güvenliği adı altında ilk defa ortaya koyulmuştur.

1980'li yılların başında Computer Science Network (CSNET)'in National Science Foundation (NSF) desteğiyle ARPANET'e erişim genişletilmiş ve TCP/IP standart ağ protokolü olarak kabul edilmiş, çeşitli üniversitelerde bilgisayar merkezleri kurulmuştur. ARPANET'le benzer özellikler gösteren fakat sadece bilgisayar bilimlerine yönelik kullanılması amacıyla geliştirilen (NSFNET - Computer Science Research Network) projesi bir geçit bilgisayarı (Gateway) kullanılarak ARPANET ile birleştirilmiş ve bu merkezlerin birbirlerine bağlandıkları geniş bir ağa dönüştürülmüştür. Birbirinden bağımsız ağların bir araya gelmesi ile birlikte internetin ilk fiziksel uygulaması da ortaya çıkmıştır. (Civelek, 2009)

1983 yılında New York Üniversitesi tarafından geliştirilen BITNET (Because It is Time for Network) ile dünyadaki en büyük Geniş Alan Ağı (WAN) kurulmuştur. Aynı yıl içerisinde Wisconsin Üniversitesi tarafından gelişitirilen ilk alan adı sunucusu (Domain Name Server) ile ağa bağlı bilgisayarlara IP numarasına karşılık gelen akılda kalıcı ".gov, .edu, .mil, .int, .com, .org, .net" olmak üzere yedi adet üst seviye alan adı ismi verilmesi mümkün olmuştur.

Tim Berners-Lee, 1989 yılında İngiltere'de bilgisayar ağ yapıları üzerine yaptığı çalışmaların sonucunda zengileştirilmiş text dökümanlarını (HTML) çalışan bir ağ sistemi ile bütünleştirerek (URL, HTTP) Internetin omurgasını oluşturan www (World Wide Web) kullanıcı arayüzünü geliştirmiştir. Bu gelişme modern internetin doğuşuna işaret etmekteydi. Küresel ağ olarak da adlandırılan bu proje ile dünyanın farklı yerlerinde bulunan kişisel bilgisayarlar ve diğer sistemler birbirleriyle iletişim kurabilecek ve internet adını verdiğimiz oluşumun ortaya çıkış süreci tamamlanacaktı. Tim Berners-Lee tarafından hazırlanan www.info.cern.ch adresi dijital dunyanın ilk web sayfasi olarak tarihteki yerini alırken, ticari internet servis sağlayıcıları ve internet üzerinden multimedya uygulamaları da bu sürecin ardından ilk defa kullanılmaya başlanmıştır. 1995 yılında kurulan Amazon ve e bay internet üzerinden ticaretin ilk adımlarını atarken yine aynı yıl Hotmail ücretsiz olarak e posta hizmeti vermeye başlamıştır. (Wikipedia, İnternet'in Tarihi, 2018)

İlk zamanlarda resmi kurumlar, üniversiteler ve endüstri sektörlerinde kullanılan internetin, 1990'ların ortalarından itibaren gelişmiş iletişim, akıllı bağlantı ve mobil teknolojilerin etkisinde ticarileşmesiyle birlikte iktisadi ve sosyal fayda oluşturması amacıyla kullanımı da yaygınlaşmış, milyonlarca kişinin bağlı olduğu dev bir küresel

ağa dönüşmüştür. İnternetin küresel ölçekte yaşadığı bu erişilebilirlik bilginin çok hızlı biçimde artışını sağlarken, internet teknolojileri, ağ sistemleri ve altyapılara yönelik güvenlik riskleri ve tehditlerinin hem nitelik hem de nicelik olarak farklılaşmasına neden olmuştur (Güngör, 2015). Bilgi sistemlerine ulaşabilmek için fiziksel temas ve erişim gereksiniminin ortadan kakması ile birlikte uzaktan bağlantıya karşı çok katmanlı kullanıcı güvenliği, erişim/şifre güvenliği, ağ güvenliği, yazılım güvenliği, kişisel veri güvenliği gibi konular bilgi güvenliği kavramının içerisinde yerini almıştır.

1999 yılında e posta yoluyla yayılan, Word, Excel ve Outlook belgelerine sızan Melissa virüsü, bilgi güvenliği açısından küresel anlamda karşılaşılan ilk ve en büyük tehlike olarak tarihteki yerini almıştır. Kanada, Hollanda, Yeni Zelanda, Katar, Singapur, İsveç ve Birleşik Krallık'a kadar farklı ülkelerde rapor edilen Melissa, dünya genelinde 1 milyondan fazla bilgisayarı etkileyip 1.1 milyar dolarlık zarara yol açmıştır. (Melissa, 2018) Melissa virüsünün etkilerinden birisi de bilgi teknolojileri ve yazılım şirketlerinin bilgi güvenliğinin sağlanması konusunda yeni ve daha kapsamlı çalışmalar başlatmaları olmuştur.

2000'li yılların hemen başında ortaya çıkan kablosuz ağlar, mobil iletişim teknolojileri ve Nesnelerin İnterneti (Internet of Things - IoT) gibi kavramlar ile bilginin çok daha hızlı ve farklı şekillerde üretilmesi, işlenmesi, saklanması ve paylaşılabilmesinin de önü açılmış oluyordu. Çeşitli protokoller aracılığıyla birbirleri ile ve diğer teknolojik cihazlarla haberleşen, bilgi üreten, bağlı bulundukları ağlar sistemleri üzerinden çevreleriyle bilgi alış verişi yapabilen mobil iletişim cihazları, akıllı makineler ve nesnelerin oluşturduğu siber uzay adı verilen yeni bir dijital ekosistem ortaya çıkmıştır. Fiziksel ve sanal varlıklarının birbirleri ile bütünleştiği bu dijital ekosistemde, hem

internet üzerinden e-posta, anlık mesajlaşma, VoIP, video görüşme, tartışma forumları, bloglar, sosyal ağlar, çevrimiçi alışveriş gibi kaynaklardan üretilen hem de makine ve nesneler tarafından üretilen bilginin korunma ihtiyacının boyutları da tamamen değişmiştir.

5.3. **Bilgi Güvenliğinin Unsurları**

Bilgi güvenliği ile ilgili alanyazındaki tanımlar incelendiğinde genel olarak bilginin korunan niteliği birbirleriyle bağlantılı üç temel unsurdan oluşmaktadır. Bunlar; gizlilik (yetkisiz kişilerin bilgiye erişiminin olmaması), bütünlük (varolan bilginin bozulmaması, değiştirilmemesi) ve erişilebilirliktir (bilginin ulaşılabilir, kullanılabilir olması) (Saltzer & Schroeder, 1975). Başka bir ifade ile temel olarak bilgi güvenliği bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin bütünleşik bir şekilde korunmasını hedeflemektedir.

Elektronik ortamlarda bilginin izinsiz/yetkisiz erişimlerden, kullanılmasından, ortaya çıkarılmasından, silinmesinden, değiştirilmesinden veya zarar verilmesinden korunması bağlamında güvenlik staratejileri oluşturulırken bu üç temel unsur arasında bir denge kurulması gerekmektedir. Dijital teknolojilerin ve gelişmiş veri iletim ağlarının bilgi erişimini kolaylaştırması güvenlik anlamında riskleri de beraberinde getirmiştir (Henkoğlu, 2017). Bilgi varlıklarının korunması açısından bu üç temel unsurun yanı sıra güvenilirlik, inkâr edememe, kimlik sınaması, yetkilendirme ve izlenebilirlik ya da kayıt tutma olmak üzere yeni alt başlıklar da bilgi güvenliğinin unsurları kapsamda değerlendirilmektedir.

5.3.1. **Gizlilik (Confidentiality)**

Bilgi gönderici ve alıcı arasında taşındığı/iletildiği tüm ortamlarda yetkisiz erişimlerden korunmalıdır. Gizlilik, erişim yetkisi olmayan kullanıcıların bilgilerin bulunduğu, saklandığı bilgisayar ve ağ sistemlerine, erişimlerinin engellenmesidir. Saldırganlar sistemler üzerinde yazılım hatalarını, açıklıklarını kullanarak sızma, ele geçirme, takip etme ya da sosyal mühendislik teknikleri gibi farklı yöntemlerle yetkili kullanıcıları istismar ederek bilgilere izinsiz olarak erişim sağlayabilmektedir (Yıldız M. , 2014). Stratejik olarak bilgi gizliliğinin sağlanması için alınacak önlemler incelenecek olursa, bilgilerin istenmeyen kişilerin eline geçmesi durumunda yaratabileceği zararın miktarı ve türüne göre kategorize edilmesi yaygın bir planlama türüdür. Veri şifreleme, kimlik ve biyometrik doğrulama, güvenlik belirteçleri, ağ bağlantısı kesilmiş depolama aygıtları, yetkisiz kullanıcıların erişimlerinin engellenmesinde kullanılan uygulamalar olarak karşımıza çıkmaktadır (Rouse, 2014).

5.3.2. **Bütünlük (Integrity)**

Bütünlük, bir veritabanında, veri ambarında ya da başka bir yapı içerisinde depolanan bilgilerin tüm yaşam döngüsü boyunca bozulmasını, değiştirilmesini, silinmesini engelleyerek tutarlılığını, doğruluğunu ve güvenilirliğini sürdürmeyi içerir. Bir durumu, süreci veya işlevi tanımlamak için kullanılan bütünlük kavramı eksiksiz veya tam bir yapıya sahip bilginin niteliğini ifade etmektedir. Bilginin taşınması sırasında izlediği yol boyunca bütün özellikleri, iş kuralları, ilişkileri, tarihleri ve tanımları doğru olmalıdır. Kısacası bilgi gerektiği şekilde tutulmalı ve korunmalıdır. Bu amaçla bilginin bütünlüğü için erişim kontrolünün gerçekleşmesi ve belli aralıklarla yedekleme işleminin yapılması gerekmektedir. Böylelikle bilginin gerek kayıtlı bulunduğu ortamda gerekse

de iletildiği ortamlarda yetkisiz kişilerce değiştirilmeden, ekleme çıkarma yapılmadan, tekrar edilmeden, bütünlüğü bozulmadan alıcısına ulaşması sağlanmış olur (Başaranoğlu, 2016). Bilgi bütünlüğün korunması için elektronik imza, açık anahtar altyapısı gibi teknolojiler kullanılmaktadır.

5.3.3. **Erişilebilirlik (Availability)**

Herhangi bir bilgi sisteminin amacına hizmet etmesi için, erişim yetkisi bulunan kullanıcıların ihtiyaç duydukları bilginin her an ulaşılabilir ve kullanılabilir durumda olması gerekir. Erişilebilirlik, bilginin işlenmesi, taşınması ve depolanması için yapılandırılan bilişim sistemlerinin, içeriden ve dışarıdan gelebilecek tehditlere karşı kullanılan güvenlik kontrollerinin ve erişimi sağlayan iletişim kanallarının doğru çalışması gerektiği anlamına gelir. Yüksek erişilebilirlik özellikli sistemler, elektrik kesintileri, donanım arızaları ve güncellemeler nedeniyle yaşanabilecek servis kesintilerini önlerken, ağa izinsiz giriş ve hizmet reddi saldırılarına (DDoS) karşı güvenlik sağlar. (Keung, 2014)

5.3.4. **Güvenilirlik (Reliability-Consistency)**

Güvenirlik, bir bilgisayar ya da bilgi iletişim sisteminin kurallar doğrultusunda, tasarımına uygun olarak sürekli çalışması, kendisinden beklenen şeyleri eksiksiz olarak tutarlı bir şekilde yapabilmesidir (Canbek & Sağıroğlu, 2006). Başka bir ifadeyle sistemler üzerindeki bilginin öngörülen ve beklenilen davranışları ile ortaya çıkan sonuçları arasında tutarlığının sağlanmasıdır.

5.3.5. **İnkâr Edememe (Non-Repudiation)**

İnkâr edememe bilgi güvenliğinde yaygın olarak kullanılan ve verilerin kaynağını ve verilerin bütünlüğünü kanıtlayan bir hizmet anlamına gelen yasal bir kavramdır. Bilgi sistemleri üzerinde gönderici ve alıcı durumundaki kullanıcılar arasında mesajların iletilmesi sırasında ortaya çıkabilecek iletişim sorunları ve anlaşmazlıkların çözülmesinde kullanılmaktadır. Sistem içerisinde iletilen bir mesajın nereden geldiği, kim tarafından kabul edildiği ile ilgili olarak işlemsel geçerliliğin ve bilginin orjinalliğinin inkâr edilememesidir. Gerçek zamanlı işlemlerin yapıldığı, mesaj iletiminin garanti edildiği finans sistemlerinde, dijital sözleşmelerde, imzalarda ve e-posta iletilerinde kullanılır. (Cryptomathic, 2018)

5.3.6. **Kimlik Doğrulaması (Authentication)**

Bilişim sistemi dâhilindeki bir sunucunun kendi bilgilerine veya sisteme tam olarak kimin eriştiğini bilmesi gerektiğinde cihaz veya kullanıcının sunucuya kimliğini kanıtlaması kimlik doğrulaması olarak tanımlanmaktadır. Kimlik doğrulama, kullanıcının hangi görevleri yapabileceğini veya hangi dosyalara erişebileceğini belirlemez, yalnızca kullanıcının kim olduğunu tanımlar, doğrular ve sisteme giriş yapılmasını sağlar. (TechWeb, 2018)

Kimlik doğrulama işlemi bilgi işlenen, iletilen, saklanan bir bilgisayar ya da ağ sistemininin güvenliği kapsamında erişim izni verilmeden önce kullanıcının sunucu tarafından kontrol edilen geçerli bir kullanıcı adı ve şifre girmesi ile tanımlanmasıdır. Sunucu, kullanıcının kimlik doğrulama bilgilerini bir veritabanında depolanan diğer kullanıcı bilgileriyle karşılaştırır, kimlik bilgileri eşleşirse, kullanıcıya erişim izni verilir, kimlik bilgileri değişiklik gösteriyorsa, kimlik doğrulama başarısız olur ve

erişim reddedilir (Rouse, 2014). Fiziksel sistemlerin gelişmesiyle birlikte akıllı kartlar, retina taraması, ses tanıma, parmak izi gibi biyometrik teknoloji uygulamaları da kimlik doğrulaması amacıyla kullanılmaktadır.

5.3.7. **Yetkilendirme (Authorization)**

Yetkilendirme, genel olarak kullanıcının kimliğini başarıyla doğruladığını varsayarak, bilgi güvenliği ve bilgisayar güvenliği ile ilgili bir dosyaya ya da kaynağa erişmek için uygun izne sahip olup olmadığının, belirli bir işlemi gerçekleştirip gerçekleştirmediğinin kontrol edilerek düzenlenmesidir. Bir başka deyişle, tanımlanmış ve kimlik doğrulaması yapılmış bir kullanıcının, sistemde hangi bilgiye erişebileceği ile ilgili izinlerin ve hangi eylemleri gerçekleştirebileceğiyle ilgili yetkilerin belirtilmesidir. (Curphey, 2002)

5.3.8. **İzlenebilirlik/Kayıt Tutma (Accountability)**

İzlenebilirlik ya da kayıt tutma bilgi güvenliği planı çerçevesinde bir bilişim sistemi içerisinde gerçekleşen herşeyin kayıt altına alınmasıdır. Kimliği doğrulanan bir kullanıcının sistem içerisindeki bütün hareketleri tarih, saat, ağ adresi vb. parametrelerle en alt seviyeden itibaren kaydedilmesi bilgi güvenliği açısından problemlerin denetimi, takip edilmesi, analizi ve çözümlenmesi için gereklidir.

İzlenebilirlik, eylemlerin veya eksikliklerin sorumluluğunu oluşturmak için eylemleri ve olayları zaman içinde kullanıcılara, sistemlere veya işlemlere geri izleme olanağı sunan bir kontrol mekanizmasıdır. Bir sistem ya da ağ yapısı içerisinde kullanıcılara ait iş ve işlemler izlenebilir ve kayıt altına alınabilir durumda değilse o sistem ya da ağ yapısı güvenli değildir (Bragg, 2002). İzlenebilirlik kapsamında kayıt altına alınacak bilgilere

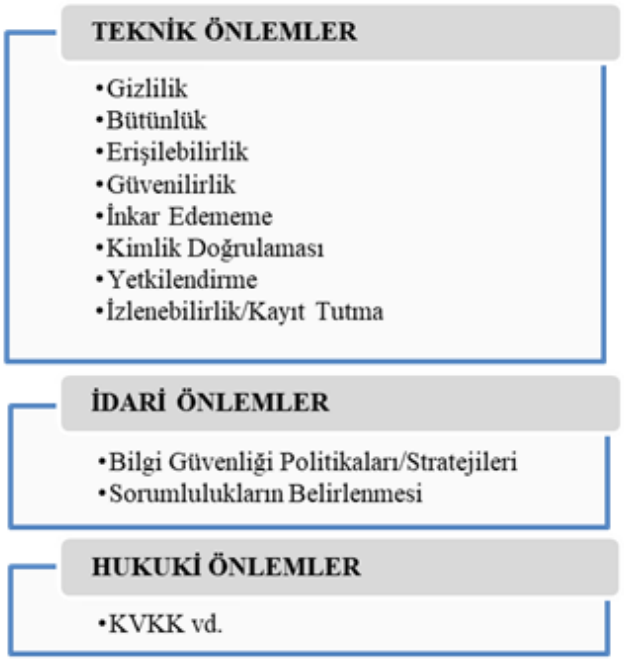
örnek olarak, bir web sitesine ya da çevrimiçi bir sisteme bağlanılması, ağ üzerindeki sunuculara erişim, e-posta gönderimi, sistem logları, olay günlükleri, kullanıcı adı ve şifre, web hareketleri vb. gösterilebilir. Herhangi bir sistem ya da ağ yapısı üzerinde depolanan olay kayıtları, kullanıcı kaynaklı bilinçli ya da bilinçsiz hataların tespit edilmesinde, ağ ya da sisteme yönelik saldırılara ve saldırganlara karşı alınması gereken önlemlerin belirlenmesinde kritik rol oynamaktadır.

5.4. **Bilgi Güvenliği Yönetimi**

Bilişim teknolojilerinin gelişimiyle ortaya çıkan elektronik altyapılı ağlar, web uygulamaları, uzaktan erişime açık çevrimiçi sistemler vb. sağladığı verimlilik artışı, iş süreçlerini ve iletişimi hızlandırma, organizasyon gibi özellikleriyle bilginin üretildiği ve kullanıldığı çok farklı ortamların oluşmasını sağlarken, bilgi varlıklarına yönelik risk ve tehditleri de beraberinde getirmiştir. Bilişim sistemlerine karşı yapılan saldırıların nitelik ve boyut olarak artışı karşısında geliştirilen teknik güvenlik önlemleri tek başlarına bilginin güvenliğini sağlamada yetersiz kalmaktadır. Yapılan araştırmalarda bilgi güvenliğine yönelik tehditler sıralamasında kişiler ve kurum içi çalışan kullanıcılar hala en başta gelen unsur olarak dikkat çekmektedir. (Tekerek, 2008)

Bilgi güvenliğinin sağlanması konusunda korunması gereken bilgi varlıklarının uygulama alanları içerisinde sınıflandırılması, güvenlik önlemleri ve tedbirlerin sistematik bir şekilde belirlenmesi ve bu kapsamda yürütülecek bütün faaliyetler bilgi güvenliği yönetimi süreci olarak tanımlanabilir. Bilgi güvenliği yönetimi süreci bilgi işlem merkezleri, veritabanları ve ağ sistemlerine yönelik alınacak teknik tedbirlerler ve sorumluluk paylaşımı temeline dayanan yönetsel (idari-hukuki) önlemlerin birarada planlandığı stratejilerle birlikte, insan faktörünün ön planda tutulduğu eğitim ve

farkındalık çalışmalarının bütünsel bir şekilde gerçekleştirilmesiyle sağlanabilir. (Henkoğlu, 2017)



Şekil 5.1 Bilgi Güvenliği Yönetimi Başlıca Unsurlar (Henkoğlu, 2017)

5.5. **Bilgi Güvenliği Sınıflandırması**

Bilgi güvenliği ile ilgili stratejiler ve standartlar bir araştırma firması olan Securosis tarafından şu şekilde sınıflandırılmıştır (Dilek, 2017);

- Ağ Güvenliği (Network Security)
- Uç/Son Nokta Güvenliği (Endpoint Security)
- Veri Güvenliği (Data Security)
- Uygulama Güvenliği (Application Security)
- Kimlik ve Erişim Yönetimi (Identity and Access Management)
- Güvenlik Yönetimi (Security Management)
- Sanallaştırma ve Bulut (Virtualization and Cloud)

5.5.1. **Ağ Güvenliği (Network Security)**

Bilgi ve kaynakların paylaşılması temelinde kurumlar ve şirketler tarafından kurulan bilgisayar ağları, kişisel kullanımı da içeren internet ile birlikte küresel çapta birbirine sistematik biçimde bağlı ağ sistemlerini ortaya çıkarmıştır. Bilgisayarlar ve farklı cihazların belirli standartlar ve protokoller çerçevesinde birbirlerine bağlandıkları ağ sistemlerinin sağladığı paylaşım ve uzaktan erişim imkânı kullanıcılar, kurumlar ve bilgi varlıkları için güvenlik açıklarını da beraberinde getirmektedir. Bilgisayar ağlarına ve sunuculara bu açıklıkları kullanarak içeriden ve dışarıdan yetkisiz erişim sağlayan saldırganlar, bilgi kaynaklarına zarar verme, sistem ve servislerin yapılarını değiştirme ya da tamamen kullanılamaz hale getirme gibi yöntemlerle kişisel ve kurumsal bilgi güvenliğine karşı ciddi tehdit oluşturmaktadırlar.

Ağ güvenliği, ağ altyapısının yetkisiz erişim, yanlış kullanım, arıza, değişiklik, imha veya uygunsuz ifşadan korunması ve böylece bilgisayarların, kullanıcıların ve programların görevlerini yerine getirebilmeleri için güvenli bir platform oluşturulması, fiziksel ve yazılım önleyici tedbirlerin alınması sürecidir. (Fruhlinger, 2018)

Bilginin gizlilik, bütünlük ve erişilebilirlik prensiplerinin korunmasını merkeze alan ağ güvenliğinin sağlanması süreci, ağ üzerindeki sistemlere bağlı çalışan donanımsal ve yazılımsal teknolojilerin güvenlik duvarları, saldırı tespit/önleme sitemleri, anti virüs sunucuları web filtreleri, log kayıtları vb. güvenlik mekanizmaları kullanılarak risk analizinin yapılmasıyla başlamaktadır. Organizasyon, kurum ve şirketlerin internet teknolojileri üzerinden genişlettikleri kendi ağ sistemlerine bağlı kaynakların kullanılması ile ilgili kuralların, risk analizi yapılan teknoloji altyapılarının ve alınacak güvenlik önlemlerinin genel hatlarıyla belirlendiği, ağ güvenlik politikalarının

oluşturulmasıyla da tamamlanmaktadır. (Can, 2014)

Güvenlik politikaları oluşturulurken korunacak ağ sistemi ve teknolojik altyapıyı sağlayan cihazların kullanacağı standartlar, sunucu protokolleri, erişim kuralları ile ilgili ayarlar yapılmalı ve zayıf noktaların tespiti için test edilmelidir. Ayrıca ağ güvenliği kapsamında korunacak nesnelerin nasıl ve kime karşı korunacağının belirlenmesi, bilgi varlıklarının saklama/yedekleme/arşivleme yöntemlerinin kurallara bağlanması, kullanıcılar, çalışanlar, yöneticiler için de sorumluluk alanı ve yaptırımların açıklanması diğer önlemler olarak gösterilebilir. (Karaarslan, 2017)

5.5.2. **Uç/Son Nokta Güvenliği (Network Security)**

Bir ağ sistemine bağlanabilen bütün cihazlar uç nokta olarak kabul edilir. Bilgi kaynaklarına yönelik güvenlik tehditleri için giriş noktaları olarak tanımlanan uç nokta cihazları ağ ve sistem güvenliğinin en zayıf halkası olmaları sebebiyle güçlü bir şekilde korunmaları gerekir.

Uç/Son Nokta Güvenliği bir ağ sitemine bağlı çalışan güvenlik için potansiyel bir giriş noktası oluşturan bilgisayar, tablet, akıllı telefon, barkod okuyucu, POS terminalleri gibi cihazların merkezi bir yapı üzerinden denetlendiği, ağ kaynaklarına erişimlerine izin verilmeden önce yetki ve kontrollerin sağlandığı, organizasyonel bir güvenlik çözümüdür. Kısaca ifade etmek gerekirse uç nokta güvenlik yönetim sistemleri, bir ağ sistemine erişim isteyen bilgisayar ve cihazları keşfeder, yönetir ve kontrol eder. (Carbon Black, 2018)

Ağ üzerindeki olağan aktiviteleri öğrenip olağan dışı bir aktivite tespit edildiğinde, şüpheli eylemi otomatik olarak durdurarak yetkili kontrol mercine uyarı göndermek

prensibiyle çalışan Uç/Son Nokta Güvenlik Yönetim Sistemleri, merkezi olarak yönetilen bir sunucu veya ağ geçidinin güvenlik programını barındırdığı ve her bir ağ cihazına eşlik eden bir istemci programının kurulu olduğu bir VPN istemci/sunucu modelinde, onaylanmış bir işletim sistemi ve güncellemeleri olan bir virüsten koruma yazılımı ile birlikte çalışır.

Uç/Son Nokta Güvenlik Sistemi, bir ağ yapısı üzerinde istemci tarafından oturum açılmaya çalışıldığında, sunucu programı ağa erişime izin vermeden önce tanımlı kurumsal güvenlik politikalarına uyulduğundan emin olmak için kullanıcı kimlik bilgilerini doğrular ve bilgisayar ya da cihazı tarar. Ağ güvenliği politikasına uymayan istemci uç noktalar, sistem tarafından farklı değişkenlerle kontrol edilerek yerel yönetim hakları olmayan sınırlı erişim izni verilir veya sanal bir LAN'da (VLAN) karantinaya alınır. (Kadrich, 2007)

Devletler, bilgisayar korsanları, organize suçlular ve kötü niyetli kullanıcılar vd. kaynaklı Uç/Son Nokta tehditlerinin hacmi ve karmaşıklığı giderek arttıkça, daha gelişmiş güvenlik çözümlerine ihtiyaç duyulmaktadır. Günümüzde uç nokta güvenliği sistemleri, devam etmekte olan saldırıları hızlı bir şekilde tespit etmek, analiz etmek, engellemek ve içermek üzere diğer güvenlik teknolojileriyle işbirliği yapacak şekilde tasarlanmakta ve geliştirilmektedir.

5.5.3. **Veri Güvenliği (Data Security)**

Veri Güvenliği, farklı veri kümelerinin göreceli önemini, hassasiyetlerini, yasal uyumluluk gerekliliklerini belirleyerek, dijital gizlilik kapsamında yetkisiz erişimleri önleyen bir dizi kontrol, uygulama ve teknik benimseyerek bir ağ üzerindeki dosyaları, veritabanlarını ve hesapları koruma işlemidir. (Winston, 2018)

Veri güvenliğinin ana odağı, verilerin sadece yetkisiz erişimlerden değil aynı zamanda her türlü yıkıcı tehlikeden uzakta, güvenli ve korumalı tutulmasını sağlamaktır. Veriler, veritabanlarında, bilgisayarlarda ve ağ sistemleri üzerinde ham form halinde satırlar ve sütunlar şeklinde depolanır. Bu verilerin bir kısmının gizlilik düzeyi yüksek nitelikli olmayabilirken, değeri özel ve önem taşıyan veriler bilgisayar virüsleri, yetkisiz erişim, yolsuzluk, sızdırma, veri hırsızlığı, kötüye kullanma, güvenlik ihlali gibi tehditlerle karşı karşıya kalmaktadır (Martin, 2015). Bilgi varlıklarına yönelik tehditlerin gerçekleşme olasılığı, sistemlerin fiziksel açıklıkları ve sahip olunan bilgi kaynaklarının değeri ile doğru orantılıdır.

Veri güvenliği 3 temel alan içerisindeki faaliyetleri kapsamaktadır.

Yangın, deprem, sel gibi doğal afetler ya da çalınma, düşme, zarar görme benzeri dış etkenler sonucu güç kaynakları, santraller vb. teknoloji altyapısında meydana gelen donanımsal arızalar karşısında uygulanacak fiziksel güvenlik;

Bilgi kaynaklarına, sistemlere, cihazlara fiziksel olarak erişebilen kullanıcıların yetki ve izinlerinin kontrol edilmesinden, sistem arızalarının giderilmesine kadar uzanan geniş bir koruma durumunu ifade eden bilgisayar, cihaz güvenliği;

Belirli bir alan içerisindeki yerel alan ağlarından (LAN) başlayarak, internet teknolojileriyle genişletilmiş karmaşık ağ yapılarına kadar ağ sitemleri dâhilinde çalışan bilgisayar ve cihazların birbirleriyle iletişimlerinden ortaya çıkan risk ve tehditlerin önlenmesi amaçlı sağlanacak iletişim güvenliği bu alanları oluşturmaktadır. (Kaya Ö. F., 2017)

5.5.4. **Uygulama Güvenliği (Application Security)**

Uygulama güvenliği, kişi ve kuruluşların kritik verilerini dışarıdan gelen bütün tehditlere karşı korumaları için, üretilen/satın alınan/indirilen uygulamaların güvenlik zaafiyetleri açısından incelenmesidir (Profelis, 2018). İnternet ve iletişim teknolojilerinin gelişmesiyle birlikte sosyalleşme, bilgi paylaşımı, kamu hizmetleri, ticaret, finans, eğlence gibi pek çok alanda yaygın kişisel ve kurumsal kullanım imkânı bulan uygulama yazılımları siber saldırıların ve veri hırsızlarının hedefi haline gelmiştir. Saldırganlar hem ağ sistemleri, bilgisayarlar ve mobil iletişim araçlarının zaafiyetlerini kullanarak, hem de bu ortamlarda işlevselliği bulunan uygulama yazılımlarının açıklıkları üzerinden bilgi varlıklarının güvenliğine yönelik tehdit ve risk oluşturmaktadırlar. (Fearn, 2018)

Güvenlik standartları perspektifinde uygulama yazılımlarının potansiyel açıkları ve zayıf noktalarının tespit edilmesine yönelik davranış analizi, zaafiyet tarayıcı sistemler vb. teknolojiler karşımıza çıkmaktadır.

5.5.5. **Kimlik Doğrulama ve Erişim (Identity and Access Management)**

Kimlik ve Erişim Yönetimi (IAM), kullanıcıların uygulamalara ve sistemlere erişimi de dâhil olmak üzere, ağdaki kullanıcıları ve kaynakları yönetmeye odaklanan işlemler için kullanılan bir terimdir. Kimlik ve Erişim Yönetimi (IAM), doğru kullanıcının doğru zamanda, doğru bilgiye ulaşmasında sistemlerle etkileşim halindeki kullanıcıların erişim haklarının belirlenmesi, uygulanması ve yetkilendirilmesi sürecidir. (Tools4ever, 2019)

Kimlik ve Erişim Yönetimi güvenliğinde yaygın uygulamalar kullanıcı adı ve şifre kombinasyonları, akıllı kartlar, tek kullanımlık parolalar, elektronik imza ve biyometrik (retina, parmak izi) teknolojilerdir.

5.5.6. **Güvenlik Yönetimi (Security Management)**

Güvenlik yönetimi, bir organizasyon ya da kuruluşa ait bütün varlıkların (insanlar, binalar, makineler, sistemler, finans kaynakları ve bilgi varlıkları dâhil) tanımlanması ve ardından bu varlıkların korunması için gerekli fiziksel /dijital altyapının hazırlanması, tehdit ve risklere karşı erişim denetimi odaklı güvenlik politikaları ve prosedürlerin geliştirilmesi, belgelendirilmesi ve uygulanmasıdır. (Wikipedia, 2019)

Güvenlik yönetimi, yöneticiler ve çalışanların çalışma ortamının düzenlenmesi için insan kaynakları güvenliği, fiziksel/çevresel güvenlik, uygunluk, iş sürekliliği yönetimi, haberleşme/operasyon yönetimi kapsamında gerekli standartların oluşturulduğu, sistemlerin verimli çalışabilmesi çerçevesinde de bilgi güvenliğine yönelik risklerin belirlenmesinin ardından erişim kontrol ve denetimi, bilgi sistemleri edinimi, organizasasyon, geliştirme ve bakım, olay yönetimi gibi farklı kontrol alanlarının kullanıldığı sistematik bir yapıdır. (Uğuz, 2018)

5.5.7. **Sanallaştırma Yönetimi ve Bulut Bilişim (Virtualization and Cloud)**

Bulut Teknolojisi/Bulut Bilişim (Cloud Computing) kavramı bilgi güvenliği sınıflandırması içerisinde diğer önemli bir yapıyı ifade etmektedir. Dijital dünyada gelişmiş akıllı teknolojilerin kullanımıyla kullanıcılar tarafından üretilen verinin çeşitliliği ve boyutu her geçen gün sınırsız bir şekilde artmaya devam etmektedir. Üretilen bu sınırsız verinin güvenliğinin sağlanarak saklanması ve istenildiğinde kullanılmak üzere her yerden, çok hızlı bir şekilde ulaşılabilir olması temeline dayanan bulut bilişim ile ilgili alanyazına girmiş farklı tanımlar mevcuttur. Yapılan tanımlarda yaygın olarak temel alınan Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ‘e göre Bulut Bilişim, en az yönetim çabası ve servis sağlayıcı

etkileşimi ile hızlı bir şekilde erişilebilen, paylaşılabilir ve yapılandırılabilir bir bilgi işlem kaynağına (ağlar, sunucular, veri depolama alanları, uygulamalar ve hizmetler) her yerden, kolaylıkla, isteğe bağlı ağ erişiminin sağlandığı bir modeldir. (Mell & Grance, 2011)

Bulut Bilişim tanımı içerisinde kullanılan bilişim kaynaklarının kullanıldığı ortak ve paylaşıma açık bir ortam; her türlü cihazla, istenilen yerden, istenildiği zaman bilgi kaynaklarına ulaşmayı sağlayan internet'e karşılık gelmektedir. İnternet ile birlikte tanımlanacak olursa, Bulut Bilişim internet altyapısı içerisinde kullanıcıların hizmetlere ve verilere zamana ve mekâna bağlı kalmaksızın daha hızlı ulaşabilmelerine olanak sağlayan, çoklu sunucu bağlantıları sayesinde erişim gerçekleştirilen yazılım tabanlı uygulamaları ve bu hizmetlerin yürütüldüğü veri işleme ve depolama ortamlarını kapsayan teknolojik yapıdır. (Bulut, 2018)

Bulut Bilişim hem altyapısında farklı teknolojilerin kullanılıyor olması hem de verilerin ortak bir alanda saklanması ve sunulan servislerin, uygulamaların erişim özellikleri nedeniyle geleneksel bilişim teknolojileri ortamlarından daha fazla güvenlik riskine sahiptir. Bulut Bilişim yüksek erişilebilirlik ve veri güvenliğini temel alan güvenlik politikalarının oluşturulması ile servis ve altyapı hizmetlerine yönelik saldırı ve sızma girişimlerine karşı korumayı hedeflemektedir. Bu çerçevede bulut bilişim modeli içerisinde kullanıcıları zararlı yazılımlara, sistem üzerindeki açıklıklara ve saldırılara karşı korumak amacıyla bulut-içi (in the cloud) tarama hizmetleri, saldırı tespit sistemleri gibi güvenlik çözümleri kullanılmaktadır. (Furuncu, 2018)

Son kullanıcı cihazları, uygulamalar, web servisleri, veri depolama merkezleri gibi bileşenlerin oluşturduğu bulut bilişim altyapısındaki önemli platformlardan birisi

sanallaştırma teknolojisidir. Sanallaştırma teknolojisi ile donanım altyapısı ve sistem yazılımları arasındaki iletişim ve bilgi paylaşımı çerçevesinde kullanıcıların ölçeklendilmiş katmanlı bir model içerisinde farklı servis ve hizmetlerden yararlanması sağlanmaktadır.

Sanallaştırma, mevcut donanım kaynaklarının mantıksal bölümlere ayrıştırılırak birden fazla sunucu ya da fiziksel makinenin aynı kaynakları paylaşmasını sağlayan yazılım uygulamalarıdır. Başka bir ifadeyle misafir olarak tanımlanan birden fazla işletim sisteminin aynı donanım kaynaklarını (sunucu, depolama, ağ cihazları vb.) paylaşarak ağ üzerinde yüklü yazılımların fiziksel bağımlılıklarını en aza indiren sistemlerdir (Moral, 2016). Sanallaştırma, yazılım temelinde işletim sisteminin, donanımsal olarak ta bilgisayarların, cihazların, depolama ortamlarının ve ağ yapısının fiziksel varlığının yerine sanal bir uygulamasının oluşturulmasıdır.

Sanallaştırma yazılımlarıyla birden fazla işletim sistemini aynı bilgisayar içerisinde paralel olarak çalıştırabilen sanal makineler (Virtual Machine - VM) kullanıcının doğrudan fiziksel sistem kaynaklarına erişim sağlayamadığı katmanlı bir yapı meydana getirirler. Sanallaştırma mimarisi fiziksel donanımlar üzerinde çalışan Hypervisor veya VMM (Virtual Machine Monitor) olarak adlandırılan sanal makineleri ve işletim sistemlerini yöneten mantıksal bir katman tarafından oluşturulur. Hypervisor sanal sistemlerin yöneticisi olarak kullanıcı ile donanım yapısı arasında kurduğu sürekli iletişim ile sisteme ait fiziksel kaynakları işletim sisteminden gizler ve erişimlerin yönlendirilmesini sağlar. Sanallaştırılmış bir IT ortamı olan katmanlı yapı içerisinde sanal alt yapı, sanal makineler (Virtual Machine - VM), paylaşılan işlemciler, veri depolama alanları, bellekler ve diğer kaynaklar bulunur. (Moral, 2016)

Sanallaştırma teknolojileri uygulama alanlarına göre farklı yapılar içerisinde sınıflandırılır.

- Ağ ve Sunucu Sanallaştırma
- İşletim Sistemi Sanallaştırma
- Oturum Sanallaştırma
- Depolama Alanı Sanallaştırma
- Masaüstü ve Dizüstü Sanallaştırma
- Uygulama Sanallaştırma

Sanallaştırma teknolojileri, organizasyon ve kurumsal anlamda ölçeklendirme, işlevsellik, maliyetlerin azalması, iş gücü verimliliği, kaynak tasarrufu, yük dengeleme gibi avantajlar sunmasının yanı sıra, bilgi güvenliği süreçlerini de desteklemektedir. Sistem üzerindeki merkezileşen kaynakları ortak kullanan sanal makineler, birbirlerinden bağımsız çalışabilme özellikleriyle, sanal sistem yapısını ve kendilerine ait kaynakları olası saldırı ataklarından, zararlı yazılımlardan soyutlayarak, izole biçimde tutabilirler. (Çalışkan, 2014)

Sanallaştırma uygulamalarında bilgi güvenliği kapsamında sistem ve sunucular açısından; Yazılımların güncel sürümlerinin kullanılması, ağ trafiğinin fiziksel altyapısına yönelik güvenlik politikalarının uygulanması, yönetim hesaplarının farklı seviyelerde yetkilendirilmesi, sanal sistemlere ait log kayıtlarının, imaj ve görüntülerin tutulması, zaman bilgilerinin NTP sunucularından alınması, sistemlere erişim kısıtlaması getirilmesi, gereksiz donanımların kaldırılması, güvenlik açığı oluşturabilecek servislerin (rdp, ntp sunucu, telnet, tftp vb.) kapatılması, uygulama güvenlik seviyesinin artırılması ve ağa bağlı yapıların birbirlerinden izole hale

getirilmesi gereklidir. Ayrıca fiziksel sisteme, altyapıya ya da fiziksel sisteme bağlı çalışan herhangi bir sanal sisteme sızılması durumunda bütün fiziksel ve sanal sistemlere sızma olduğu varsayılarak bilgi kaynakları koruma altına alınmalı ve güvenlik sağlanmalıdır. (webhostingturkey, 2015)

5.5.8. **Siber Güvenlik**

Teknolojik parametrelerin genişlemesiyle sayısı milyarlarla ifade edilen bilgisayar ve elektronik cihazın, ağ tabanlı sistemler üzerinden internet aracılığıyla birbirlerine bağlanarak etkileşim içerisinde olduğu dijital dünya siber uzay olarak adlandırılan yeni bir yapıyla tanımlanmaktadır.

Verilerin bilgisayarlar ve elektronik cihazlar kullanılarak üretildiği, iletildiği, değiştirildiği ve depolandığı başta internet olmak üzere ağ sistemleri ve iletişim platformlarını, bilgi teknolojileri altyapısını, kullanıcıları ve diğer tüm aktörleri tanım alanı içerisinde barındıran siber uzay çok yönlülüğüyle bilgi güvenliğinin boyutlarının da değişmesine neden olmuştur. Dijital teknolojilerin bireyler, kurumlar ve devletler tarafından sosyo-ekonomik, siyasal ve endüstriyel bütün alanlarda kullanılmasıyla birlikte neredeyse bilginin bulunduğu coğrafi ve fiziksel her noktanın bir hedef haline geldiği siber uzayda, bilginin güvenliğinin sağlanması kapsamında alınacak tedbir ve önlemler bilgi güvenliğinin bir alt kümesi olarak nitelendirilen siber güvenlik kavramını ortaya çıkarmıştır. (Amit, 2016)

Siber güvenlik, siber uzayı oluşturan küresel devlet, organizasyon ve kuruluşların sahip oldukları endüstriyel, finansal, askeri, teknolojik bütün alanlarda kullanılan bilgi teknolojilerini, telekomünikasyon sistemlerini, kritik altyapılarını ve iletilen, depolanan bilgi varlıklarını korumak için geliştirdikleri stratejilerin bütünüdür. (Buch, 2018)

Bilgi güvenliği ve siber güvenlik kavramları güvenlik terminolojisinde genellikle içiçe kullanılmaktadır. Bilgi güvenliği uzmanları bilgi güvenliğini varolduğu her ortamda bilginin korunmasına yönelik bütün uygulamalar olarak geniş bir perspektifde değerlendirirken siber güvenliği dijital teknoloji altyapısına ve bilgi varlıklarına dışardan gelecek saldırılara karşı alınacak önlemler olarak ifade etmektedir. Günümüzde siber uzayda varolan bilgilerin elektronik ortamlarda kaydediliyor olması ve yetkisiz kullanıcılar tarafından yapılan siber saldırıların bilgi bütünlüğüne, gizliliğine zarar vermeyi amaçlaması nedeniyle bilgi güvenliği ve siber güvenlik aynı yapısal özellikleri göstermektidir. Dolayısıyla da alanyazında genel ifade ediliş biçimiyle birbirlerinin yerine kullanılabilmektedir.

Siber güvenlik ile ilgili tanımsal çerçeve incelendiğinde geçerliliği olan en kapsamlı tanım Uluslararası Telekomünikasyon Birliği (ITU) tarafından yapılmıştır. ITU'ya göre siber güvenlik, organizasyon, kurum ve kullanıcıların dijital ortamlardaki telekomünikasyon altyapıları, iletişim ağlarına bağlı bilgisayarlar, mobil cihazlar, hizmetler ve bütün bu sistem içerisindeki iletilen/depolanan bilgilerden oluşan varlıklarını korumak için kullanılan araçlar, politikalar, güvenlik önlemleri, risk yönetimi yaklaşımları, eylemler, eğitimler, en iyi uygulamalar ve teknolojilerin bütünüdür. (ITU, 2018)

Küresel dijital dünyada siber tehditlerin en çok etkilediği alan endüstriyel ekosistem içerisinde aksamaları ya da bozulmaları durumunda sosyal ve ekonomik yapıya ciddi zarar verebilecek toplumsal düzenin, devlet ve kurumların sağlıklı bir şekilde işlemesi için gerekli olan birbirlerine bağlı fiziksel ve sayısal sistemler, organizasyonlar şeklinde tanımlanan kritik altyapılardır. Enerji üretim ve dağıtım sistemleri (nükleer

santraller, doğalgaz üretim işleme tesisleri), telekomünikasyon altyapısı, su ve kanalizasyon sistemleri, uzay-uydu sistemleri, ulaşım ağları, askeri komuta ve kontrol tesisleri, barajlar vb. sistemler kritik altyapılar olarak örneklendirilebilir. (CoESS, 2018)

Bilgi ve iletişim teknolojilerinde yaşanan çok hızlı değişimle ortaya çıkan yeni çoklu özel ve genel bulut stratejileri, gittikçe artan sayıda IoT ve uç nokta cihazları, işletmelerin ve bireylerin dijital ayak izlerini genişletirken, hem sahip olunan teknolojilere hem de bilgi varlıklarına yönelik siber tehditlerin boyutunu, kapsamını ve etki alanını da genişletmektedir.

Kaspersky Lab'in küresel internet trafiğini izlemek üzere programladığı tehdit izleme altyapısından elde edilen verilere dayanarak hazırlanan rapor (Kaspersky Security Bulletin 2018) (Vicente, 2019), veri ihalleri ve siber tehditlerin günümüzde geldiği nokta açısından önemli ayrıntılar içermektedir. 2018 yılı içerisinde Kaspersky Lab tespit teknolojileri tarafından dijital ortamda yılın ilk on ayında her gün 346 bin yeni zararlı dosya yakalanmış, dünya genelinde çevrimiçi kaynaklar üzerinde 554 milyon kötü niyetli URL web adresi ve 21 milyon benzersiz zararlı nesne ile tüm dünyada kullanılan bilgisayarların yaklaşık olarak %30'unu etkileyen 1 milyar 876 milyon farklı siber saldırının gerçekleştirildiği tespit edilmiştir.

Zararlı yazılımların tür ve çeşitliliği siber saldırganların ilgi alanlarının, yazılımları dağıtım yöntemlerinin ve kullandıkları vektörlerin geniş bir stratejik perspektife ulaştığını göstermektedir. Saldırıların sayısındaki artışla birlikte bu saldırılardan etkilenen tekil kullanıcı sayısı da 2017 yılına oranla önemli ölçüde artmıştır. 2017 yılı içerisinde siber saldırırlar nedeniyle zarar gören kullanıcı sayısı 774 bin kişiyken 2018 yılında yaklaşık 10 milyon kişiye ulaşmıştır. 765 bin kullanıcıyı etkileyen, küresel çapta

5 milyar dolar maddi kayıp yaşanmasına neden olan fidye yazılımları (ramsomware) kullanıcıların en çok karşılaştığı siber saldırı çeşidi olmuştur.

Siber tehditler, kaynakları, yöntem ve hedefleri bakımından küresel dijital dünyanın en önemli sorunlarından birisi halini almış durumdadır. Son iki yıl içerisinde yaşanan önemli siber güvenlik olayları etkileri açısından bu durumu açıkça göstermektedir.

Tablo 5.1 Siber Saldırı ve Veri Sızıntısı Olayları (Bus. Ins., 2018) (Gb, 2018)

HBO Şubat 2017	ABD'li TV kanalı ve yayıncı HBO'yu hackleyen Mr. Smith adlı hacker grubu Game of Thrones dizisinin senaryolarını, oyuncularının kişisel telefon numaralarını, e-posta adreslerini yayınladı.
WannaCry Mayıs 2017	150'ye yakın ülkede 300.000'den fazla sistem saldırıdan etkilendi. Başta sağlık sektörü ve telekomünikasyon şirketlerinde olmak üzere dünya çapında kuruluşları etkiledi.
EQUIFAX Mayıs 2017	Dünyanın önde gelen kredi raporlama ve kimlik hırsızlığına karşı koruma hizmetleri veren firmalarından Amerikan EQUIFAX'în 143 milyon müşterisinin kişisel bilgileri çalındı.
NotPetya Haziran 2017	Ukrayna'nın devlet kurumları ve büyük ölçekteki şirketlerin öncelikle hedef alındığı saldırı, kısa zamanda petrol ve gaz şirketlerinden (Rosneft-Rusya), limanlara

	(Maersk-Danimarka) kadar uluslararası çapta yarattığı etki ve verdiği zararla şimdiden tarihteki en büyük siber olaylardan birisi haline gelmiştir.
DYN Ekim 2017	Mirai adındaki zararlı yazılım kullanılarak yapılan siber saldırı, medya ve eğlence sektöründe hizmet veren aralarında Twitter, Spotify, HBQ, Netflix'in de bulunduğu büyük internet sitelerine alan adı sağlayıcılığı yapan DYN'i hedef almıştır.
Olimpiyat Destroyer Şubat 2018	Güney Kore'de gerçekleşen Pyeongchang Kış Olimpiyatları, açılış töreni siber korsanların hedefi oldu. Açılış töreninin yapıldığı stadyumda internet ve televizyon bağlantıları kesildi.
MyFitnessPal Nisan 2018	ABD'nin en büyük spor giyim ve ayakkabı üreticilerinden Under Armour'a yönelik siber saldırı nedeniyle yaşanan veri sızıntısı sonucu yaklaşık 150 milyon kullanıcıya ait bilgiler çalındı.
Saks Lord & Taylor Nisan 2018	Saks and Lord&Taylor mağazalarında yazarkasa sistemlerine yerleştirilen bir yazılım aracılığıyla 5 milyon müşteriye ait kredi kartı bilgileri çalındı.
MyHeritage Haziran 2018	İsrail merkezli DNA web platformu olan MyHeritage'in yaşadığı veri ihlaliyle 26 Ekim 2017'ye kadar sisteme kayıt olan yaklaşık 92 milyon kullanıcı etkilendi.

British Airways Ağustos 2018	British Airways web sitesinden ve mobil uygulaması üzerinden uçak bileti satın alan yaklaşık 380.000 kişinin kişisel verileri çalındı.
T-Mobile Ağustos 2018	Dünyanın en büyük telekom operatörleri arasında yer alan T-Mobile'a yapılan siber saldırıyla 2,3 milyon kullanıcıya ait kişisel veriler çalındı.
Facebook Eylül 2018	Sosyal medya platformu facebook'un sistemleri üzerindeki bir güvenlik açığı nedeniyle 50 milyon kullanıcıya ait bilgiler siber korsanlar tarafından çalındı.
Chegg Eylül 2018	Eğitim teknolojileri alanında faaliyet gösteren ABD'li Chegg şirketine ait veritabanları siber saldırıya uğradı. 40 milyon kullanıcıya ait bilgiler saldırıdan etkilendi.
C. P. Airways Ekim 2018	Hong Kong merkezli Cathay Pacific Havayolları şirketine yapılan siber saldırı ile 9,4 milyon müşteriye ait veriler çalındı.
Marriot and Starwood Aralık 2018	Dünyanın önde gelen otel zincirlerinden birisi olan Marriott'un ziyaretçi veri tabanı hacklendi. Son 4 yılda bu otellerde kalan 500 milyon müşterinin isim, adres, telefon numarası, e-posta, pasaport numarası, kredi kartı hesap bilgileri, varış ve kalkış bilgileri siber saldırganlar tarafından ele geçirildi.

Quora Aralık 2018	Soru-cevap kaynaklı internet bilgi platformu Quora'ya yapılan siber saldırı ile 100 milyon kullanıcıya ait ad ve soyad, e-posta adresleri, şifreler, platformda paylaştıkları iletiler ve bağlantılı hesaplardan içe aktarılan bilgiler hackerlar tarafından ele geçirildi.

5.6. **Bilgi Güvenliğine Yönelik Tehditler**

Sistemler arası veri/bilgi aktarımının ön planda olduğu, veriler ve insanlar arasındaki bağlantıları tek bir çatı altında toplayan internetin gelişimiyle birlikte, kişiler, kurumlar ve devletler teknolojik altyapılarını bilişim sistemleriyle bütünleştirmişlerdir. Bu bütünleşme hem elektronik ortamlarda saklanan bilgi kaynaklarının güvenliğine yönelik, hem de sunulan hizmet, iş ve işlemlere yönelik tehditleri de beraberinde getirmiştir. Kurumlar, işletmeler ve kullanıcılar sistemler üzerindeki açıklıklar, bilgisayar korsanları, kurum içi çalışanlar, zararlı yazılımlar, yangın, su baskını, terör gibi iç ve dış kaynaklı tehditlerin hedefi haline gelmiştir. Bilgi güvenliğine yönelik iç ve dış kaynaklı bu tehditler yetkisiz erişim, veri hırsızlığı, sistemlere zarar verme, servisleri izinsiz kullanma, ağ trafiğini meşgul etme, hizmet durdurma, sistemleri devredışı bırakma, kritik altyapılara sabotaj vb. şekillerde karşımıza çıkmaktadır. Bilgi güvenliğini tehdit eden saldırı türleri şu şekilde gruplandırılabilir. (BGA, 2018)

5.6.1. **Gelişmiş Hedef Odaklı Saldırılar (Advanced Persistent Threats)**

Daha önceden belirlenen bir ağ sistemine farklı sızma yöntemlerini kullanarak (internet üzerinden ya da fiziksel yollardan zararlı yazılım bulaştırma, insan faktörü, dış çevreden

bilgi toplama, sosyal mühendislik) yetkisiz erişim sağlayan saldırganların, sistemi tamamen etkisiz hale getirmeyerek haftalar aylar boyunca farkedilmeden sistem içerisinde kalıp maksimum miktarda veriyi topladığı saldırı türüdür. Saldırgan bilindik saldırı teknikleriyle sistemi bir anda ele geçirmek yerine durum ve yapıyı gözlemleyerek sistemi yavaş yavaş ele geçirir. Hedef sistem ne kadar güçlü korunursa korunsun APT saldırıları hedefe odaklanması, çok yönlü oluşu, gelişmiş sofistike araçların, iç tehdit unsurlarının ve güvenli bağlantıların kullanılması sebebiyle sonuçları tehlikeli ve oldukça zarar vericidir. (Kayar, 2014)

Sistem üzerinde APT saldırısı olduğunu gösteren bazı durumlar şunlardır;

- Çalışma saatleri dışında sistem üzerinde alınan log kayıtları,
- Saldırganın sisteme tekrar girmesini sağlayan arka kapı trojan yazılımlarıyla karşılaşılması,
- Bilgisayarlar ve sunucular arasında normal dışı veri akışları,
- Büyük miktarlarda sıkıştırılmış verilerin tespit edilmesi,

5.6.2. **Zararlı Yazılımlar (Maliciosus Software - Malware)**

Zararlı (Kötücül) yazılım (Malware), bilgisayar ya da ağ sistemlerine zarar vermek, aksatmak, çalışmalarını engellemek, bilgi kaynaklarında kayıtlı bilgileri çalmak ya da kullanıcıları rahatsız etmek amacıyla hazırlanmış istenmeyen türdeki yazılımların genel adıdır (Canbek, 2005). Zararlı yazılımlar, işletim sistemleri, programlar ya da uygulamalardaki güvenlik zaafiyetleri ve açıklıkları kullanarak, program güncelleme, dosya indirme, e posta, mesaj vb. harici kaynaklardan gelen eklentilerin çalıştırılması ile ziyaret edilen bir web sitesinden, bağlantı için kullanılan bir wifi ağı üzerinden veya USB bellek, taşınabilir harddisk vb. fiziksel araçlar gibi çok farklı şekillerde sistemlere

bulaşabilmektedir. Kişisel kullanıcıları ve sistemleri tehdit eden zararlı yazılımlar, internet ve ağ teknolojilerinin gelişimiyle birlikte elde ettikleri hareket kolaylığı ile hedef sistemlere çok hızlı biçimde ulaşabilmektedir.

Genel olarak yaşam döngüleri içerisinde kendi kendini çoğaltabilme, gizlenme, yokedilmeye karşı direnç gösterme, özerklik gibi karakteristik özellikleriyle bilgi ve bilgisayar güvenliğini tehdit eden zararlı yazılımların, virüsler, solucanlar (worms), truva atları, casus yazılımlar (spyware), arka kapılar (back doors), klavye izleyiciler (keylogger), mesaj sağanakları (spam), reklam görünümlü (adware) vd. alt türleri bulunmaktadır. (Canbek & Sağıroğlu, 2007)

5.6.3. **Virüsler**

Virüs, bilgisayar ortamında programlar ya da dosyalar içerisinde gömülü olarak bulunan, sistem kaynaklarını kullanarak kendi kendini çoğaltabilen, kopyalandığı ya da paylaşıldığında diğer dosya, belge veya bilgisayarlara bulaşabilen, işletim sistemi, programlar ya da uygulamalara zarar verebilen yazılım kodlarıdır (Keleştemur, 2015). Virüslerin diğer zararlı yazılımlardan ayrıldığı en önemli nokta etkileşim gerektirmesidir. Bilgisayar sistemlerine virüs kodu taşıyan dosyanın ya da programın açılması, e posta ile gelen bir linke tıklanması, virüs bulaşmış bir USB belleğin takılması vb. farklı şekillerde bulaşabilen virüsler, yayılmak için mutlaka insan etkileşimine ihtiyaç duyarlar.

İşletim sistemleri içerisinde karşılaşılan dosya virüsleri, sabit diske bulaşan ve bilgisayar her açıldığında etkinleşen önyükleme (boot) virüsleri, Word, Excel gibi makro desteğiyle çalışan programları etkileyen makro virüsleri ve Visual Basic, HTML, Java vb. programlama dillerinin kod yapısını bozan betik (script) virüsler başlıca virüs

türleridir. (Kaya A. , 2016)

Solucanlar (Worms)

Solucanlar benzer niteliklerde oldukları virüsler gibi kendilerini bir bilgisayardan ya da cihazdan başkasına kopyalamak amacıyla oluşturulmuşlardır. Karmaşık yapılarıyla herhangi bir sisteme girdiklerinde dosya, veri transferi yapan fonsiyonel programların ve uygulamaların denetimini ele geçirirler, kullanıcı etkileşimine ihtiyaç duymadan, kendilerini çoğaltarak e posta ya da adres listesi gibi veri kaynaklarını kullanarak, ağ ve sistemler üzerinde bulunan diğer kullanıcılara ulaşmaya çalışırlar. Başka sistemlere ve bilgisayarlara bulaşmak için herhangi bir programın ya da dosyanın içerisine gizlenmeden kendilerine yarattıkları bir tünelle sistemleri uzaktan erişime açarlar. Solucanlar bulaştıkları ağ üzerindeki veri kaynaklarını ve bant genişliklerini kullandıkları için, ağ sisteminin devre dışı kalmasına, bilgisayarların kilitlenmesine, sunucuların aşırı yüklenmesine ya da internet erişim hızının düşmesine sebep olabilmektedirler. (BİDB, 2013)

Truva Atları (Trojans)

Truva atları yararlı ve kullanılabilir gibi görünen herhangi bir programın ya da uygulamanın içerisine gizlenmiş bilişim sistemlerine zarar veren zararlı yazılımlardır. Temel çalışma prensibi hedef sistem içerisinde yarattıkları boşluklar ile programcısına müdehale edebileceği bir ortam ve alan yaratmaktır. Truva atları gönderilen bir dosya program ya da veri paketinin içerisinde gizlenen zararlı kodun çalıştırılmasıyla arka kapı adı verilen portları açarak bilgisayar sistemlerine yetkisiz erişim sağlanması ve kullanıcıların şifre, kredi kartı gibi kişisel bilgilerinin elde edilmesi amacıyla kullanılmaktadır. Virüslerden farklı olarak kendi kendilerini çoğaltamayan truva atları,

bilgisayar ortamında işletim sisteminin yavaşlaması, mikroişlemcinin işleme süreçlerindeki anormallik, kendiliğinden açılan pencereler, reklamlar ve spam maillerdeki artış vb. durumlar yaratabilmektedir. (Zacks, 2018)

Casus Yazılımlar (Spyware)

Casus yazılım bilgisayar sistemlerine sızarak kullanıcılara ait hassas bilgilerin ya da internet kullanımı gibi işlem verilerinin kullanıcının haberi olmadan izlenerek, toplanmasını ve kötü niyetli kişilere aktarılmasını sağlayan yazılım kodlarıdır. Genellikle internet üzerinden indirilen oyun, program, uygulama gibi ücretsiz yazılımlardan, yarışma, reklam benzeri web sitelerinden ya da spam mailler yoluyla sistemlere bulaşan casus yazılımlar virüsler ya da solucanlar gibi kendi kendilerini çoğaltarak farklı ortamlara yayılma ihtiyacı hissetmezler. Casus yazılımların temel amacı hedef seçilen sistem içerisinde gizlenerek istenilen bilgileri toplamaktır. (Canbek & Sağıroğlu, 2007)

Arka Kapılar (Back Doors)

Farklı senaryo ve saldırı teknikleriyle bilgisayar sistemleri üzerindeki açıklıklardan faydalanarak, erişim/kimlik kanıtlama süreçleriyle tespit edilemeyecek bir biçimde o sisteme sızmak için oluşturulan açık noktalar arka kapı olarak tanımlanmaktadır. Kısaca arka kapı herhangi bir bilgisayar sistemine erişim izni olmaksızın giriş yapabilmek amacıyla sistem üzerinde oluşturulan açıklardır. Arkakapı saldırılarıları farklı yöntem ve teknikler kullanılarak gerçekleştirilebilir. Hedef bir web sunucusu üzerinden sisteme sızmak için varolan portları kullanarak ya da yeni bir port açarak veri çıkışının sağlanması, sistem erişimi için yeni bir kullanıcı hesabının yaratılması ya da xss, sql

injection gibi açıklara sebep olabilecek kodların sisteme bulaştırılması arka kapı oluşturmak için yaygın kullanılan yöntemlerdir. (Kayar, Lostar, 2016)

Arka kapılar kendi kendilerini çoğaltma özellikleri olmaması sebebiyle genellikle virüsler, truva atları ve casus yazılımlar aracılığıyla yayılırlar. Sistem içerisine bulaşmış bir arkakapı kodu saldırganlara uzaktan donanımları kontrol etme, ayarları değiştirme, klavye tuş hareketlerini ve ekran görüntülerini kaydetme, hassas verileri erişim sağlama, bilgileri çalma gibi tehditlere imkân sağlar. (Kiguolis, 2016)

Klavye İzleyiciler (Keylogger)

Klavye izleme; kullanıcıların klavyeden dokunduğu tuşlar ile bilgisayar üzerinde yaptıkları işlemlerin casus yazılımlar ile kaydedilmesini sağlayan tehdit yöntemidir. Klavye izleyici programlar saldırganlar tarafından bilgisayar sistemlerine yüklenebileceği gibi e posta, mesaj, dosya indirme yoluyla kullanıcılar tarafından da bulaştırılabilir. Klavye izleyiciler bilgisayar üzerinden gerçekleştirilen sohbet ve mesajlaşmaları, yapılan işlemleri, web gezinti geçmişini, kamera ve mikrofon üzerinden ses ve görüntüleri kayıt altına alabilmektedir. Klavye izleyici programlar ebeveynler tarafından çocuklarının bilgisayar ve internet ortamındaki hareketlerinin takibi ve güvenliği için de kullanılabilmektedir. (Çağala, 2017)

Mesaj Sağanakları (Spam, Junkmail)

Mesaj sağanakları (spam, junkmail), kullanıcının isteği dışında ticari reklam, tanıtım, siyasi bir görüşün propagandasını yapmak ya da bir sistemin çalışmasını engellemek amacıyla gönderilen toplu mesaj ya da e postalardır. (DEBİS, 2019)

Reklam Görünümlü Yazılımlar (Adware)

Reklam görünümlü yazılımlar (Adware), bilgisayarda ve web ortamında kullanıcıdan izin almaksızın ya da bildirimde bulunmaksızın arama kayıtlarını, ziyaret edilen web sayfalarına yönelik alışkanlıkları ve davranışları kullanarak pazarlama ve ticari maksatla kullanıcıları farklı web sitelerine yönlendirmek için hazırlanmış programlardır. Reklam görünümlü yazılımlar genellikle truva atı ya da casus yazılım özellikleri taşıyan programlarla karşımıza çıkmaktadır. Kullanıcının iznini alarak bildirimlerde bulunan reklam yazılımları kötü amaçlı yazılım olarak kabul edilmemektedir. Reklam görünümlü yazılımların en çok bulunduğu kaynaklar ise çevrimiçi oyun siteleri, ücretsiz dosya/uygulama indirme ortamları (crack site) ve şiddet, pornografi ya da virüs barındıran web sayfalarıdır. (Kaspersky, 2019)

5.6.4. **Oltalama/Kimlik Avı (Phishing)**

Oltalama (Phishing) kullanıcı hesaplarına bilinen bir web sitesi, banka, internet servis sağlayıcı ya da resmi bir kurumdan gönderilmiş gibi görünen e posta ve mesajları kullanarak kredi kartı bilgileri, şifre gibi kişisel verileri ele geçirmek amacıyla yapılan çevrimiçi bir saldırı türüdür. Bu e posta ya da mesajların içerisinde genellikle sahte ya da değiştirilmiş bir web sitesine yönlendiren URL bağlantısı bulunur. URL bağlantısıyla erişilen web siteleri e posta hizmeti veren servisler, çevrimiçi oyunlar, bankalar, sosyal paylaşım siteleri vb. görünümünde hazırlanmış, kullanıcının kişisel bilgilerini girmesini, şifrelerini güncellemesini, bir bağlantıya tıklamasını, bir dökümanı açmasını ya da bir yazılımı kurmasını isteyen, uygulamalar ve yönlendirmeler içerir. Oltalama (Phishing) dolandırıcılığı için mesaj ya da e postayı alan kişiyi inandırmak amaçlı bu yöntem

dışında telefon görüşmeleri, yarışmalar ya da sosyal medya araçları da yaygın biçimde kullanılmaktadır. (AKÜ, 2018)

5.6.5. **Zombi Makineler/Botnet (Botnets)**

Günümüzde siber saldırganların sıklıkla kullandığı saldırı türlerinden birisi de Botnet'lerdir. Botnet saldırısı temel olarak herhangi bir ağ sistemi üzerinde bulunan bilgisayar ya da cihazın, saldırganlar tarafından yazılımlar aracılığıyla suç işlemek ve kötü amaçlar doğrultusunda kullanılmak üzere kontrol altına alınmasıdır. Saldırganlar tarafından kontrol altına alınan bot (robot) ya da zombie olarak tanımlanan, internete bağlı bilgisayarlar, cihazlar ve dolayısıyla kullanıcılar, farkında olmaksızın siber suçların işlendiği bir ordunun parçası haline gelmektedir. (Turkhackteam, 2018)

Genellikle açık bırakılan portlar ve güvenlik duvarlarındaki zaafiyetler nedeniyle sistemlere truva atı benzeri kötücül yazılımların bulaştırılması sonucu kontrol altına alınarak Botnet'e dönüştürülen bilgisayarlar ve cihazlar, veri hırsızlığı, casusluk, web siteleri üzerinden pop-uplar ile başka bir sitenin reklamını yapmak, e postalarda spam mailler oluşturmak gibi kişisel kullanıcıları hedef alan görece basit saldırılarda ya da DDoS saldırıları ile ağ sistemlerine zarar verme, hizmet dışı bırakma şeklinde küresel çapta zarara yol açabilecek siber suçların gerçekleştirilmesinde kullanılmaktadırlar. (Korolov, 2019)

Botnet saldırılarının küresel çapta oluşturduğu tehditlerin boyutunun anlaşılabilmesi için 2016 yılında siber korsanlar tarafından yapılan Mirai Botnet saldırısı örnek verilebilir. Mirai adındaki zararlı yazılım kullanılarak yapılan

siber saldırı, medya ve eğlence sektöründe hizmet veren aralarında Twitter, Spotify, HBQ, Netflix'in de bulunduğu büyük internet sitelerine alan adı sağlayıcılığı yapan DYN'i hedef almıştır. bulunduğu birçok şirketi etkileyen saldırı internete bağlı nesnelerin (kameralar, yazıcılar) kullanılmasıyla DDoS (Distruption of Service) saldırılarında yeni bir boyuta ulaşmıştır. (Mirai, 2016)

5.6.6. **Dağıtılmış Ağ Saldırıları (Distributed Denial Of Service (Ddos))**

Kurum ya da kuruluşların web sitesi, e-posta sistemi, online ödeme sistemi gibi internet üzerinden verdikleri hizmetlerin ve uygulamaların karşılaştığı diğer bir güvenlik tehditi de DDoS (Distributed Denial of Service – Dağıtık Servis Dışı Bırakma) saldırılarıdır. DDoS saldırıları, bir web sitesi kaynağı, ağ sunucusu ya da diğer altyapılardaki belirli bir hedefe yönelik, kullanıcıların bilgisi dışında uzaktan yönetilen köle bilgisayarlar (zombi, bot) aracılığıyla, hedef alınan sistem üzerinde aşırı trafik yaratarak sistemi erişilemez ya da işlevsiz duruma getirmek amacıyla yapılır. DDoS saldırılarında temel motivasyon ağ sistemlerine sızma ya da bilgi hırsızlığı değildir. DDoS saldırıları genellikle TCP/IP protokolü kullanan web siteleri ve uygulamalarının bulunduğu ağ sistemlerine yönelik gerçekleştirilmektedir. Web sitelerinin yazılımsal tabandaki karmaşık yapıları ve uygulama sunucularının proxyler, veritabanları gibi çok sayıda sistemle birlikte çalışıyor olmaları saldırı hedefi olarak seçilebilecek alanları genişletmektedir. Çoklu sistemsel yapı ve protokol katmanları, web sitelerinin ya da uygulamaların düşük yoğunluklu saldırı paketleriyle bile performans sorunları yaşamalarına neden olmakta ve sistemi DDoS saldırılarına açık hale getirmektedir. (Çevik, 2019)

5.6.7. **Fidye Yazılımları (Ransomware)**

Fidye yazılımlar, ağ sistemleri, bilgisayarlar ve mobil cihazlarda bulunan verilerin siber saldırganlar tarafından ele geçirilerek şifrelenmesi/kilitlenmesi ve bu verilere yeniden erişim sağlanabilmesi için fidye ödenmesini talep ettikleri kötü niyetli ve zararlı yazılımlardır. Saldırganlar reklam, e posta, mesaj ya da sosyal mühendislik gibi farklı yöntemlerle sistemlere erişim sağlayarak kullanıcılara ait veri, bilgi kaynaklarını karmaşık algoritmalar ile şifrelemekte, bu şifre algoritmalarını çözebilecek özel anahtarları da farklı sunucular içerisinde saklamaktadırlar. Saldırganlar tarafından gönderilen, kullanıcıların saldırıdan etkilenen veri, bilgi kaynaklarına tekrar erişim sağlayabilmeleri için belirlenen bir süre içerisinde ve şekilde (Ucash, Bitcoin, Moneypack vb.) ödeme yapması gerektiğini gösteren uyarı mesajları da fidye saldırılarının bilinen özelliklerindendir. (Çelik & Çeliktaş, 2018)

Son yıllarda gerçekleşen fidye yazılımı saldırılarında kullanılan yöntemlerin çeşitliliği ve hacmi, siber saldırganların motivasyonlarını artırmış ve dolayısıyla saldırıların şiddet alanını da genişletmiştir. Medya ve e ticaret şirketleri, finansal aktörler, kamu kurum kuruluşları, endüstriyel altyapılar ve kişisel web kullanıcıları saldırganların hedefi haline gelmiştir. Hem kişisel kullanıcıların ev ortamında hem de kurum ve kuruluşların iş süreçlerinin yürütülmesinde büyük rol oynayan internete bağlanabilen cihazların (IoT) ve mobil teknolojilerin yaygınlaşmasıyla birlikte bu cihazlar üzerindeki yazılımsal zaafiyetler ve güvenlik açıkları saldırganların sistemleri ele geçirmelerini kolaylaştırmıştır.

Siber güvenlik firmalarının yaptığı araştırma sonuçları fidye yazılımlarının 2018 yılında bütün siber tehdit kategorileri içerisinde en fazla sayıda gerçekleştirilen ve en çok zarar

yaşanmasına sebep olan saldırı türü olduğunu göstermektedir. Güvenlik uzmanlarının tespitlerine yansıdığı şekliyle 2017 yılında başlayan uluslararası ölçekteki fidye yazılımı saldırılarındaki artış eğilimi global şirketlerin ve kişisel kullanıcıların milyarlarca dolarlık maddi kayıp yaşamasına sebep olmuştur. Cyber Security Ventures tarafından yapılan analizlere göre 2019 yılında her 14 sn'de bir fidye yazılımı saldırısı gerçekleşmesi ve maddi olarak 11,5 milyar dolarlık bir zararın oluşması öngörülüyor. 2017 yılında yaşanan 100'ün üzerinde ülkenin doğrudan etkilendiği, 4 milyar dolar zarara yol açan tüm zamanların en büyük siber saldırılarından birisi olan "WannaCry" ve 2018 yılında 150 milyon kişiye ait verilerin çalınmasıyla sonuçlanan "MyFitnessPal" fidye yazılım saldırıları sonuçları itibariyle bu öngörüleri doğrular nitelikte veriler içermektedir. (Morgan, 2018).

5.6.8. **Silici/Yokedici Zararlı Yazılımlar (Wiper Attacks)**

Silici/yokedici yazılımlar, (Wiper Attack) hedef aldıkları sistem üzerindeki bütün verileri silmek, imha etmek amacıyla tasarlanmış çok tehlikeli bir yazılım türüdür. Tespit edilmesi oldukça zor olan, genellikle politik motivasyona sahip siber saldırganlar tarafından, finansal çıkar sağlamak için kritik altyapılar, endüstriyel tesisler ya da devletlere ait kurumları hedef alan silici/yokedici yazılımlar, sonuçları itibariyle oldukça geniş bir alanda yıkıcı etkilere sahiptir (Lawyer, 2018). Silici/yokedici yazılımlar tarafından saldırıya uğrayan bir yapı içerisindeki veritabanları, sistemsel, finansal, kişisel bütün veriler, dosyalar kalıcı biçimde yokedilme tehlikesiyle karşı karşıyadır. Silici/yokedici saldırıları korkutucu yapan diğer bir özelliği ise bu saldırıların ardından saldırıda kullanılan program ya da dosyaların da silinerek yok olması ve geriye saldırıyla ilgili hiçbir iz bırakılmamasıdır (Robinson, 2015).

Bugüne kadar karşılaşılan silici/yokedici saldırılar ağırlıklı olarak Ortadoğu ve Asya'da bulunan ülkelere ait kritik altyapıları, nükleer tesisleri ya da şirketleri hedef almıştır. 2012 yılında İran'a ait petrol ve enerji tesislerini hedef alan ve Wiper adı verilen saldırı silici/yokedici saldırıların benzersiz bir örneği olarak kabul edilmektedir. Narilam, Groovemonitor, Shamoon, Dark Seul, Black Energy, ExPetr/Not Petya ve Olympic Destroyer uluslararası çaptaki silici/yokedici tür saldırıların diğer önemli örnekleri olarak gösterilebilir. (Raiu, 2013)

5.6.9. **Ortadaki Adam Saldırısı (Man In The Middle (MITM))**

Ortadaki adam saldırıları, (MITM) herhangi bir ağ yapısı ya da internet üzerinden iletişimde bulunan iki farklı bilgisayar ya da cihazın aralarına giren saldırganın giden gelen veri trafiğini kendisine yönlendirerek güvenlik zaafiyeti yaratması temeline dayanan saldırı türüdür. Kullanıcılara ait veriler iletişim kanalı olarak kullanılan sunucular üzerinden değil öncelikle saldırgana ait bilgisayara/cihaza giderek hedefine yönlendirilir. Bu tür saldırılar teknik olarak yerel ağlara bağlı olarak çalışan bilgisayar ve cihazların MAC adreslerinin birbirleriyle haberleşmesi için kullanılan adres çözümleme protokolünün (ARP) açıklarından yararlanılarak yapılır. Network ya da Wi-Fi ağına bağlanan saldırgan gerçekleştirdiği ARP atakları ile kendisini hedef kullanıcıların ağ üzerindeki çıkış izinlerinin verildiği ağ geçidi (Gateway) olarak belirler. Bu saldırı sonucu hedef bilgisayar/cihazlar ağ geçidi olarak saldırgana ait bilgisayar/cihazı kullanmaya başlar. Kullanıcılar saldırgan üzerinden kurulan iletişimin farkına varmadan ağ bağlantılarını ya da normal çalışmalarını devam ettirirler. Ortadaki adam saldırıları ile yönlendirilmiş bir sistem üzerindeki bütün trafik saldırgan tarafından izlenir, kontrol edilir, yönlendirilir. Hedef kullanıcıların ağ/internet üzerinde paylaştıkları herşey saldırgana açık hale gelir. (Özdemiroğlu, 2018)

5.6.10. **Otomatik Olarak Yüklenen Zararlılar (Drive By Downloads)**

Saldırganlar tarafından web sitelerine enjekte edilen zararlı kodların, web sitesine erişim sağlandığı anda kullanıcının herhangi bir bilgisi ya da onayı olmaksızın kendiliğinden otomatik olarak çalışması mantığına dayanan drive by downloads saldırıları bilgi güvenliğine yönelik yaygın tehditlerden bir diğeridir. Drive by downloads saldırılarında web sayfalarının içerisine otomatik çalışan kötü amaçlı nesneler ya da zararlı kodlar yerleştirilerek, genellikle meşru olan bir web sitesi tehlikeli hale getirilmektedir. Bu zararlı nesneler, kötü amaçlı JavaScript kodu enjeksiyonlarından, reklamlara, siteler arası komut dosyası çalıştırma saldırılarından (XSS), yönlendirme tuzaklarına ya da kullanıcıların kendilerinin tespit edemeyeceği diğer farklı saldırı tekniklerine kadar uzanabilir. Bir kullanıcı saldırganlar tarafından zararlı kod eklenmiş bir web sitesini ziyaret ettiğinde, herhangi bir tıklamada bile bulunmasına gerek kalmadan tarayıcı otomatik olarak kötü niyetli kodu yükleyerek kullanıcının işletim sistemindeki ve diğer kullandığı uygulamalardaki güvenlik açıklarının tespit edilmesini sağlar. (Laing, 2017)

5.6.11. **Antivirüs Olarak Görünen Yazılımlar (Scareware, Rogue Software)**

Rogue - Scareware, bilgisayar kullanıcılarını sistemlerinde virüs varmış gibi kandırarak antivirüs, antimalware yazılımı almak için ödeme yapmaya ya da kötü amaçlı yazılım bulaşmış web sitelerini ziyaret etmeye zorlayan yazılımlardır. İnternet ortamında saldırganlar tarafından hazırlanmış Rogue - Scareware içeren bir web sitesinin ziyaret edilmesiyle aktifleşen zararlı kodlar nedeniyle kullanıcının bilgisayarında pop-uplar ve virüs uyarıları gelmeye başlar. Kullanıcıyı sisteminde virüs olduğuna inandırıp, korkutarak bu virüsleri temizlemesi için sahte bir antivirüs, antimalware yazılımını

yüklemeye ikna ettikten sonra ödeme yaptırtmak ya da farklı türlerde zararlı yazılımların sisteme bulaştırılması şeklinde uygulanmaktadır. (Kaspersky, 2018)

5.6.12. **Fikri Mülkiyet Hırsızlığı (Intellectual Property Theft)**

Fikri Mülkiyet Hırsızlığı/Korsanlığı, kurum, kuruluş, şirket ya da devletlere ait ticari/mesleki sırlardan film, müzik, yazılım, tasarım, edebi eser gibi insan aklının üretimi ürünlere kadar, fikir ya da buluş kapsamındaki her şeyin kötü niyetli kişiler tarafından izinsiz olarak ele geçirilmesidir. Devlete ait savunma sanayi ile ilgili yeni bir projenin şeması, sağlık sektöründe bir firmanın geliştirdiği bir ilaç, genetik alanda yürütülen bir çalışma, yapımcı bir şirketin çektiği dizi, film ya da herhangi bir prodüksiyon veya bir yazarın yayımlanmamış romanı fikri mülkiyet kapsamında değerlendirilebilir. (FBI, 2019)

Özellikle dijital teknolojilerin ve İnternet dosya paylaşım ağlarının yükselişiyle birlikte büyüyen bir tehdit haline gelen Fikri Mülkiyet Hırsızlığı/Korsanlığı genel olarak ticari/mesleki sırlar ve telif haklarına yönelik gerçekleştirilsede, son yıllarda medya ve eğlence sektöründe meydana gelen uluslararası şirketlerde büyük ölçekli maddi zarara yolaçan farklı saldırılarla adından söz ettirmektedir (Özcan, 2018). 2014 yılında yapımcı Sony Pictures'ın yeni filmi "The Interview" vizyona girmeden Kuzey Kore'li siber saldırganlar tarafından ele geçirilmesi, 2017 yılında ABD'li TV kanalı ve yayıncı HBO'yu hackleyen Mr. Smith adlı hacker grubunun çevrimiçi yayın kuruluşu Netflix dizisi Game of Thrones'un senaryolarını, oyuncuların kişisel telefon numaralarını, e-posta adreslerini yayınlaması Fikri Mülkiyet Hırsızlığı/Korsanlığı saldırılarının yakın zamanlı örnekleridir.

5.6.13. **Sosyal Mühendislik (Social Engineering)**

Sosyal mühendislik, teknoloji kullanımından bağımsız olarak insan etkileşimleri yoluyla gerçekleştirilen, kullanıcıları iletişim, duygu, düşünce tarzı, bilişsel/fiziksel zaafiyetlerinden yararlanarak güvenlik hataları yapma veya hassas bilgiler verme konusunda kandırmak için psikolojik manipülasyon uygulama yöntemidir. Bilgi güvenliği çerçevesinde diğer teknolojik tehditlerle eşdeğer önemde bir tehdit çeşidi olan ve temel amaç olarak herhangi bir sisteme giriş sağlayabilmek için insan odaklı, teknik olmayan yöntemlerin kullanıldığı sosyal mühendislik saldırıları, birbirini sistemli bir şekilde takip eden farklı adımlarla gerçekleştirilir. (Incapsula, 2019)

Sosyal mühendislik saldırılarının birinci aşaması sistem giriş noktalarının ve zayıf güvenlik protokollerinin tespit edilmesi için hedef yapıya çalışan personel olarak sızmak, teknik destek veriyormuş gibi iletişime geçmek, çalışanlarla arkadaşlık kurmak gibi yöntemlerle saldırı yapılacak sistem etrafındaki her türlü bilginin toplanmasıdır. Bilgi toplanmasının ardından analiz edilen bilgilerle mağdurun güvenini kazanmak, kritik kaynaklara erişim sağlamak gibi güvenlik uygulamalarını kıran diğer eylemleri için çeşitli uyaranları sağlar. Analiz edilen bilgilerle birlikte saldırgana sistem üzerindeki iletişim kanalları bildirilir. İletişim kanalları üzerinden ikna etme, kandırma vb. gibi çeşitli aldatma yöntemleriyle saldırı atağı gerçekleştirilir ve son olarak da geride bir iz bırakmamak için saldırı ile ilgili tüm kanıtlar yokedilir (Parsons, 2010).

VI. BİLGİ GÜVENLİĞİ FARKINDALIĞI ANALİZİ

6.1. **Yöntem**

Bu bölümünde araştırmanın amaçları ve kapsamı, modeli, veri toplamada kullanılan araçların yapısı, istatiksel yöntem ve teknikler ile araştırmaya ait hipotezlerle ilgli ayrıntılı değerlendirme yapılmıştır.

6.2. **Amaç Ve Kapsam**

Araştırmanın asıl amacı İnternet kullanıcılarının kişisel bilgi güvenliği farkındalığının göstergeleri olarak, riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı olgularının ölçümlenip aralarındaki ilişkilerin ortaya koyulmasıdır. Araştırmada asıl amaca ek olarak internet kullanıcılarının demografik özelliklerine bağlı riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı olguları bakımından farklarının incelenmesi de kapsam dâhilinde tutulmuştur.

6.3. **Veri Toplama Araçları**

Bilgi ve iletişim teknolojilerinin kullanımı ile ilgili davranışlara ve bilgi güvenliği farkındalığına yönelik yapılan bu çalışma kapsamında farklı yaş, cinsiyet ve eğitim seviyesinde 200 kişiden oluşan bir örneklem grubundan yararlanılmıştır.

Araştırmada veri toplanması kapsamında yüzyüze görüşme yöntemi ve anket uygulaması benimsenmiştir. Başkent Üniversitesi, Ticari Bilimler Fakültesi, İstatistik ve Bilgisayar Bilimleri Anabilim Dalı, Yönetim Bilişim Sistemleri Bölümü Öğretim

Görevlisi Gizem Öğütçü tarafından geliştirilen anket formu 5 kısımdan oluşmaktadır. Araştırma kapsamında 20 adet 5'li likert tipte toplamda 80 sorudan oluşan 4 ayrı kategori ölçekten ve katılımcıların demografik ve tanımlayıcı özelliklerine dair istatistiklerin toplanabilmesi amacıyla 7 adet kategorik sorudan oluşan kişisel bilgi formu uygulanmıştır.

6.3.1. **Riskli Davranışlar Ölçeği**

Riskli davranışlar ölçeği katılımcıların internet kullanımı sırasında bulundukları riskli davranışların düzeyini ölçmek üzere tasarlanmış, toplamsal bir ölçektir.

Tablo 6.1 Riskli Davranışlar Ölçeği

	Hiçbir Zaman	Nadiren	Bazen	Sık Sık	Her Zaman
Msn Messenger, GTalk, Skype ve benzeri sohbet programlarını kullanırım					
Bir iletişim aracı olarak elektronik posta (e-mail) kullanırım.					
Kurumsal e-posta adresimi günlük işlerde de kullanırım					
İnternette e-posta gruplarına üye olurum					
Facebook, Twitter ve benzeri sosyal ağ sitelerini kullanırım					
Sosyal ağlarda gönderilen uygulama davetlerini kabul ederim					
İnternet bankacılığı kullanırım.					
İnternet üzerinden alışveriş yaparım.					
E-Vatandaşlık hizmetleri veren web sayfalarını (TC kimlik no sorgulama, sosyal güvenlik primi sorgulama vb.) kullanırım					
İnternet üzerinden oyun oynarım					
İnternet üzerinden müzik, film, program ve dosya indiririm/kaydederim					
İnternet üzerinden video/film izlerim.					
İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM No, e-posta, Adres) paylaşırım.					
İnternet ortamında gerektiği durumlarda özlük bilgilerimi paylaşırım. (Ad, Soyad, Doğum Tarihi vb…)					
Sohbet (chat) yaparken dosya transferi yaparım					
Bilgisayarımdaki dosyaları paylaşıma açarım.					
Halka açık internet erişimi olan yerlerde internet bankacılığı kullanırım					
Parolalarımı başkalarıyla paylaşırım.					
Parolalarımı yazılı olarak kolay ulaşabileceğim yerlerde saklarım.					
Tanımadığım kişilerden gelen e postaları açarım, gelen ekleri indiririm.					

6.3.2. **Korumacı Davranışlar Ölçeği**

Korumacı davranışlar ölçeği katılımcıların internet kullanımı sırasında bulundukları korumacı davranışların düzeyini ölçmek üzere tasarlanmış, toplamsal bir ölçektir.

Tablo VI.2 Korumacı Davranışlar Ölçeği

	Hiçbir Zaman	Nadiren	Bazen	Sık Sık	Her Zaman
Birden fazla elektronik posta adresi kullanırım.					
Bilgisayarımda orijinal (lisanslı) yazılım kullanmaya dikkat ederim					
Virüs temizleme, casus yazılım önleme vb. programları kullanırım.					
Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.					
İçerik filtreleme programları kullanırım					
E-posta filtreleme yazılımları kullanırım.					
İzleme yazılımları kullanarak internet üzerinde yapılan etkinlikler hakkında bilgi sahibi olurum.					
Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.					
Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve Web gezinti geçmişlerini silerim.					
Dosyalarımı şifrelerim					
İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım					
Elektronik/ Mobil imza kullanırım.					
İnternet sitelerine girerken genellikle sık kullanılanlar listesini kullanırım					
Bilgisayarım şifre ile açılır					
Bilgisayarımda otomatik kullan özelliğini kapatırım					
Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim					
Parolalarımı sık sık değiştiririm.					
Kablosuz modem şifremi değiştiririm					
Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım					
Kullandığım programların güncellemelerini düzenli olarak yaparım.					

6.3.3. **Suça Maruziyet Ölçeği**

Suça maruziyet ölçeği katılımcıların internet kullanımı sırasında bulundukları suça maruziyet düzeyini ölçmek üzere tasarlanmış, toplamsal bir ölçektir.

Tablo 6.3 Suça Maruziyet Ölçeği

	Hiçbir Zaman	**Nadiren**	**Bazen**	**Sık Sık**	**Her Zaman**
Msn Messenger, GTalk, Skype ve benzeri sohbet programlarını kullanırım					
Bilgisayar virüsleri nedeniyle sorun yaşadım.					
Online alışverişten dolayı maddi zarara uğradım.					
Kredi kartım kopyalandı					
Kişisel bilgilerimi internette paylaştığım için sıkıntı yaşadım					
Elektronik bankacılık kullandığım için maddi zarara uğradım.					
Kişisel bilgilerim iznim olmadan üçüncü şahıslarla paylaşıldı/ internette yayınlandı.					
İnternet üzerindeki hesaplarıma ait kullanıcı adım ve şifrem ele geçirildi					
İnternette kimliği belirsiz kişiler tarafından şahsıma yönelik hakaret, tehdit, ahlaksız teklif aldım.					
Kumar içerikli siteler nedeniyle zarara uğradım					
Sosyal ağ siteleri nedeniyle zarara uğradım.					
Arkadaşlık siteleri nedeniyle zarara uğradım.					
İnternette gezerken isteğim dışında şiddet ya da pornografik içerikli yayınlarla karşılaştım.					
Bilgisayarımdaki dosyalarım çalındı/silindi.					
Adıma sahte hesaplar açıldı.					

6.3.4. **Tehlike Algısı Ölçeği**

Tehlike algısı ölçeği katılımcıların internet kullanımı sırasında algıladığı tehlikelerin düzeyini ölçmek üzere tasarlanmış, toplamsal bir ölçektir.

Tablo 6.4 Tehlike Algısı Ölçeği

	Hiçbir Zaman	**Nadiren**	**Bazen**	**Sık Sık**	**Her Zaman**
Bilgisayar virüsleri nedeniyle sorun yaşadım.					
Online alışverişten dolayı maddi zarara uğradım.					
Kredi kartım kopyalandı					
Kişisel bilgilerimi internette paylaştığım için sıkıntı yaşadım					
Elektronik bankacılık kullandığım için maddi zarara uğradım.					
Kişisel bilgilerim iznim olmadan üçüncü şahıslarla paylaşıldı/ internette yayınlandı.					
İnternet üzerindeki hesaplarıma ait kullanıcı adım ve şifrem ele geçirildi					
İnternette kimliği belirsiz kişiler tarafından şahsıma yönelik hakaret, tehdit, ahlaksız teklif aldım.					
Kumar içerikli siteler nedeniyle zarara uğradım					
Sosyal ağ siteleri nedeniyle zarara uğradım.					
Arkadaşlık siteleri nedeniyle zarara uğradım.					
İnternette gezerken isteğim dışında şiddet ya da pornografik içerikli yayınlarla karşılaştım.					
Bilgisayarımdaki dosyalarım çalındı/silindi.					
Adıma sahte hesaplar açıldı.					
İnternet üzerinden yaptığım yazışmalar isteğim ve bilgim dışında başkaları tarafından izlendi, kaydedildi.					
Halka açık internet erişimi olan yerlerde internet bankacılığı kullanırım					
Parolalarımı başkalarıyla paylaşırım.					
Parolalarımı yazılı olarak kolay ulaşabileceğim yerlerde saklarım.					
Tanımadığım kişilerden gelen e postaları açarım, gelen ekleri indiririm.					

6.3.5. **Kişisel Bilgi Formu**

Kişisel bilgi formu katılımcıların demografik ve tanımlayıcı özelliklerine dair istatistiklerin toplanabilmesi amacıyla oluşturulmuş 7 adet kategorik sorudan oluşan kısımdır.

Şekil 6.1 Kişisel Bilgi Formu

Yaşınız:.....
Cinsiyetiniz: Kadın [ ] Erkek [ ]
Yaşadığınız Şehir: .....
Eğitim Düzeyiniz: İlköğretim mezunu [ ]
Lise mezunu [ ]
Onlisans / Lisans mezunu [ ]
Y.Lisans mezunu [ ]
Doktora mezunu [ ]

Unvanınız: .....

Çalıştığınız Birim/Bölüm:
.....

İşyeriniz dışındaki internet erişim şekliniz nedir? (Birden fazla şık işaretleyebilirsiniz.)

Kablolu modem ile bağlantı [ ]
Kablosuz modem ile bağlantı [ ]
Cep telefonu aracılığı ile bağlantı [ ]
İnternet kafeden bağlantı [ ]
Erişimim yok [ ]

Bilgisayar güvenliği / internet güvenliğine yönelik eğitim aldınız mı veya iş deneyiminiz oldu mu?
Evet [ ] Hayır [ ]

Ortalama kaç yıldır internet kullanıyorsunuz? .....yıl

Ortalama internet kullanım sıklığınız:
Günde ..... Saat
Haftada ..... Gün
Diğer .....

6.4. **Araştırma Hipotezleri**

Araştırma amaçları doğrultusunda oluşturulan araştırma hipotezleri şu şekildedir;

H1: İnternet kullanıcılarında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri arasında ilişki vardır.

H2: Kadın ve erkek internet kullanıcıları arasında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri bakımından fark vardır.

H3: Farklı yaş grubundaki internet kullanıcıları arasında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri bakımından fark vardır.

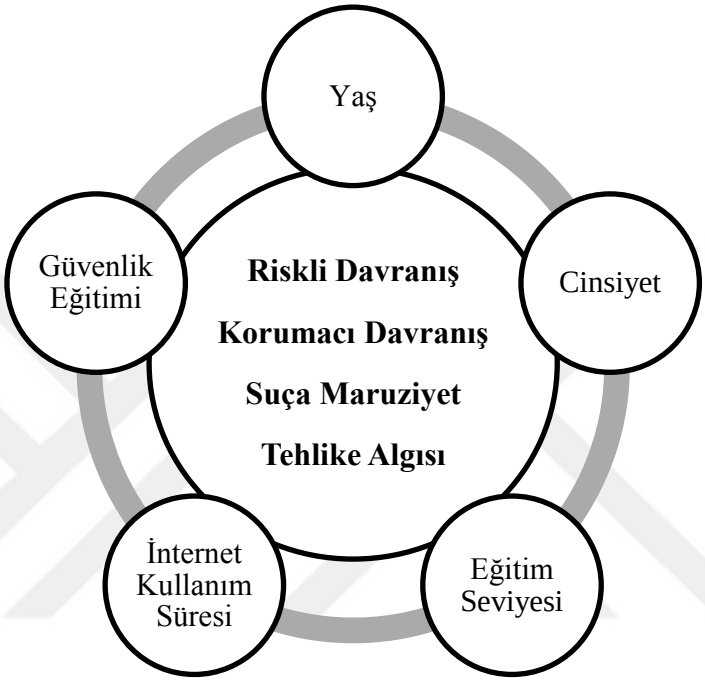
H4: Farkı eğitim seviyesindeki internet kullanıcıları arasında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri bakımından fark vardır.

H5: Farklı sürelerdir internet kullanan internet kullanıcıları arasında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri bakımından fark vardır.

H6: Güvenlik eğitimi alan ve almayan internet kullanıcıları arasında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri bakımından fark vardır.

6.5. **Araştırma Modeli**

Tarama modeli ile gerçekleştirilen araştırmaya ait hipotez ve amaçlarla oluşturulan araştırma modeli Şekil 6.2'deki gibi görselleştirilebilir.



Şekil 6.2 Araştırma Modeli

6.6. **Veri Analizi**

Araştırma kapsamında toplanan veriler Microsoft Excel programına girilmiş, ardından gerekli kodlamalar yapılarak IBM SPSS 23.0 versiyonuna aktarılmıştır. Bulgular bölümünün ilk kısmında araştırma katılımcılarına ait demografik ve tanımlayıcı istatistikler tablo ve yorumlar ile birlikte paylaşılmıştır. İkinci kısımda ölçek sorularına verilen cevapların frekans dağılımları ile ortalama ve standart sapma değerleri hesaplanıp tablolanmıştır. Üçüncü kısımda araştırmanın ölçme araçları olan ölçek betimsel istatistikleri ve normal dağılım testleri sunulmuştur. Ölçeklerin normal dağılıma uymadığı görüldüğünden sonraki bölümdeki testlerde parametrik olmayan

sınamalar kullanılmıştır. İki farklı sayısal ölçüm arasında doğrusal bir ilişki olup olmadığını, varsa bu ilişkinin detaylı sonuçlarını belirleyebilmek için istatiksel korelasyondan faydalanılmıştır. Ölçeklerden elde edilen verilerin normal dağılıma sahip olmaması nedeniyle çalışmada Sperman Korelasyonu kullanılmıştır.

Sperman Korelasyonunda farklı değişkenler arasındaki **ilişkinin gücü r değeri istatiksel anlamlılık düzeyi ise p değeri** ile gösterilir. Değişkenler arasındaki ilişki gücünü gösteren r değeri (korelasyon katsayısı) -1 ile +1 arasında değerler alabilir. R değerinin pozitif olması karşılaştırılan değişkenler arasında doğrusal bir ilişkiyi, negatif olması ise ters yönlü bir ilişkinin olduğunu kanıtlar. R değeri +1'e yaklaştıkça korelasyon şiddeti de artar. P değeri herhangi bir karşılaştırmada ortaya çıkan istatiksel anlamlı fark vardır sonucunun olası hata miktarını ortaya koyar. P değerinin 0,05'in altında bulunması karşılaştırmada anlamlı farklılık olduğununu gösterir. P değeri küçüldükçe istatiksel olarak anlamlı fark düzeyi yükselir. (Kul, 2019)

Gruplar arasındaki farklılıkların irdelenmesine dayalı hipotez testlerinin sınamasında ise Mann Whitney U (MWU) ve Kruskall Wallis H (KWH) testinden faydalanılmıştır. Gruplar arası farklılık incelemesini içeren araştırma sorularında ise iki grup arası farklar MWU testi, ikiden fazla grup arasındaki farklar ise KWH testi ile incelenmiştir. MWU testi sonucu gruplar arasında anlamlı farklılık bulgulanması halinde grupların sıra ortalamaları karşılaştırılarak yorumlanmıştır. Diğer yandan KWH testi sonucu anlamlı farklılık bulgulanması durumunda ise farklılığın kaynağı olan grup veya grupların tespiti amacıyla her grup birbiri ile MWU testi ile karşılaştırılmıştır.

6.7. **Bulgular**

Araştırmanın bu kısmında anket verilerinin analizi ile ortaya çıkan sonuçlar istatiksel tablolara göre yorumlanarak sunulmuştur.

6.7.1. **Tanımlayıcı Bulgular**

Tablo 6.5 Tanımlayıcı İstatistikler

Özellik	Kategori	Frekans (n)	Yüzde (%)
Cinsiyet	Kadın	106	53.3%
	Erkek	94	46.7%
	Toplam	200	100.0%
Yaş Grubu	20-30	39	19.6%
	31-40	79	39.2%
	41-50	65	32.7%
	>51	17	8.5%
	Toplam	200	100.0%
Eğitim	İlköğretim	18	9.0%
	Lise	25	12.6%
	Önlisans/Lisans	94	46.7%
	Y.Lisans	41	20.6%
	Doktora	22	11.1%
	Toplam	200	100.0%

Tablo 6.6 İnternet Kullanım Süresi

Özellik	Kategori	Frekans (n)	Yüzde (%)
İnternet Kullanım Süresi	1-10 Yıl	64	32.2%
	11-20 Yıl	76	37.7%
	21 Yıl ve Üzeri	60	30.2%
Günlük İnternet Kullanım Süresi	1-2 Saat	53	26.6%
	3-4 Saat	73	36.2%
	5 Saat ve Üzeri	74	37.2%

Tablo 6.7 İnternet Erişim Şekli

İnternet Erişim Şekli	Frekans (n)	Yüzde (%)
Kablolu Modem	39	19.60%
Kablosuz Modem	167	83.92%
Cep Telefonu	196	98.49%

Tablo 6.8 Bilgi Güvenliği ile İlgili Eğitim Alma Durumu

Özellik	Kategori	Frekans (n)	Yüzde (%)
Güvenlik Eğitimi	Evet	52	26.1%
	Hayır	148	73.9%
	Toplam	200	100.0%

Tablo 6.9 Ölçek Betimsel İstatistikleri

Değişken	N	Minimum	Maksimum	Ortalama	Std. Sapma
Riskli Davranışlar	200	1.20	4.00	2.57	0.53
Korumacı Davranışlar	200	1.20	4.65	2.74	0.67
Suça Maruziyet	200	1.00	2.73	1.31	0.30
Tehlike Algısı	200	1.46	4.50	3.02	0.50

6.8. **Hipotezlerin İstatiksel Sonuçları**

H1: İnternet kullanıcılarında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri arasında ilişki vardır.

Hipotezin sınanması amacıyla riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı ölçekleri arasında yapılan spearman korelasyon analizi bulguları Tablo 6.10'daki gibidir.

Tablo 6.10 Spearman Korelasyon Matrisi

Değişken	İstatistik	1	2	3	4
1.Riskli Davranışlar	r	1.000	,193	,394	-.101
	sig.		.006	.000	.156
	n	200	200	200	200
2.Korumacı Davranışlar	r		1.000	-.035	,201
	sig.			.620	.004
	n			200	200
3.Suça Maruziyet	r			1.000	-.090
	sig.				.207
	n				200
4.Tehlike Algısı	r				1.000
	sig.				
	n				

(r=0.193, sig.<0.05)

Riskli davranışlar düzeyi artıkça korumacı davranışlar düzeyi artmakta, riskli davranışlar düzeyi azaldıkça korumacı davranışlar düzeyi de azalmaktadır.

(r=0.394, sig.<0.01)

Riskli davranışlar düzeyi artıkça suça maruziyet düzeyi artmakta, riskli davranışlar düzeyi azaldıkça suça maruziyet düzeyi de azalmaktadır.

(r=-0.101, sig.>0.05).

Riskli davranış düzeyi ile tehlike algısının ilişkisiz olduğu görülmüştür.

(r=-0.035, sig>0.05).

Korumacı davranışlar düzeyi ile suça maruziyet düzeyinin ilişkisiz olduğu görülmüştür.

r=0.201, sig.<0.01).

Korumacı davranışlar düzeyi artıkça tehlike algısı artmaktada, korumacı davranışlar düzeyi azaldıkça tehlike algısı da azalmaktadır.

(r=-0.090, sig.>0.05).

Suça maruziyet düzeyi ile tehlike algısı arasında bir ilişki bulgulanamamıştır.

H2: Kadın ve erkek internet kullanıcıları arasında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri bakımından fark vardır.

Kadın ve erkek katılımcılar arasında farkları sınayan MWU testi istatistikleri Tablo 6.11'deki gibidir.

Tablo 6.11 Kadın ve Erkek İnternet Kullanıcıları (MWU) Test İstatistikleri

Değişken	Cinsiyet	N	Ortalama	Ortalama Sıra	z	sig.
Riskli Davranışlar	Kadın	106	2.587	101.802	-0.471	0.637
	Erkek	94	2.556	97.946		
Korumacı Davranışlar	Kadın	106	2.682	96.241	-0.984	0.325
	Erkek	94	2.811	104.285		
Suça Maruziyet	Kadın	106	1.318	97.778	-0.586	0.558
	Erkek	94	1.322	102.532		
Tehlike Algısı	Kadın	106	3.043	102.811	-0.736	0.462
	Erkek	94	2.997	96.796		

Riskli Davranışlar (z=-0.471, sig.>0.05), .Korumacı Davranışlar (z=-0.984, sig.>0.05), Suça Maruziyet (z=-0.586, sig.>0.05) ve Tehlike Algısı (z=-0.735, sig.>0.05) bakımından kadın ve erkek internet kullanıcıları arasında istatistiksel olarak bir fark saptanamamıştır.

H3: Farklı yaş grubundaki internet kullanıcıları arasında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri bakımından fark vardır.

Farklı yaş grubundaki katılımcıların arasındaki farkları sınayan KWH testi istatistikleri ve gruplar arasındaki MWU testi karşılaştırma bulguları Tablo 6.12'deki gibidir.

Tablo 6.12 Yaş Grupları (MWU) Test İstatistikleri

Değişken	Yaş Grubu	N	Ortalama	Ortalama Sıra	Ki-Kare	Sig.	Karşılaştırma
Riskli Davranışlar	20-30	39	2.910	137.974	44.125	0.000	1>2
	31-40	79	2.690	112.128			1>3
	41-50	65	2.355	75.000			1>4
	>51	17	2.097	52.824			2>3
Korumacı Davranışlar	20-30	39	2.773	103.090	2.257	0.521	--
	31-40	79	2.721	98.077			
	41-50	65	2.811	105.015			
	>51	17	2.513	82.559			
Suça Maruziyet	20-30	39	1.456	128.372	33.360	0.000	1>3
	31-40	79	1.371	114.417			1>4
	41-50	65	1.187	71.662			2>3
	>51	17	1.278	77.118			2>4
Tehlike Algısı	20-30	39	2.742	68.167	15.022	0.002	2>1
	31-40	79	3.078	105.801			3>1
	41-50	65	3.105	109.985			4>1
	>51	17	3.082	108.235			

Riskli davranışlar bakımından 20-30 yaş (O.S=137.974), 31-40 yaş (O.S=112.128), 41-50 yaş (O.S.=75.000) ve 51 yaş ve üzeri (O.S=52.824) internet kullanıcıları arasında istatistiksel olarak farklılıklar saptanmıştır. (Ki-Kare=44.125, sig.<0.05).

20 ile 30 yaş arasındaki internet kullanıcılarının riskli davranışlar düzeyi diğer tüm internet kullanıcılarından daha yüksek bulgulanmıştır. 31 ile 40 yaş arasındaki internet kullanıcıları ise 41 ile 50 yaş arasındaki ve 51 yaş ve üzeri internet kullanıcılarından daha yüksek düzeyde riskli davranışlara sahiptir.

Korumacı davranışlar bakımından farklı yaş gruplarından internet kullanıcıları arasında istatistiksel olarak bir fark saptanmamıştır. (Ki-Kare=2.257, sig.>0.05).

Suça maruziyet bakımından 20-30 yaş (O.S=128.372), 31-40 yaş (O.S=114.417), 41-50 yaş (O.S.=71.662) ve 51 yaş ve üzeri (O.S=77.118) internet kullanıcıları arasında istatistiksel olarak farklılıklar saptanmıştır. (Ki-Kare=33.360, sig.<0.05).

20 ile 30 yaş arasındaki katılımcılar ve 31 ile 40 yaş arasındaki katılımcıların suça maruziyet düzeyleri 41-50 yaş arasındaki katılımcılar ve 51 yaş ve üzeri katılımcılardan daha yüksektir.

Tehlike algısı bakımından 20-30 yaş (O.S=68.167), 31-40 yaş (O.S=105.801), 41-50 yaş (O.S.=109.985) ve 51 yaş ve üzeri (O.S=108.235) internet kullanıcıları arasında istatistiksel olarak farklılıklar saptanmıştır. (Ki-Kare=15.022, sig.<0.05).

20 ile 30 yaş arasındaki katılımcıların tehlike algısı düzeyi diğer tüm katılımcılardan daha düşük düzeydedir.

H4: Farkı eğitim seviyesindeki internet kullanıcıları arasında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri bakımından fark vardır.

Farkı eğitim seviyesindeki katılımcılar arasındaki farkları sınayan KWH testi istatistikleri ve gruplar arasındaki MWU testi karşılaştırma bulguları tablo 6.13'deki gibidir.

Tablo 6.13 Eğitim Seviyeleri (KWH) Test İstatistikleri

Değişken	Eğitim Seviyesi	N	Ort.	Sıra	Ki-Kare	Sig.	Karş.
Riskli Davranışlar	İlköğretim	18	1.837	30.722	33.088	0.000	2>1
	Lise	25	2.824	123.180			3>1
	Lisans	94	2.656	108.258			4>1
	Y.Lisans	41	2.595	103.695			5>1
	Doktora	22	2.495	88.545			5>2
Korumacı Davranışlar	İlköğretim	18	2.263	60.472	30.906	0.000	3>1
	Lise	25	2.643	95.080			4>1
	Lisans	94	2.668	91.833			5>1
	Y.Lisans	41	2.849	110.134			5>2
	Doktora	22	3.365	153.568			5>3
Suça Maruziyet	İlköğretim	18	1.252	68.444	20.951	0.000	2>1
	Lise	25	1.478	125.160			3>1
	Lisans	94	1.317	105.710			4>1
	Y.Lisans	41	1.348	105.463			5>1
	Doktora	22	1.158	62.909			2>5
Tehlike Algısı	İlköğretim	18	3.049	101.194	7.219	0.125	--
	Lise	25	2.941	93.200			
	Lisans	94	2.960	91.505			
	Y.Lisans	41	3.106	110.720			
	Doktora	22	3.191	122.682			

Riskli davranışlar bakımından ilköğretim (O.S=307.22), lise (O.S=123.180), önlisans (O.S=108.258), yüksek lisans (O.S=103.695) ve doktora (O.S=88.545) eğitim

seviyesindeki katılımcılar arasında istatistiksel olarak farklılıklar saptanmıştır. (Ki-Kare=33.088, sig.<0.05).

İlköğretim düzeyinde eğitime sahip katılımcılarım riskli davranış düzeyleri diğer tüm katılımcılardan düşük düzeydeyken doktora seviyesinde eğitime sahip katılımcıların riskli davranış düzeyleri ise diğer tüm katılımcılardan yüksek düzeyde bulgulanmıştır.

Korumacı Davranışlar bakımından ilköğretim (O.S=60.472), lise (O.S=95.080), önlisans (O.S=91.833), yüksek lisans (O.S=110.134) ve doktora (O.S=153.568) eğitim seviyesindeki katılımcılar arasında istatistiksel olarak farklılıklar saptanmıştır. (Ki-Kare=30.906, sig.<0.05).

İlköğretim düzeyinde eğitime sahip katılımcıların korumacı davranış düzeyleri diğer tüm katılımcılardan düşük düzeydeyken, doktora seviyesinde eğitime sahip katılımcıların korumacı davranış düzeyleri ise diğer tüm katılımcılardan yüksek düzeyde bulgulanmıştır.

Suça Maruziyet bakımından ilköğretim (O.S=68.444), lise (O.S=125.160), önlisans (O.S=105.710), yüksek lisans (O.S=105.463) ve doktora (O.S=62.909) eğitim seviyesindeki katılımcılar arasında istatistiksel olarak farklılıklar saptanmıştır. (Ki-Kare=20.951, sig.<0.05).

İlköğretim düzeyinde eğitime sahip katılımcıların suça maruziyet düzeyi diğer tüm katılımcılardan düşük düzeyde iken, doktora seviyesinde eğitime sahip katılımcıların suça maruziyet düzeyi ise ise diğer tüm katılımcılardan yüksek düzeyde bulgulanmıştır

Tehlike Algısı bakımından farklı eğitim seviyelerinde katılımcılar arasında istatistiksel olarak bir fark saptanamamıştır. (Ki-Kare=7.219, sig.>0.05)

H5: Farklı sürelerdir internet kullanan internet kullanıcıları arasında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri bakımından fark vardır.

Farklı sürelerdir internet kullanan katılımcılar arasındaki farkları sınayan KWH testi istatistikleri ve gruplar arasındaki MWU testi karşılaştırma bulguları tablo 6.14'deki gibidir.

Tablo 6.14 İnternet Kullanım Süreleri (KWH) Test İstatistikleri

Değişken	İnternet Kullanım Süresi	N	Ort.	Ort. Sıra	Ki-Kare	Sig.	Karş.
Riskli Davranışlar	1-10	64	2.413	85.227	8.829	0.012	2>1
	11-20	76	2.712	114.167			
	>21	60	2.570	98.050			
Korumacı Davranışlar	1-10	64	2.536	81.508	13.206	0.001	3>1
	11-20	76	2.744	100.533			
	>21	60	2.962	119.058			
Suça Maruziyet	1-10	64	1.340	102.305	1.310	0.519	--
	11-20	76	1.326	103.633			
	>21	60	1.291	93.000			
Tehlike Algısı	1-10	64	2.894	84.430	7.303	0.026	2>1
	11-20	76	3.066	104.573			3>1
	>21	60	3.101	110.892			

Riskli davranışlar bakımından 1-10 yıl (O.S=85.227), 11-20 yıl (O.S=114.167) ve 21 yıl ve üzeri süredir (O.S=98.050) internet kullanan katılımcılar arasında istatistiksel olarak farklar saptanmıştır. (Ki-Kare=8.829, sig.<0.05).

11 ile 20 yıl arasında süredir internet kullanan katılımcıların riskli davranış düzeyleri 1 ile 10 arasında süredir internet kullanan katılımcılardan daha yüksek düzeyde iken, diğer gruplar arasında manidar bir fark yoktur.

Korumacı davranışlar bakımından 1-10 yıl (O.S=81.508), 11-20 yıl (O.S=100.533) ve 21 yıl ve üzeri süredir (O.S=119.058) internet kullanan katılımcılar arasında istatistiksel olarak farklılıklar saptanmıştır. (Ki-Kare=13.206, sig.<0.05).

11 ile 20 yıl arasında süredir internet kullanan katılımcıların korumacı davranış düzeyleri 21 yıl ve üzeri süredir internet kullanan katılımcılardan daha düşük düzeyde iken, diğer gruplar arasında manidar bir fark yoktur.

Suça maruziyet ile katılımcıların internet kullanım süreleri arasında istatistiksel olarak bir fark saptanmamıştır. (Ki-Kare=1.310, sig.>0.05).

Tehlike algısı bakımından 1-10 yıl (O.S=84.430), 11-20 yıl (O.S=104.573) ve 21 yıl ve üzeri süredir (O.S=110.892) internet kullanan katılımcılar arasında istatistiksel olarak farklılıklar saptanmıştır. (Ki-Kare=7.303 sig.<0.05).

1 ile 10 yıl arası süredir internet kullanan katılımcıların tehlike algı düzeyi diğer tüm katılımcılardan daha yüksek iken, 11 ile 20 yıl arası ve 21 yıl ve üzeri süredir internet kullanan katılımcılar arasında bu bakımdan bir fark saptanmamıştır.

H6: Güvenlik eğitimi alan ve almayan internet kullanıcıları arasında riskli davranışlar, korumacı davranışlar, suça maruziyet ve tehlike algısı düzeyleri bakımından fark vardır.

Güvenlik eğitimi alan ve almayan katılımcılar arasındaki farkları sınayan MWU test istatistikleri tablo 6.15'deki gibidir.

Tablo 6.15 Güvenlik Eğitimi Mann Whitney U Test İstatistikleri

Değişken	Güvenlik Eğitimi	N	Ort	Ort Sıra	Z	sig.
Riskli Davranışlar	Evet	52	2.625	103.048	-0.444	0.657
	Hayır	148	2.554	98.922		
Korumacı Davranışlar	Evet	52	3.165	134.067	-4.969	0.000*
	Hayır	148	2.593	87.949		
Suça Maruziyet	Evet	52	1.266	85.615	-2.114	0.034*
	Hayır	148	1.339	105.088		
Tehlike Algısı	Evet	52	3.116	112.346	-1.799	0.072
	Hayır	148	2.988	95.633		

"Riskli davranışlar bakımından güvenlik eğitimi alan (O.S=103.048) ve almayan (O.S=98.922) katılımcıların arasında istatistiksel olarak anlamlı bir fark saptanamamıştır.(z=-0.444, sig.>0.05).

Korumacı davranışlar bakımındaın güvenlik eğitimi alan (O.S=134.067) ve almayan (O.S=97.949) katılımcılar arasında bir fark saptanmıştır. (z=-4.969, sig.<0.05).

Ortalama sıra değerleri incelendiğinde güvenlik eğitimi alan katılımcıların daha yüksek ortalama sıra değerlerine sahip olduğu görülür. Bu durumda güvenlik eğitimi alan katılımcıların daha yüksek korumacı davranış düzeyinde oldukları söylenebilir.

Suça maruziyet bakımından güvenlik eğitimi alan (O.S=85.615) ve almayan (O.S=105.088) katılımcılar arasında istatistiksel olarak farklılıklar saptanmıştır. (z=-2.114, sig.<0.05)

Ortalama sıra değerleri incelendiğinde güvenlik eğitimi almayan katılımcıların daha yüksek ortalama sıra değerlerine sahip olduğu görülür. Bu durumda güvenlik eğitimi almayan katılımcıların daha yüksek suça maruziyet düzeyine sahip oldukları söylenebilir.

Tehlike algısı bakımından güvenlik eğitimi alan (O.S=112.346) ve almayan (O.S=95.633) katılımcılar arasında istatistiksel olarak bir fark saptanmamıştır.(z=-1.799, sig.>0.05)

VII. DEĞERLENDİRME

Bilgi ve iletişim teknolojilerinin etkisinde gerçekleşen dijital dönüşüm ile birlikte internet başta olmak üzere farklı kaynaklardan üretilen bilgi miktarındaki artış, bu bilgilerin güvenliğine yönelik tehdit ve riskleri de beraberinde getirmiştir. Eğitimden sağlığa, iletişimden finans ve ekonomiye toplumsal yaşamın bütün faaliyet ve uygulama alanları, yaşanmakta olan dijital dönüşüme uygun bir şekilde bilginin temel kaynak olarak üretildiği ve kullanıldığı elektronik altyapılı sistemlerle düzenlenmekte ya da tasarımlanmaktadır. Bu dönüşümün yaşandığı önemli alanlardan bir tanesi de vatandaşların artan hizmet ihtiyaçları ile kamu hizmetlerinin sunulması kapsamında devlet yönetimi yapısıdır.

Devlet-vatandaş-iş dünyası ve çalışanlar arasında kullanılan hizmet uygulamaları sayesinde bürokratik işleyişin azalmasıyla hizmetler daha hızlı ve kolay bir şekilde sunulmaktadır. Ancak kamu kurumları ve vatandaşlara ait bilgilerin bulunduğu, iletildiği ya da saklandığı hizmet uygulamalarının ve kullanıcı erişimlerinin güvenliğinin sağlanması varolan tehdit ve risklerin önlenmesi bakımından zorunluluk haline gelmiştir. 2016 yılında ortaya çıkan 50 milyon vatandaşa ait nüfus ve kimlik kayıtlarının tutulduğu Merkezi Nüfus İdare Sistemi (MERNİS) veritabanındaki bilgilerin çalınması olayı bu durumun hassasiyetini ortaya koyan önemli bir örnektir. Bu bağlamda bilgi kaynaklarına sürekli olarak erişim sağlanan her türlü dijital ortamda oluşabilecek olumsuz durumların önüne geçilebilmesi için kurum/kuruluşların ve devlet mekanizmasının bütün teknik ve idari güvenlik önlemlerini sistematik bir şekilde düzenlemesi gerekmektedir.

Bilgi kaynaklarının, özellikle de internet, sosyal medya vb. elektronik ortamların kullanımı sonucu ortaya çıkan kişisel veri olarak nitelendirilen bilgilerin hedef alındığı saldırıların nitelik ve boyut olarak artışı karşısında teknik/idari güvenlik önlemleri tek başlarına bilginin güvenliğini sağlamada yetersiz kalmaktadır. Bu durum bilginin üretilmesi, elde edilmesi, saklanması ve yok edilmesine kadar olan bilgi işleme sürecinde sorumluluk paylaşımı temeline dayanan hukuksal önlemleri de beraberinde getirmektedir. Ülkemizde 2016 yılında iç hukukta karşılığını bulan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve beraberinde çıkartılan farklı yasal düzenlemeler kişisel bilgi güvenliğinin hukuki çerçevesini oluşturmuştur. KVKK ile kişilere ait bilgilerin kim tarafından hangi yollarla elde edildiği, hangi amaçlarla işlendiği, nerede, hangi şartlarla korunduğu ve zamanı geldiğinde nasıl yokedileceği ile ilgili süreçlerin hukuki açıdan açık biçimde ortaya koyulması amaçlanmıştır (Henkoğlu, 2017).

Çalışmanın "Bilgi Güvenliği" bölümünde belirtildiği gibi temelde bilginin bütünselliğine, gizliliğine ve erişilebilirliğine ya da kısaca bilginin kişisel ve kurumsal mahremiyetine yönelik tehdit ve riskler, yangın, su baskını gibi doğal afetlerden, teknolojik altyapıdaki arızalara, sistemler üzerindeki açıklardan kullanıcı hatalarına kadar çeşitli şekillerde oluşabilmektedir. Alanyazın incelendiğinde yapılan farklı araştırmaların sonuçları bilgi güvenliğine yönelik en önemli sorunun insan kaynaklı faktörler olduğunu göstermektedir. Bilgi güvenliğini tehlikeye sokan insan kaynaklı tehdit ve riskler, kişilerin bilinçsiz teknoloji kullanımı ile ilgili alışkanlıkları ya da bilinçli olarak başka kullanıcılara ve sistemlere zarar verme odaklı bütün davranışları şeklinde karşımıza çıkmaktadır. Kişisel bilgi güvenliği farkındalığı kapsamında insanların bilgi iletişim teknolojileri ve internet kullanımı ile ilgili alışkanlıkları

arasındaki ilişkinin incelendiği bu çalışmada da yapılan araştırmalara benzer sonuçlar ortaya çıkmıştır.

Çalışmada kişilerin bilgi iletişim teknolojileri kullanımı ile ilgili alışkanlıkları riskli ve korumacı davranışlar düzeyinde karşılaştırılmış, bu alışkanlıklar sonucu ortaya çıkan davranışların dijital ortamlarda kişilerin suça maruz kalmasına ve tehlike algılarına olan etkileri değerlendirilmiştir. Ortaya çıkan sonuçlar riskli ve korumacı davranışlar, suça maruz kalma ve tehlike algısı bağlamında bilgi güvenliğinde farkındalığın önemini ortaya koymak amcıyla şu şekilde yorumlanmıştır.

Örneklem grubundaki kişilerin gün içerisinde bilgi iletişim teknolojileri ve internet kullanım yoğunlukları oldukça fazladır (Günde 3 saatten fazla %74). Dijital ortamda kullanımla ilgili alışkanlıklara bakıldığında, sosyal medya, video, film izleme, müzik dinleme, program indirme, oyun oynama, kamu hizmetlerinden yararlanma (e-Devlet) ve e posta gibi uygulamaların tercih edildiği görülmüştür. Kişilerin bilgi iletişim teknolojileri ve internet kullanım süreleri arttıkça riskli davranışlar düzeyi de aynı şekilde artmaktadır.

Örneklem grubundaki kişilerin korumacı davranış oluşturabilecek alışkanlıkları incelendiğinde bilgi güvenliğine yönelik tehdit ve risklerin önlenmesi açısından önemli olan antivirüs, güvenlik duvarı, SSL, izleme programları, filtreleme, gibi yazılım uygulamalarını kullanım ve farkındalık düzeyleri oldukça düşüktür.

Örneklem grubundaki kişilerin suça maruz kalma açısından en sık karşılaştıkları durum ise virüsler nedeniyle zarar görme ve internet ortamında istekleri dışında şiddet ve pornografik içerikle karşılaşılmasıdır.

Örneklem grubundaki kişilerin dijital ortamda bilgi güvenliği açısından tehdit ve risk içeren durum ve kavramlara karşı tehlike algıları ve farkındalıkları diğer alışkanlıklarına oranla daha yüksek düzeyde çıkmıştır. Kişilerin %88'i nüfus cüzdanı bilgileri, cep telefonu numarası gibi kişisel nitelikteki bilgilerinin başkaları tarafından bilinmesinin tehlikeli olabileceğini düşünmektedir. Ayrıca kişilerin bilgisayar ve mobil cihazlarda parola kullanımıyla ilgili alışkankanlıkları ve farkındalıklarının yüksek olması da önemlidir.

Sonuç olarak, günümüzde karşılaşılan tehdit ve risklerin çeşitliliği, teknik ve idari zaaflar, bilinçsiz teknoloji kullanımı ve en önemlisi kullanıcı farkındalığının düşük olması gibi nedenlerle bilgi güvenliği farklı disiplinlerle birarada düşünülmesi gereken bütüncül bir süreç olarak değerlendirilmelidir. Bilgi güvenliğinin sağlanması kapsamında bilgi varlıklarının uygulama alanları içerisinde sınıflandırıldığı, teknik, idari ve hukuksal olarak alınacak önlemlerin sistematik bir şekilde belirlendiği stratejiler ve bütün faaliyetler bu kapsamda yürütülmelidir. Dijital dünyada kişilerin bilgi iletişim teknolojilerini kullandıkları her ortamda bilgi güvenliğine yönelik tehdit ve riskleri önlemek için farkındalık oluşturulması önemlidir. Bilgi iletişim teknolojileri ve internet kullanımı konusunda iyi eğitilmiş, dikkatli, bilinçli ve farkındalık sahibi bireylerden oluşan toplum yapısı kurum, kuruluş ve devletlerin üzerinde hassasiyetle durması gereken öncelikli konulardan birisidir.

KAYNAKÇA

AA. (2019). İnfografik, https://www.aa.com.tr/tr/info/infografik/12767 adresinden alınmıştır.

Afyonluoğlu, M. (2017). *Türkiye'de Bilişim Mevzuatı.* http://afyonluoglu.org/ bilisimhukuku/# adresinden alınmıştır.

Afyonluoğlu, M. (2018). *Bilgi Toplumu, E-Devlet ve Kurumsal Yapılar.* http://afyonluoglu.org/e-devlet/ed-kurumsal/ adresinden alınmıştır.

Akıncı N, A. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Çalışma Raporu 6.* Ankara: Bilgi Toplumu Dairesi Başkanlığı. http://www.bilgitoplumu.gov.tr/wpcontent/uploads/2017/07 /AB_Veri_Ko ruma_Tuzugu.pdf adresinden alınmıştır.

Aktan, C. C. (2005). *Bilgi Çaında Bilgi Yönetimi.* Konya: Çizgi Kitabevi.

Aktan, E. (2018). *Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu, Bilgi Yönetimi Dergisi Cilt: 1 Sayı: 1 s:3A.* http://dergipark.gov.tr/download/article-file/482194 adresinden alınmıştır.

AKÜ, B. (2018). *Phishing (Oltalama) Nedir? Afyon Kocateoe Üniversitesi Bilgi İşlem Daire Başkanlığı*. from https://bim.aku.edu.tr/phishing-oltalama-nedir/ adresinden alınmıştır.

Alcorta, L. (1992). The Impact of New Technologies on Scale in Manufacturing Industry:Issues and Evidence. *The United Nations University, UNI/UNITECH*.

Amit, A. (2016). *Understanding difference between Cyber Security & Information Security.* http://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information adresinden alınmıştır.

Anayasa Mahkemesi, E. 2013/122 K.2014/74 (04 09, 2014).

Anı, N. A. (2018). Kişisel Verilerin İşlenmesi ve Açık Rıza, Yüksek Lisans Tezi, İstanbul Üniversitesi, Soyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, s:68. İstanbul.

Arslantekin, S., & Doğan, K. (2015). Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum. *DTCF Dergisi 56.1*, 15.

Atak, S. (2010). Avrupa Konseyi‟nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler. *TBB Dergisi, 1(87),* 90-120.

Atak, S. (2010). Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Güvenceler. *Türkiye Barolar Birliği Dergisi, Sayı 87*, 18-23.

Atasoy, U. (2018). *Sosyal Mühendislik Saldırıları ve Korunma Yolları*. http://www.cezerisga.com/makale/sosyal-muhendislik-saldirilari-ve-korunma-yollari adresinden alınmıştır.

Atılgan, D. (2006). İletişim Teknolojileri Çağında Değişen Bilgi Hizmetleri. *İletişim Teknolojileri Çağında Değişen Bilgi Hizmetleri.* İstanbul: 1. Uluslararası Bilgi Hizmetleri Sempozyumu.

Ayözger, A. Ç. (2016). Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması Yayımlanmış Doktora Tezi. İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

B.İ.T. D. Bşk. (2018). *T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Bilgi ve İletişim Teknolojileri Dairesi*. http://www.bilgitoplumu.gov.tr/bilgi-toplumu/ulkemizde-bilgi-toplumuna-donusum/ adresinden alınmıştır.

Barutçugil, İ. (2002). *Bilgi Yönetimi, İstanbul, s.57.* İstanbul: Kariyer Yayıncılık.

Başaranoğlu, E. (2016). *Bilgi Güvenliği Unsurları*. https://www.siberportal.org/blue-team/securing-information/concepts-of-information-security/ adresinden alınmıştır.

Bateson, G. (1979). *Mind And Nature: A Necessary Unity*. New York: Ballantine.

Baykara, M., Daş, R., & Karadoğan, İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. *1st International Symposiumon Digital Forensics and Security (ISDFS'13)*, (pp. 1-15). Elazığ.

Bengshir, T. K. (2011). TODAİE E-Devlet Merkezi Uygulamalı e-imza Semineri Sunumu. Ankara.

Bernard, M. (2018). *Walmart: Big Data analytics at the world's biggest retailer.* https://www.bernardmarr.com/default.asp?contentID=690 adresinden alınmıştır.

BGA. (2018). *Siber Tehdit İstihbaratı*. https://www.bgasecurity.com/2018/01/siber-tehdit-istihbarati/ adresinden alınmıştır.

BİDB, İ. (2013). *Virüs, Solucan ve Truva Atı*. http://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/virüs-solucan-ve-truva-atı adresinden alınmıştır.

Bilgin, A. A. (2017). Avrupa Birliğinde Verilerin Korunması ve Tamamen Kişisel veya Ev/Hane Halkı Faaliyetleri İstisnası Yayımlanmış Makale. *Ankara Üniversitesi Yayınları, No:564*, 171.

Bilişim Şurası. (2002). *Türkiye Bilişim Şurası, E-Devlet yapısı, E-Devlet Çalışma Grubu Raporu,*. www.bilisimsurasi.org.tr adresinden alınmıştır.

Binark, M. (2017). Sosyal Bilim Araştırmalarında Türkiye'de Veri Etiği Politikası: Sosyal Medya Ortamlarından Veri Toplanması. https://www.researchgate .net/publication/321682314_Sosyal_Bilim_Arastirmalarinda_Turkiye'de_Veri_Etigi_Politikasi_Sosyal_Medya_Ortamlarindan_Veri_Toplanmasi).Sosyoloji Divanı, 5(9): 101-128. ISBN: 2147-8902.

BM, TR. (2016). Birleşmiş Milletler E-Devlet Gelişmişlik Endeksinde Türkiye, https:// www.dijitaldonusum.gov.tr/olcumlerde-turkiye/#BirlesmisMilletler adresinden alınmıştır.

Bragg, R. (2002). *CISSP Security Management and Practices*. http://www.pearsonit certification.com/articles/article.aspx?p=30287&seqNum=2 adresinden alınmıştır.

BTD. (2018). Kamu Bilgi ve İletişim Teknolojileri Yatırımları, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, Bilgi Toplumu Dairesi http://www.bilgi toplumu.gov.tr/wpcontent/uploads/2018/06/Kamu_BIT_Yatirimlari_2018.pdf adresinden alınmıştır.

BTK. (2016). Türkiye'de İnternet Hukuku, Bilgi Teknolojileri ve İletişim Kurumu, http://internet.btk.gov.tr/turkiye-de-internet-hukuku-detay-71.html adresinden alınmıştır.

BTK. (2016). Türkiye'de İnternet Hukuku, http://internet.btk.gov.tr/turkiye-de-internet-hukuku-detay-71.html adresinden alınmıştır.

Buch, R. (2018). *World of Cyber Security and Cybercrime.* https://www.researchgate .net/publication/327110771_World_of_Cyber_Security_and_Cybercrime adresinden alınmıştır.

Bulut, C. (2018). *Bulut Bilişim (Cloud Computing) Nedir?* https://www.endustri40. com/bulut-bilisim-cloud-computing-nedir/ adresinden alınmıştır.

Bus. Ins. (2018). The 21 scariest data breaches of 2018, https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12 adresinden alınmıştır.

Can, Ö. (2014). Kurumsal Ağ ve Sistem Güvenliği Politikalarinin Önemi ve Bir Durum Çalışması. *Türk Bilim Araştırma Vakfı Dergisi,Cilt: 7, Sayı: 2*, 16-31.

Canada. (2018). *Top 10 Ways Your Privacy is Threatened.* http://www.gov.pe.ca/photos/original/oipc_dpdthreats.pdf adresinden alınmıştır.

Canbek, G. (2005). Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Canbek, G., & Sağıroğlu, Ş. (2006). Ankara: Bilgi ve Bilgisayar Güvenliği Casus Yanlımlar ve Korunma Yöntemleri, Grafiker Yayınları.

Canbek, G., & Sağıroğlu, Ş. (2006). *Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, Cilt 9, Sayı 3*, 165-174.

Canbek, G., & Sağıroğlu, Ş. (2007). *Gazi Üniv. Müh. Mim. Fak. Der. Cilt 22, No 1 Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma*, 121-136.

Carbon Black. (2018). *7 Experts on Moving to a Cloud-Based Endpoint Security Platform*. https://www.carbonblack.com/resources/definitions/what-is-endpoint-security/ adresinden alınmıştır.

Civelek Y., D. (2011). Kişisel Verilerin Korunmasi ve Bir Kurumsal Yapilanma Önerisi. *Planlama Uzmanlığı Tezi*. Ankara,: Yayın No: 2821, DPT,.

Civelek, M. (2009). *İnternet Çağı Dinamikleri.* İstanbul: Beta Yayınları.

CoESS. (2018). *CoESS Kritik Altyapıların Güvenliği Çalışma Komitesi Sunuş Raporu.*

Columbus, L. (2014). *Ten Ways Big Data Is Revolutionizing Manufacturing.* https://www.forbes.com/sites/louiscolumbus/2014/11/28/ten-ways-big-data-isrevolutionizing-manufacturing/#3f4ed2f5ce16 adresinden alınmıştır.

Cryptomathic. (2018). *What is non-repudiation?* https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-non-repudiation adresinden alınmıştır.

Curphey, M. (2002). *Access Control and Authorization, A Guide to Building Secure Web Applications*. https://www.cgisecurity.com/owasp/html/ adresinden alınmıştır.

Çağala, C. (2017). *Keylogger Nedir? Ne İşe Yarar? Ne Amaçla Kullanılır?* https://www.tech-worm.com/keylogger-nedir-ne-ise-yarar-ne-amacla-kullanilir/ adresinden alınmıştır.

Çalık, D. (2009). Geçmişten Günümüze Bilgi Yaklaşımları Bilgi Toplumu ve İnternet. İstanbul: XIV. Türkiye'de İnternet Konferansı Bildirileri, Bilgi Üniversitesi.

Çalışkan, M. (2014). Sanallaştrma Teknolojilerinin Saldırı Tespit ve Önleme Sistemlerinin Performansı Üzerine Etkisi, Hava Harp Okulu Havacılık ve Uzay Teknolojileri Enstitüsü, Yüksek Lisans Tezi. İstanbul.

Çapar, B. (2005). Konya: Bilgi Yönetimi". Bilgi Çağı Bilgi Yönetimi ve Bilgi Sistemleri İçinde, 175-195, Çizgi Kitabevi.

Çapar, B. (2008). Bir İletişim Sistemi Olarak Bilgi Yönetimi: Teorik Bir Yaklaşım, https://tr.scribd.com/document/9588671/Bilgi-Yonetimi-Teorik-Bir

Çelebioğlu, F. (2018). *Enformasyon Toplumunun Temel Parametreleri ve Türkiye'nin Durumu.*https://www.academia.edu/26285079/enformasyon_toplumunun_temel_paramet releri_ve_türkiyenin_durumu

Çelik, S., & Çeliktaş, B. (2018). Güncel Siber Güvenlik Tehditleri Fidye Yazılımlar,. *Cyberpolitik Journal Vol. 3, No. 5, http://cyberpolitikjournal.org/wp-content/uploads/2018/08/cyberpolitik_journal_no_5.pdf*, 105-133.

Çetiner, Y. T. (2011). E-Dönüşümde Türkiye Nerede? *http://www.mfa.gov.tr/data/Kutuphane/yayinlar/EkonomikSorunlarDergisi/sayi31/Turan.pdf*, 41-48.

Çevik, D. (2019). *DDoS Saldırıları*. Biznet Bilişim: https://www.biznet.com.tr/ddos-saldirilari-101/

Dal, B. (2013). *Perakendecilikte Büyük Veri Kullanım Alanları,*. http://www.retailturkiye. com/bulent-dal/perakendecilikte-buyuk-veri-kullanim-alanlari

DEBİS. (2019). *Spam Nedir? Dokuz Eylül Üniversitesi Bilgi Sistemi*. http://web.deu.edu.tr/ sss/spam.html adresinden alınmıştır.

Demirel, D. (2006). *Değişimin Rotası e-Türkiye, E-Devlet ve Dünya Örnekleri, Sayıştay Dergisi Sayı:61.* https://kontrol.bumko.gov.tr/Eklenti/6833,demirel-d-e-devlet-ve-dunya-ornekleri.pdf adresinden alınmıştır.

Derinözlü, C. (2007). Büyük Veri ve Mahremiyet (Big Data And Privacy). *TUBITAK 1.Ulusal Bulut Bilişim ve Büyük Veri Sempozyumu B3S17 Sempozyumu Bildiri Kitabı.* TÜBİTAK.

Dğş. (12.09.2010). https://www.tbmm.gov.tr/anayasa/anayasa_2017.pdf adresinden alınmıştır.

Dilek, U. (2017). *Bilgi Güvenliği Nedir ve Nasıl Sınıflandırılır?* https://tr.linkedin.com/pulse/bilgigüvenliği-nedir-venasılsınıflandırılır-ufuk-dilek adresinden alınmıştır.

Doğan, M. (2014). Büyük Veri'nin Kişiler ve Kurumlar Üzerindeki Etkileri. *Bilgi Üniversitesi, Yüksek Lisans Tezi*. İstanbul.

Dokuz, A. Ş., & Çelik, M. (2018). Bulut Bilişim Sistemlerinde Verinin Farklı Boyutları Üzerine Derleme. *Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi, Cilt 6, Sayı 2*, 316-338.

Durna, U., & Demirel, Y. (2008, Ocak-Haziran). *Bilgi Yönetiminde Bilgiyi Anlamak, Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Sayı: 30, s.138.* http://dergipark.ulakbim.gov.tr/erciyesiibd/article/view/5000115376 adresinden alınmıştır.

EC, 8. (1981, 01). *28 Ocak 1981 tarih ve 108 sayılı "Avrupa Konseyi Kişisel Verilerin Otomatik İşlenmesine İlişkin Olarak Bireylerin Korunması Hakkındaki Avrupa Sözleşmesi.* http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktaraflisoz/ak/turkce/108_tur.pdf adresinden alınmıştır.

ECJ. (2014). *(C-293/12 ve C-594/12 Birleşik Davası) EU:C:2013:845EU:C:2014:238.* http://www.abgm.adalet.gov.tr/abadaletdivani/belgeler/karar_.pdf adresinden alınmıştır.

ECJ. (2014). *The Court of Justice declares the Data Retention Directive to be invalid.* https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf adresinden alınmıştır.

E-Devlet. (2018). E-Devlet Nasıl Çalışıyor, https://www.turkiye.gov.tr/bilgilendirme?konu=nasilCalisiyor

E-Devlet. (2018). Türkiye'de Dijital Dönüşüm, Organizasyon Yapısı, https://www.dijital donusum.gov.tr/organizasyon-yapisi/ adresinden alınmıştır.

E-Devlet. (2019). https://www.turkiye.gov.tr/cok-kullanilan-hizmetler adresinden alınmıştır.

Endeks, B. (2016). *Birleşmiş Milletler E-Devlet Gelişmişlik Endeksinde Türkiye.* https:// www.dijitaldonusum.gov.tr/olcumlerde-turkiye/#BirlesmisMilletler adresinden alınmıştır.

Erkul, R. E. (2004). Dünyada Kamu Yönetimindeki Dönüşüm ve Türkiye'de Kamu Yönetimi Öğretimine Yansımaları. *II. Kamu Yönetimi Forumu*, (pp. 212-225). Ankara.

EU TR. (2016). *Avrupa Birliği E-Devlet Gelişmişlik Endeksinde Türkiye.* https://www. dijitaldonusum.gov.tr/olcumlerde-turkiye/#AvrupaBirligi adresinden alınmıştır.

Exastax. (2017). Büyük Veri ve Veri Analizi Telekom Operatörleri İçin Nasil Değer Sağlar? https://www.exastax.com.tr/buyuk-veri/buyuk-veri-analizi-telekom-icin-nasil dege r-saglar/ adresinden alınmıştır.

Exastax. (2018). Finansal Teknoloji Sektöründe Büyük Veri Kullanım Senaryoları, https://www.exastax.com.tr/finansal-teknolojiler/finansal-teknoloji-sektorunde-buyuk-veri -kullanim-senaryolari/ adresinden alınmıştır.

Eyüpoğlu, C. (2017). *Büyük Veride Kişi Mahremiyetinin Korunması, Bilişim Teknolojileri Dergisi, Cilt: 10, Sayı: 2,.* http://dergipark.gov.tr/download/article-file/297868 adresinden alınmıştır.

Fadhıl, W. M. (2014). Geleneksel Devlet Anlayışından E-Devlete: Türkiye ve Irak E-Devlet Algısı Karşılaştırması. *Bilişim Teknolojileri Dergisi, Cilt: 7, Sayı: 3*.

FBI. (2019). Intellectual Property Theft/Piracy, https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft adresinden alınmıştır.

Fearn, N. (2018). *Application security more important than ever*. https://www.computer weekly.com/feature/Application-security-more-important-than-ever adresinden alınmıştır.

Fortune. (2018). http://www.fortuneturkey.com/akilli-uretim-cagi-endustri-40-42841 adresinden alınmıştır.

Fruhlinger, J. (2018). *What is network security? Definition, methods, jobs & salaries.* https://www.csoonline.com/article/3285651/what-is-network-security-definition-methods-jobs-and-salaries.html adresinden alınmıştır.

Furuncu, E. (2018). *Bulut Bilişim Güvenliği 85.* Gebze Yüksek Teknolojisi Enstitüsü: http://anibal.gyte.edu.tr/hebe/AblDrive/59669005/w/Storage/104_2010_2_673_59669005/Homeworks/cloud-sec.pdf? adresinden alınmıştır.

Gaitho, M. (2018). *How Applications of Big Data Drive Industries.* https://www.simplilearn.com/big-data-applications-in-industries-article adresinden alınmıştır.

Gb. (2018). Cyber attacks 2017: What were their impacts, and what to expect in cybersecurity for 2018, https://www.gb-advisors.com/cyber-attacks-2017/ adresinden alınmıştır.

Global Dig. Rpr. (2018). *Global Digital Report 2018.* UK: https://digitalreport.wearesocial.com/. adresinden alınmıştır.

Go Globe. (2017). *Things That Happen Every 60 Seconds.* https://www.go-globe.com/blog/things-that-happen-every-60-seconds/ adresinden alınmıştır.

Grant, N. (2018). *Amazon Lands $1 Billion in Cloud Deals With SAP, Symantec.* https://www.bloomberg.com/news/articles/2018-10-09/amazon-is-said-to-win-1-billion-in-cloud-deals-with-sap-symantec adresinden alınmıştır.

Greenleaf, G. (2008). Accession to Council of Europe Privacy Convention 108 by non European States. *Privacy Laws and Business International, 94(1),* 1-3.

Gümüş, S. (2014). *İnternet Reklamlarının Tüketicinin Satınalma Davranışlarına Etkileri.* İstanbul: Hiperlink Yayınları.

Güngör, M. (2015). Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapilanma, Uzmanlık Tezi. Ankara: Bilgi Toplumu Dairesi Başkanlığı.

Gürak, H. (2006). *Önce Bilgili İnsan, Ekonomik Büyüme ve Refahın Gerçek Kaynakları Olan: Üretim Bilgisi (Teknoloji) ve Nitelikli Emek Üzerine.* https://www.academia.edu/417662/Önce_Bilgili_İnsan_nitelikli_emek_beşeri_sermaye_hakkında adresinden alınmıştır.

Henkoğlu, T. (2017). *Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme, Arşiv Dünyası Dergisi, Sayı 17-18, ISSN: 2147-2599,*, 46-56.

Henkoğlu, T. (2017). Veri Koruma Kanununun Getirdikleri, What Data Protection Law Brings in, Yayımlanmış makale, http://dergipark.gov.tr/download/article-file/359655 adresinden alınmıştır.

Henkoğlu, T. (2017). *Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme, Arşiv Dünyası Dergisi, Sayı:17-18, İstanbul*.

Hootsuite & We Are Social. (2017). *Hotsuite & we are social. Digital in 2017: Global Overview.* https://wearesocial.com/special-reports/digital-in-2017-global-over view adresinden alınmıştır.

IDC. (2017). *Big data market to climb to $210 billion by 2020.* http://ecsnamagazine.arrow.com/big-data-market-to-climb-to-210-billion-by-2020/ adresinden alınmıştır.

Incapsula. (2019). *What is Social Engıneering*. https://www.incapsula.com/web-application-security/social-engineering-attack.html adresinden alınmıştır.

İnce, N. M. (2001, Ağustos). *Elektronik Devlet Kamu Hizmetlerinin Sunulmasında Yeni İmkanlar*.http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Murat_ Ince_E-Devlet.pdf

ISO. (2005). *Code Of Practice for Information Security Management, ISO: 27002:2005.* Switzerland: ISO Publications.

ITU. (2018). *Definition of cybersecurity, referring to ITU-T X.1205*. https://www.itu.int /en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx adresinden alınmıştır.

Kadrich, M. S. (2007). *Endpoint Security*. SearchSecurity: https://searchsecurity. techtarget.com/feature/Endpoint-Security adresinden alınmıştır.

Kalkınma, B. (2018). *T.C. Kalkınma Bakanlığı Kamu Bilgi ve İletişimTeknojileri Yatırımları, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, Bilgi Toplumu Dairesi.*http://www.bilgitoplumu.gov.tr/wpcontent/uploads/2018/06/Kamu_BIT_ Yatirimlari_2018.pdf adresinden alınmıştır.

Kalseth, K., & Sarah, C. (2001). *Knowledge Management: Development Strategy or Business Strategy?". Information Development, 163-172.*

Karaarslan, E. (2017). *Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması.* http://csirt.ulakbim.gov.tr/dokumanlar/BilgisayarAglarindaGuvenlikPolitikalarini nUygulanmasi.pdf

Karaca, İ. (2015). *Büyük Veri Analizlerinin Kurumsal Faaliyetlerde Kullanım Alanları.* Ankara: Ankara Üniversitesi.

Karagülmez, A. (2010). *Elektronik Devlet Kavramı, Türkiye Adalet Akademisi Dergisi, Yıl:1, Sayı:2 s.457.* http://www.taa.gov.tr/indir/elektronik-devlet-kavrami adresinden alınmıştır.

Kasapoğlu, C. (2017). Siber Güvenlik: Beşinci Boyutu Anlamak. In *EDAM Siber Politikalar Kağıtları Serisi.* İstanbul.

Kaspersky. (2018). What is Scareware? https://www.kaspersky.com.tr/resource-center/definitions/scareware adresinden alınmıştır.

Kaspersky. (2019). Reklam Yazılımı Nedir?, https://www.kaspersky.com.tr/resource-center/threats/adware adresinden alınmıştır.

Kavrakoğlu, F. (2018, Haziran 17). Sanayi Devrimleri: http://blog.kavrakoglu.com/tag/ikinci-sanayi-devrimi/ adresinden alınmıştır.

Kaya, A. (2016). *Virüs Nedir? Çeşitleri Nelerdir?* https://www.tech-worm.com/virus-nedir-cesitleri-nelerdir-2/

Kaya, B. M. (2017). *Büyük Verinin Hukuki Boyutları, Büyük Veri ve Açık Veri Analitiği : Yöntemler ve Uygulamalar, s:181.* Ankara.

Kaya, C. (2005). Ankara: İdare Hukukunda Bilgi Edinme Hakkı, s:88, Seçkin Yayınları.

Kaya, C. (2011). Avrupa Birliği 1995/46/EC Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, ÎÜHFM, C. LXIX, S. l -2 s: 318, http://dergipark.gov.tr/download/article-file/97634 adresinden alınmıştır.

Kaya, Ö. F. (2017). Kurumsal İşletmelerde Bilgi ve Veri Güvenliği, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü, Siber Güvenlik Anabilim Dalı, Yüksek Lisans Tezi. İstanbul.

Kayar, E. (2014). Advanced Persistent Threat (APT), https://lostar.com.tr/2014/11/advanced-persistent-threat-apt.html adresinden alınmıştır.

Kayar, E. (2016). Lostar: Backdoor (Arka Kapı), https://lostar.com.tr/2016/09/backdoor-arka-kapi.html adresinden alınmıştır.

Keleştemur, A. (2015). *Siber İstihbarat, 1. Baskı.* İstanbul: Yazın Basın Yayınevi Matbaacılık Trz.Tic.Ltd.Şti.

Kent, E. (2018). *Endüstrinin Gelişimine Bakış.* http://www.endustri40.com/endustrinin-gelisimine-bakis/+

Keser, L. (2014). *Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi.* İstanbul: Bilgi Üniversitesi Yayınları.

Keung, Y. H. (2014). *Editorial Open Access, Basic Principle of Information Security*. https://www.omicsonline.org/open-access/basic-principle-of-information-security-2168-96 95.1000e120.php?aid=25302 adresinden alınmıştır.

Kiguolis, L. (2016). *Arka Kapı Nedir ve Nasıl Temizlenir?* Virüsler: http://virusler. info.tr/arka-kapi/ adresinden alınmıştır.

Kılınç, D. (2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması. *Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 61(3)*, 1128.

Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences.* London: Sage.

Korkmaz, İ. (2016). Kişisel Verilerin Korunmasi Kanunu Hakkinda Bir Değerlendirme. *Türkiye Barolar Birliği Dergisi*, 124.

Korolov, M. (2019). *What is a botnet? And why they aren't going away anytime soon*. https://www.csoonline.com/article/3240364/what-is-a-botnet-and-why-they-arent-going-away-anytime-soon.html adresinden alınmıştır.

Köksal, A. (2018). *Bilişim Toplumu: Bir Tanım Denemesi.* http://aydinkoksal. gen.tr/shared/files/Yayinlar/Yd17_ak_BilsmTopl_TBA05.doc adresinden alınmıştır.

Kul, Seval. (2019). Biyoistatistik SPSS ile İstatistik Veri Analizi http://www.p005 .net/pdegerinedir adresinden alınmıştır.

Kutlu, Ö. (2017). Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi, An Analysis of Personal Data Protection Policy in Turkey. *Politik Araştırmalar Dergisi, Ekonomi ve Yönetimi*, 52-53.

KVKK. (2016). http://www.resmigazete.gov.tr/eskiler/2016/04/20160407.pdf adresinden alınmıştır.

KVKK. (2017). Kişisel Verilerin Korunması Kanunu ve Uygulaması, https://www.kvkk .gov.tr/yayinlar/kişiselverilerinkorunmasikanunuveuygulamasi.pdf adresinden alınmıştır.

KVKK İşlenme Şartları. (2017). Kişisel Verilerin İşlenme Şartları, https://www.kvkk. gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari adresinden alınmıştır.

KVVK İlkeler. (2017). Kişisel Verilerin İşlenmesine İlişikin Temel İlkeler, https:// www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler

La Rue, F. (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* New York City: United Nations.

Laing, B. (2017). *Drive-By Downloads and How to Prevent Them?* lastline: https://www.lastline.com/blog/drive-by-download/ adresinden alınmıştır.

Lawyer, S. (2018). *Wiper Malware Can Wipe You Out*. https://lp3.com/tips/wiper-malware-can-wipe-you-out/

Mantelero, A. (2012). Cloud Computing, Trans-Border Data Flows And The European Directive 95/46/EC: Applicable Law And Task Distribution. *European Journal of Law and Technology, 3(2)*, 1-6.

Martin, M. (2015). *A Complete Guide to Data Security*. https://www.cleverism.com/complete-guide-data-security/

Mass. (2016). Massachusetts Technology Collaborative Big Data Report, http://www.mass tech.org/research-and-analysis/mass-big-data-reports adresinden alınmıştır.

Mc Donald, C. (2017). *The Motivation for Big Data.* https://mapr.com/blog/big-data-opportunities-telecommunications/ adresinden alınmıştır.

Media Click. (2019). *Bootstrap nedir?* Media Click: https://www.mediaclick.com.tr/blog/bootstrap-nedir adresinden alınmıştır

Melissa, 1. (2018). *Melissa*. http://malware.wikia.com/wiki/Melissa adresinden alınmıştır.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology.* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf adresinden alınmıştır.

Meola, A. (2016). *Why Iot, Big Data & Smart Farming are The Future of Agriculture.* http://www.businessinsider.com/internet-of-things-smart-agriculture-2016-10 adresinden alınmıştır.

Micro, T. (2018). *Basın Bültenleri, 2018'de Siber Dünyayı Bekleyen Tehlikeler.* http://www.trendmicro.com.tr/newsroom/pr/de-siber-duenyay-bekleyentehlikeler /index. html adresinden alınmıştır.

Microsoft. (2018). *.NET framework sürümleri ve bağımlılıkları*. Microsoft: https://docs.microsoft.com/tr-tr/dotnet/framework/migration-guide/versions-and-dependencies adresinden alınmıştır

Mirai. (2016). *DDoS attack that disrupted internet was largest of its kind in history, experts say*. The Guardian: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet adresinden alınmıştır.

Moral, O. (2016). Sanallaştırma, http://www.onurmoral.com/8-data-centre/7-veri-merkezi-sanallast-rma adresinden alınmıştır.

Morgan, S. (2018). *Global Ransomware Damage Costs Predicted To Exceed $8 Billion In 2018.* Cybersecurity Ventures: https://cybersecurityventures.com/global-ransomware-da mage-costs-predicted-to-exceed-8-billion-in-2018/ adresinden alınmıştır.

MTC. (2016). *Massachusetts Technology Collaborative Big Data Report.* http://www.masstech.org/research-and-analysis/mass-big-data-reports adresinden alınmıştır.

MÜSİAD. (2017). *Endüstri 4.0 ve Geleceğin Lojistiği Lojistik Sektör Raporu 2017.* http://www.musiad.org.tr/F/Root/Pdf/lojistik_raporlari_2017_12_25.PDF adresinden alınmıştır.

ODTÜ. (2018). *İnternet Tarihi*. Orta Doğu Teknik Üniversitesi Bilgi İşlem D. Bşk. http://www.internetarsivi.metu.edu.tr/tarihce.php adresinden alınmıştır.

OECD. (2013). *Organisation for Economic Co-Operation and Development.* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm adresinden alınmıştır.

OECD. (2015). İstanbul: Türkiye'de ve AB'de Kişisel Verilerin Korunmasi, Yayın No:278, s:14, İktisadi Kalkınma Vakfı Yayınları.

Oğuz, H. (2013). *Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum:.* http://dergipark.gov.tr/mdergi/issue/16883/175778 adresinden alınmıştır.

Oliveira, A. (2014) A History of the Work Concept: From Physics to Economics. New York: Springer

Öğüt, A. (2003). *Bilgi Çağında Yönetim (2. Baskı), s.11.* Ankara: Nobel Yayıncılık.

Öğütçü, G. (2010). E-Dönüşüm Sürecinde Kişisel Bilgi Güvenliği Davranışı ve Farkındalığı. Yayınlanmamış Yüksek Lisans Tezi. Başkent Üniversitesi FBE. Ankara.

Özcan, R. (2018). Yükselen yeni siber risk: Fikri mülkiyet hırsızlığı, http:// www.sigortacigazetesi.com.tr/yukselen-yeni-siber-risk-fikri-mulkiyet-hirsizligi/ adresinden alınmıştır.

Özçelik, T. Ö. (2010). *E-DEVLET,Uzaktan Eğitim Ders kitabı.* http://content.lms. sabis.sakarya.edu.tr/Uploads/75862/38682/edevlet_13_14.pdf adresinden alınmıştır.

Özdemiroğlu, A. (2018). *Man In The Middle (MITM) saldırıları nedir ?* https://www. teknolojik-blog.com/man-in-the-middle-mitm-saldirilari-nedir/ adresinden alınmıştır.

Özsoylu, A. F. (2017). Endüstri 4.0. *Çukurova Üniversitesi İİBF Dergisi, Cilt:21, Sayı:1*.

Öztemiz, S., & Yılmaz, B. (2013). Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği. *Bilgi Dünyası, 14 (1)*, 87-10.

Parsons, K. M. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment, Report published by Defence Science and Technology Organisation, DSTO-TR-2484, Edinburgh South Australia.* http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/10094/1/DSTO-TR-2484%20PR.pdf adresinden alınmıştır.

Profelis. (2018). *Uygulama Güvenliği Nedir?* https://www.profelis.com.tr /tr/cozumler/uygulama-guvenligi/ adresinden alınmıştır.

Raiu, C. (2013). *Destructive Malware – Five Wipers in the Spotlight*. https://securelist. com/destructive-malware-five-wipers-in-the-spotlight/58194/ adresinden alınmıştır.

Resmi Gazete (05.05.2016). Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol (181 Sayılı Ek Protokol) http://www.resmigazete.gov.tr/eskiler/2016/05/20160505.pdf adresinden alınmıştır.

Resmi Gazete (07.04.2016). Kişisel Verilerin Korunması Kanunu, http://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf adresinden alınmıştır.

Resmi Gazete (18.02.2016). Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasına Dair Kanun, http://www.resmigazete.gov.tr/eskiler/2016/02/20160218.htm adresinden alınmıştır.

Robinson, R. M. (2015). *Wiper Malware Poses Destructive Threat*. https://security intelligence.com/wiper-malware-poses-destructive-threat/ adresinden alınmıştır.

Rouse, M. (2014). Authentication, Authorization, and Accounting AAA, https:// searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting adresinden alınmıştır.

Rouse, M. (2014). *Confidentiality, Integrity, and Availability*. https://whatis.techtarget .com/definition/Confidentiality-integrity-and-availability-CIA adresinden alınmıştır.

Rukancı, F. (2004). *Bilgi Toplumu ve Toplumun Bilgilenmesinde Kütüphanelerin Rolü Information Society and Libraries' Role of Informating Society.* https://www. researchgate.net/publication/28808417

Sağıroğlu, Ş. (2016). (p. 12). Ankara: Büyük Veri Analitiği, Güvenliği ve Mahremiyeti (Big Data Analytics, Security And Privacy), Gazi Üniversitesi.

Sağıroğlu, Ş. (2017). *Yöntemler ve Uygulamaları, Büyük Veri ve Açık Veri Analitiği* (s. 15). Ankara: Gazi Üniversitesi.

Saltzer, J., & Schroeder, M. (1975). *The Protection of Information in Computer Systems* http://web.cs.wpi.edu/~guttman/cs557_website/papers/saltzer1975.pdf adresinden alınmıştır.

Sarıdal, M. (2018). *jQuery nedir*. MS Yazılımcının Not Defteri: https://www.mustafa saridal.com/webprogramlama/jquery/jquery-nedir-nerelerde-kullanilir-nasildir/ adresinden alınmıştır

Sevimli, A. (2006). *İşçinin Özel Yaşamına Müdahalenin Sınırları, 1. Baskı.* İstanbul: Legal Yayıncılık.

Shannon, S. (2018). *Updated for 2018: The five Vs of big data: how can they help your business?* https://www.xsnet.com/blog/updated-for-2017-the-vs-of-big-data-velo city-volu me-value-variety-and-veracity adresinden alınmıştır.

Siemens. (2018). *Endüstri 4.0 Yolunda.* Endüstri 4.0 Yolunda http://siemens.e-dergi.com/pubs/Endustri40/Endustri40/Default .html#p=8 adresinden alınmıştır.

Tahgizadeh, K., & Keser, G. (2015). Dördüncü Sanayi Devrimi: Yarının Fabrikaları Neye Benziyor? *Taşıt Araçları Yan Sanayicileri Derneği Dergisi, 84, 68-70.*

TBD. (2006). *TBD Kamu-BİB Kamu Bilişim Platformu E-Devlet Kavramları El Kitabı.* http://eski.tbd.org.tr/usr_img/cd/kamubib17/diger/BG3-2006.pdf adresinden alınmıştır.

TBMM. (1949). *İnsan Hakları Evrensel Beyannamesi.* https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf adresinden alınmıştır.

TDK. (2018). Teknoloji, http://www.tdk.gov.tr/index.php?option=com_gts&kelime=teknoloji adresinden alınmıştır.

Techopedia. (2018). *Definition - What does Velocity mean?* https://www.techopedia.com/definition/16762/velocity-big-data adresinden alınmıştır.

TechWeb, B. (2018). *Understanding Authentication, Authorization, and Encryption*. https://www.bu.edu/tech/about/security-resources/bestpractice/auth/ adresinden alınmıştır.

Tekerek, M. (2008). *Bilgi Güvenliği Yönetimi. KSÜ Doğa Bilimleri Dergisi, 11 (1),* http://dergipark.gov.tr/ksudobil/issue/35406/393310 adresinden alınmıştır.

Toffler, A. (1980). *The Third Way.* New York: Bantam Books.

Tools4ever. (2019). *What is Identity and Access Management?* https://www.tools4ever.com/what-is-identity-and-access-management/ adresinden alınmıştır.

Tosun, T. (2017). Dünya'da ve Türkiye'de Veri Merkezleri ve Türkiye Kamu Entegre Veri Merkezinin Kurulması. *Akademik Sosyal Araştırmalar Dergisi Yıl: 5, Sayı: 57,* 665.

TUİK. (2018). *Hane Halkı Bilişim Teknolojileri Kullanım Araştırması.* http://www.tuik.gov.tr/PreTablo.do?alt_id=1028 adresinden alınmıştır.

Turkhackteam. (2018). *DDoS Nedir, Nasıl Korunulur? Web & Server Güvenliği*. https://www.turkhackteam.org/web-server-guvenligi/1673635-ddos-nedir-nasil-korunulur. html adresinden alınmıştır.

Türkiye Bilişim Şurası. (2002). *Türkiye Bilişim Şurası, E-Devlet yapısı, E-Devlet Çalışma Grubu Raporu,*. from www.bilisimsurasi.org.tr adresinden alınmıştır.

TÜSİAD. (2016). *Türkiye'nin Küresel Rekabetçiliği İçin Bir Gereklilik Olarak Endüstri 4.0 – Gelişmekte Olan Ekonomi Perspektifi*. İstanbul: TÜSİAD.

Uçak, N. Ö. (2010). Bilgi: Çok Yüzlü Bir Kavram Information: A Multi-Faceted Concept. *Türk Kütüphaneciliği 24*, 705-722.

Uçkan, Ö. (2003). *E-Devlet, E-Demokrasi ve Türkiye, Kamu Yönetiminin Yeniden Yapılanması İçin Strateji ve Politikalar-I, s. 47*. İstanbul: Literatür Yayıncılık.

Uğuz, S. (2018). Kurumsal Bilgi Güvenliği Yönetim Sistemi Yazılımları: Örnek Bir Yazılım Geliştirilmesi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 1-11.

Ünal, F. (2016). *Türkiye'de E-Devlet Uygulamalarının Kamu Hizmetlerinin Sunumunda Etkinliği: Adalet Bakanlığı Uyap Bilişim Sistemi Örneği,D.Ü. Sosyal Bilimler Dergisi.* http://dergipark.gov.tr/download/article-file/270972 adresinden alınmıştır.

Ünal, Y. (2009). Bilgi Toplumunun Tarihçesi. *Sosyal Bilimler Enstitüsü Tarih Okulu Dergisi, Sayı 5*, 134.

Vicente, D. (2019). *Kaspersky Security Bulletin 2018. Threat Predictions for 2019*. https://securelist.com/kaspersky-security-bulletin-threat-predictions-for-2019/88878/ adresinden alınmıştır.

Ware, W. H. (1979). *Securıty Controls For Computer Systems, R-609-1, Report of Defense Science Board Task Force on Computer Security, Santa Monica, CA.* http://www.linuxsecurity.com/resource_files/documentation/R609.1.html adresinden alınmıştır.

Web Matters. (2014). *Considering a CQRS approach with ASP.Net MVC.* Web Matters: https://web-matters.blogspot.com/2014/08/cqrs-with-aspnet-mvc-entity-framework.html adresinden alınmıştır

webhostingturkey. (2015). *21 Adımda Sunucu Sanallaştırma Güvenliği*. http://www.webhostingturkey.com/post/2014/06/13/21-Adımda-Sunucu-Sanallastırma-Guvenligi.aspx adresinden alınmıştır.

Wikipedia. (2018). İnternet'in Tarihi, https://ipfs.io/ipns/tr.wikipedia-on-ipfs.org/wiki/Internetin_tarihi.html adresinden alınmıştır.

Wikipedia. (2018). *İnternet'in Tarihi*. https://tr.wikipedia.org/wiki/İnternetin_tarihi adresinden alınmıştır.

Wikipedia. (2019). Security Management, https://en.wikipedia.org/wiki/Security_management adresinden alınmıştır.

Winston, E. (2018). *What is data security?* https://www.quora.com/What-is-data-security adresinden alınmıştır.

Woods, M., & Woods, M. (2001). *Ancient Computing: From Counting to Calendars.* Twenty-First Century Books.

Yeşilorman, M. (2016). Bilgi Toplumunun Temelleri Üzerine Eleştirel Bir Bakış. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 118.

Yeşilorman, M., & Koç, F. (2018). *Bilgi Toplumunun Teknolojik Temelleri Üzerine Eleştirel Bir Bakış, Firat Universitesi Sosyal Bilimler Dergisi*, 20. Bilgi

Toplumunun Teknolojik Temelleri Üzerine Eleştirel Bir Bakış, https://www.scilit.net/article/ 2707acc71dfd107d74bedff175b280ca adresinden alınmıştır.

Yıldız, M. (2014). Siber Suçlar ve Kurum Güvenliği, Denizcilik Uzmanlık Tezi. Ankara: Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi İşlem Daire Başkanlığı.

Yıldız, T. (2017). *Dördüncü Endüstri Devrimi ve Türkiye'deki Mevcut Durum.* https://www.researchgate.net/publication/321419039_Yaklasan_Dorduncu_Endustri_Devrimi_ve_Turkiye'deki_Mevcut_Durum adresinden alınmıştır.

Yılmaz, M. (2009). Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi 49*, 95-118.

Zacks, A. (2018). *Truva Atı (Trojan Horse) Nedir ve Ona Karşı Nasıl Koruma Sağlanır?* Safety Detective: https://tr.safetydetective.com/blog/truva-ati-trojan-horse-nedir-ve-ona-karsi-nasil-koruma-saglanir/ adresinden alınmıştır.

ÖZGEÇMİŞ

Can GENÇ
Doğum Tarihi: 16/08/1980
E-Posta: cangenctr@hotmail.com
TÜRKİYE - İstanbul (AVR.) - Sarıyer
Cep Telefonu: 90 (530) 787 04 87

EĞİTİM BİLGİLERİ

Yabancı Dil: İngilizce (İyi)

- **Üniversite (Yüksek Lisans), Tübitak Bursiyeri**

Okan Üniversitesi - (Örgün Öğretim), 2019 Fen Bilimleri Enstitüsü, Bilişim Sistemleri Programı
"E-Devlet Yapısı ve Kişisel Verilerin Korunması Kapsamında Bilgi Güvenliği Farkındalığı Analizi"

- **Üniversite (Lisans),** Dokuz Eylül Üniversitesi - (Örgün Öğretim)

Bilgisayar ve Öğretim Teknolojileri Eğitimi (İngilizce), 2002

İŞ DENEYİMLERİ, PROJELER

- **ArGe** Sabancı Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Eğitimde Gizliliği Koruyan Veri Paylaşımı ve Analizi Tübitak Projesi – 2016, İstanbul
- **Eğitim Yöneticisi** MEB – 2011, İstanbul
- **Öğretim Görevlisi** İstanbul Aydın Üniversitesi – 2009, İstanbul
- **Öğretim Görevlisi** Dokuz Eylül Üniversitesi – 2004, İzmir