T.C.
POLİS AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANABİLİM DALI

BİLGİ GÜVENLİĞİ, KİŞİSEL VERİLERİN KORUNMASI VE MAHREMİYET ETKİ DEĞERLENDİRMESİ

YÜKSEK LİSANS TEZİ

Erkan AĞIRALAN

Danışman
Yrd. Doç. Dr. Yücel YİĞİT

Ankara – 2015

T.C.
POLİS AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANABİLİM DALI

BİLGİ GÜVENLİĞİ, KİŞİSEL VERİLERİN KORUNMASI VE MAHREMİYET ETKİ DEĞERLENDİRMESİ

YÜKSEK LİSANS TEZİ

Erkan AĞIRALAN

Danışman
Yrd. Doç. Dr. Yücel YİĞİT

ONAY

Erkan AĞIRALAN tarafından hazırlanan "Bilgi Güvenliği, Kişisel Verilerin Korunması ve Mahremiyet Etki Değerlendirmesi (MED)" başlıklı bu çalışma, 09./07/2015 tarihinde yapılan savunma sınavı sonucunda (~~oybirliği~~ / oyçokluğu) ile başarılı bulunarak jürimiz tarafından Güvenlik Stratejileri ve Yönetimi Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

.....

Yrd. Doç. Dr. Yücel YİĞİT (Başkan-Danışman)

.....

Yrd. Doç. Dr. Mehmet Ali TEKİNER

.....

Yrd. Doç. Dr. Mustafa YAYLA

TELİF HAKLARI BEYANNAMESİ

GÜVENLİK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Yüksek lisans tezi olarak sunduğum bu çalışmayı bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde yollama yaparak yararlandığımı belirtir; bunu şerefimle beyan ederim.

Enstitü veya başka herhangi bir mercii tarafından belli bir zamana bağlı kalmaksızın, tezimle ilgili bu beyana aykırı bir durumun tespit edilmesi durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

Tarih 05./10./.2015

İmza

Erkan AĞIRALAN

ÖNSÖZ

Yaşanan teknolojik iyileşme, e-uygulamaların yaygınlaşması, dijital teknolojideki ilerlemelerle birlikte veri ve bilgi kolayca toplanabilmekte, depolanabilmekte ve ağlar aracılığı ile bir yerden bir yere rahatlıkla iletilebilmektedir. Aynı zamanda çok kısa sürede işlenebilmekte ve illegal yollarla ele geçirilebilmektedir. Bütün bunlar birlikte düşünüldüğünde bilgi güvenliğinin sadece bireyler için değil kurum, kuruluş ve devletler için ne kadar büyük bir önem arz ettiği anlaşılmaktadır.

Diğer taraftan bireylerin kendilerini güvende hissedebilecekleri toplumların oluşturulmasında kişisel verilerin korunması büyük öneme sahiptir. Bireylerin kendilerine ait kişisel verilerin kim tarafından ve hangi amaçla kullanıldığını bilmemeleri toplumda huzursuzluk, endişe ve korku yaratır. Kişisel verilerin korunması sağlıktan ticarete, sosyal güvenlikten müşteri memnuniyetine pek çok alanda da büyük önem arz etmektedir.

Dolayısıyla kişisel verilerin korunması ve bilgi güvenliğinin sağlanması her yönüyle büyük önem arz etmektedir. Bu noktada unutulmaması gerekli olan mevzu ekonomik, siyasal ve kültürel alanda olduğu gibi bilgi güvenliği ve kişisel verilerin korunması alanında da toplumun ihtiyaçları doğrultusunda, güven ve istikrar tesis edecek doğru adımların atılmasıdır.

Bu çerçevede büyük bir özveri ile ortaya konan bu özgün çalışmanın Türkiye'de bilgi güvenliği ve kişisel verilerin korunması konusunda yeni stratejilerin oluşturulmasında karar mercilerine yol göstermesini temenni eder bu alanda çalışacak herkese yardımcı bir kaynak olmasını dilerim.

Bu çalışmanın hazırlanmasında iş yoğunluğuna rağmen benden desteğini ve yardımlarını esirgemeyen Danışmanım Yrd. Doç. Dr. Yücel YİĞİT'e, ayrıca bu süreçte bilgileri ve titiz çalışmaları ile bana yol gösteren çalışma arkadaşlarıma; son olarak büyük bir destek, sınırsız bir özveri ve fevkalade bir sabırla hep yanımda olan sevgili eşim Sibel ile bizleri yormayan sevgili oğullarımız Hakan ve Burhan AĞIRALAN'a

Teşekkürlerimle...

Erkan AĞIRALAN

Ankara, 2015

ÖZET

T.C.

Polis Akademisi

Güvenlik Bilimleri Enstitüsü

Güvenlik Stratejileri ve Yönetimi Anabilim Dalı

Bilgi Güvenliği, Kişisel Verilerin Korunması ve Mahremiyet Etki Değerlendirmesi

Hazırlayan: Erkan AĞIRALAN

Yüksek Lisans Tezi

Tez Danışmanı: Yrd. Doç. Dr. Yücel YİĞİT

2015 ve 102 (Ekler hariç)

Özellikle son zamanlarda yaşanan teknolojik iyileşme, e-uygulamaların yaygınlaşması, dijital teknolojideki ilerlemelerle birlikte veri ve bilgi kolayca toplanabilmekte, işlenebilmekte, depolanabilmekte ve ağlar aracılığı ile bir yerden bir yere rahatlıkla iletilebilmektedir. Veri ve bilgi hırsızlarının iştahını kabartan bu durum hem kişileri, hem devletleri hem de ulusal ve uluslararası kurum ile kuruluşları bilgi güvenliğinin sağlanması ve kişisel verilerin korunmasında gerekli tedbirleri almaya sevk etmektedir. Bu durumun doğal bir sonucu olarak küresel medeniyetin bilgi toplumundan mahremiyet toplumuna doğru ilerlediği ifade edilmektedir.

Bütün bu gelişmeler dikkate alındığında kişisel verilerin korunarak, bilgi güvenliğinin tesis edildiği ve mahremiyetin garanti altına alındığı güven toplumunun inşası için ortaya konan gayret ve çalışmalar yüksek bir değer taşımaktadır. Bu tezde, bilgi güvenliği ve kişisel verilerin korunması bağlamında mahremiyet etki değerlendirilmesi uygulamasının öneminin ortaya konması hedeflenmiştir. Ayrıca kişisel verilerin korunması hususunda izlenecek politika ve stratejilerin belirlenmesinde karar verici mercilere yol göstermesi, bu alanda yapılmakta olan ve yapılması planlanan reform çalışmalarına ve kurumsal oluşumlara rehberlik etmesi amaçlanmıştır.

Bu kapsamda, betimleyici araştırma yöntemi kapsamında konu hakkında ulusal ve uluslararası literatürden yararlanılarak konunun detaylı bir şekilde ele alınması sağlanmıştır. Kişisel verilerin korunması ve bilgi güvenliğinin sağlanması

çerçevesinde mahremiyet etki değerlendirmesinin yaygın bir şekilde kullanıldığı görülmüştür. Çalışmanın sonucunda Türkiye'de kişisel verilerin korunması kurumunun yanı sıra Mahremiyet Üst Kurulunun kurulması ve bu kurul altında mahremiyet uzmanlarının görev aldığı komisyonların oluşturulmasının gerektiğini ifade edilmiştir. Ayrıca gerekli yasal düzenlemelere paralel olarak kamu kurumlarında Mahremiyet Etki değerlendirme Birimlerinin de oluşturulmasının kişisel verilerin korunmasında önemli olduğu belirtilmiştir.

Anahtar Kelimeler: Kişisel Verilerin Korunması, Bilgi Güvenliği, Bilgi Güvenliği Yönetim Sistemi, Mahremiyet, Mahremiyet Etki Değerlendirmesi.

ABSTRACT
Police Academy
Institute of Security Sciences
Department of Security Strategies and Management
Information Security, Personal Data Protection and Privacy Impact Assessment
Erkan AĞIRALAN
Master's Thesis
Supervisor: Yrd. Doç. Dr. Yücel YİĞİT
2015 and 102 (Excluding appendices)

Especially, with the advent of recent technological improvement, widespread of e-applications and advances in digital technology, data and information can be collected, processed, stored and with the help of networks transmitted easily from one place to another place. This situation, which increases data and information thieves' appetite, dispatches people, states, as well as national and international institutions and organizations in order to take the necessary measures in the protection of personal data and providing information security. As a natural result of this situation it is expressed that global civilization progress from the information society towards the privacy community.

When all these developments are taken into account it can be said that all work and efforts have a great value in the establishment of confidencial society in which personal data are protected, information security is provided and privacy is guaranteed. In this thesis, it is aimed to reveal the importance of the privacy impact assessment application especially in the context of information security and protection of personal data. Also, it is aimed to create a course of action for decision and policy makers about determination of policies and strategies to follow in the framework of information security and personal data protection law and reform.

In this context, with the application of descriptive research method the topic was embraced in detail by making use of national and international literature about the topic. In the framework of personal data protection and information security, it was realized that privacy impact assessment has been used broadly. In the conclusion of this study, it is said that in addition to the Institution of Personal Data Protection in Turkey, establishment of the Supreme Board of Privacy and forming commissions

employing privacy experts under this Supreme Board is vital. Besides, it was stated that, in parallel with required legislation, constituting the Privacy Impact Assessment Units in public institutions is significant in protection of personal data.

Key Words: Personal Data Protection, Information Security, Information Security Management System, Privacy, Privacy Impact Assessment.

BİLGİ GÜVENLİĞİ, KİŞİSEL VERİLERİN KORUNMASI VE MAHREMİYET ETKİ DEĞERLENDİRMESİ

İÇİNDEKİLER

KISALTMALAR LİSTESİ

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AU	Afrika Birliği
BGYS	Bilgi Güvenliği Yönetim Sistemi
BM	Birleşmiş Milletler
BSI	British Standards Institute
ÇED	Çevresel Etki Değerlendirmesi
DARPA	The Defense Advanced Research Projects Agency
DEA	Düzenleyici Etki Analizi
EPTA	Avrupa Parlemantosu Teknolojik Değerlendirme
ET	Erişim Tarihi
GZFT	Güçlü Yanlar-Zayıf Yanlar-Fırsatlar- Tehditler
ILO	Uluslararası Çalışma Örgütü
ISO	Uluslararası Standartlar Kurumu
MED	Mahremiyet Etki Değerlendirmesi
MÖ	Milattan Önce
OECD	İktisadi İşbirliği ve Kalkınma Teşkilatı
OKDS	Otomatik Karar Destekleme Sistemlerinin
SÇED	Stratejik Çevre Etki Değerlendirmesi
SED	Sosyal Etki Değerlendirmesi
SGK	Sosyal Güvenlik Kurumu
TBMM	Türkiye Büyük Millet Meclisi
TDK	Türk Dil Kurumu

TABLOLAR LİSTESİ

GİRİŞ

İnsanoğlu doğası gereği zenginlik kaynaklarını elinde bulundurmak ister. Her çağda ekonomik değeri yüksek altın, petrol, su gibi farklı zenginlik kaynakları olmuştur. Günümüz dünyasında ise en önemli ve ekonomik değeri en yüksek olan zenginlik kaynağı hiç kuşkusuz bilgi ve veridir. Günümüz bilgi çağı olup sadece devletler değil artık ulusal ve uluslararası kurum ve kuruluşlar bu bilgi ve verilere ulaşma gayretini ortaya koymaktadır. Bu alanda oluşan rekabet ülkeleri yasa dışı yollara başvurmaya kadar sürüklemiştir. Son yıllarda ortaya çıkan ülkeler arası dinleme krizleri ya da WikiLeaks olayında bu anlatılanlar somut bir şekilde gün yüzüne çıkmıştır.

Bilginin ve verinin bu kadar değerli olduğu bir ortamda en önemli husus bu kaynakların toplanması, korunması ve gerektiğinde yok edilmesidir. Elbette bu süreç insan haklarının temel unsurlarından olan kişisel hakları ihlal etmeden gerçekleştirilmelidir. Özellikle kişisel veriler bireylerin mahrem alanının oluşturduğundan mahremiyet ihlali kurum, kuruluş ve devletlere olan güveni derinden sarsarak toplumu sosyal, ekonomik ve politik açıdan etkiler. Bu noktada Mahremiyet Etki Değerlendirmesi (MED) kişisel verilerin korunması, bilgi güvenliğinin sağlanması ve mahremiyet ihlalinin önlenmesinde önemli bir araç olarak ortaya çıkmaktadır.

Bilgi güvenliği ve kişisel verilerin korunması çerçevesinde MED'in ele alındığı bu tezde, günümüzde pek çok gelişmiş ülke tarafından uygulanan MED'in öneminin ortaya konması hedeflenmektedir. Ayrıca Ülkemizde kişisel verilerin korunması hususunda, bilgi güvenliği çerçevesinde izlenecek politika ve stratejilerin belirlenmesinde karar verici mercilere yardımcı olacak bir yol haritasının oluşturulması amaçlanmaktadır. Bunun yanı sıra, ulusal literatürde MED alanında yapılan yeterli düzeyde çalışmalara rastlanamadığından, bu çalışmanın bu alanda araştırmalar yapacak diğer kişilere de kaynak oluşturması hedeflenmektedir. Böylelikle konu hakkındaki ulusal literatürün zenginleşmesine katkı yapılacağı düşünülmektedir.

Kişisel verilerin korunması kanununun yasallaşması ile başlayacak süreçte, kurum, kuruluş ve organizasyonlarca yapılacak proje, izlenecek politika ve stratejilerin bilgi güvenliği ve kişisel/ kurumsal mahremiyet bağlamında sağlıklı bir şekilde tesis edilmesinde yol gösterici bir çalışma da olması tezin önemini ortaya koymaktadır. Ayrıca, ulusal ve uluslararası literatürdeki materyallerden yararlanılan bu çalışmada özellikle MED başlığı altında ulusal kaynakların az olmasından dolayı yabancı kaynaklardan istifade edilmiştir. Bu noktada OECD, AB ve ILO gibi çeşitli uluslararası kuruluşların konu hakkındaki yayınlamış olduğu eserlerden yararlanılmıştır.

Bunların yanında, kişilerin verilerin korunması ve bilgi güvenliği alanında Avrupa Konseyi 108 Sayılı Sözleşmesi, Avrupa Birliği 95/46/EC Sayılı Direktifi, Avrupa Birliği Temel Haklar Şartı gibi uluslararası yasal metinlerin yanı sıra, ülkemizde de T.C. Anayasası, Türk Medeni Kanunu, Borçlar Kanunu ve Türk Ceza Kanunu gibi yasal düzenlemelerden de yararlanılmıştır. Ulusal ve uluslararası literatür taramasında da EBSCO, Ulakbim, ELSEVIER gibi veri tabanlarından faydalanılarak hakemli yayınlara ulaşılmıştır.

Bu çerçevede hazırlanan çalışmanın ilk bölümünde kişisel veri kavramı, korunması, kişisel verilerin korunmasında izlenecek temel ilkeler, uluslararası düzenlemelerde kişisel verilerin korunması ve Türkiye'deki durum ele alınmıştır. Bilgi güvenliği ve bilgi güvenliği yönetim sisteminin ele alındığı ikinci bölümde ise bilgi güvenliği ilke ve parametreleri ile tarihsel süreç içerisindeki gelişimi anlatılmıştır. Bu bölümün devam eden kısımlarında ise bilgi güvenliği yönetim teorilerinin yanı sıra bilgi güveliği yönetiminde yapılan hatalar ve tehditler işlenmiştir. Üçüncü bölümde mahremiyet kavramı ele alınmış, mahremiyet yönetimi üzerinde durduktan sonra çalışmanın esas konusu olan MED'e geçilmiştir. MED'in ortaya çıkışı, tarihsel gelişimi, unsurları, faydaları, aşamaları gibi konulara değinilmiştir. Bu bölümün son kısmında ise farklı MED uygulamaları ve gelecekteki MED uygulamalarındaki beklentiler ele alınmıştır.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ VE KİŞİSEL VERİLERİN KORUNMASI

İçinde yaşadığımız dönemde teknolojik ilerlemeler ve baş döndürücü hızda gerçekleşen değişimlerle birlikte dünyanın küresel bir köy haline geldiği ifade edilmektedir. Zamanın durduğu, mekân ve sınırların neredeyse ortadan kalktığı bu durumun doğal bir sonucu olarak insanlar, maddeler ve hizmetler arası akış hızında bir artış gözlenmektedir. Daha açık bir ifade ile bir olay, bir haber, sosyal bir durum, veriler kısa bir zaman diliminde hatta bazen anlık olarak dünyanın bir ucundan diğer ucuna iletilebilmektedir. Bütün bu hareketlilik ve hızın kaçınılmaz bir sonucu olarak ortaya çıkan veri miktarında da ciddi bir artış gözlemlenmektedir. Bu verilerin önemli bir kısmı kişilere aittir ve çeşitli açılardan diğer verilerden ayrışır. Bu noktada ise kişisel verilerin veri yumağından ayrıştırılabilmesi büyük önem arz etmektedir. Sağlıklı bir ayrışma için gereklilik arz eden en önemli husus kişisel verinin tanımının yapılmasıdır. Bu kapsamda kişisel verinin tanımının yapılmasının ardından, dünyada ve ülkemizde kişisel verilerin korunmasına ilişkin mevzuatsal düzenlemeler de incelenecektir.

1.1 KİŞİSEL VERİ; TANIM VE KAVRAMLAR İLE KİŞİSEL VERİLERİN KORUNMASI HAKKI

Yeni bir kavram olan kişisel veri özellikle son yüzyılda meydana gelen teknolojik ilerlemenin etkisiyle üzerinde sıklıkla durulan fakat tanımında mutabakat sağlanamayan bir olgudur. Literatürde yer alan tanımlardan bir kısmı doğrudan doğruya kişisel verinin ne olduğunu anlatırken bazı tanımlamalarda bir veriyi kişisel veri yapan unsurlar teker teker açıklanarak dolaylı bir tanımlama yapılmaktadır. Örneğin İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından kabul edilen ve kişisel verilerin korunmasını konu alan uluslararası alanda ilk resmi belge niteliğini taşıyan "Kişisel Verilerin Sınır Aşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri" başlıklı eserin birinci maddesinde kişisel veri "belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgiler" şeklinde tanımlanmıştır (Murray,

1997: 948). 1980 yılında OCED belgelerinde yapılan bu tanımlamanın yanı sıra Avrupa Birliği (AB) resmi dokümanlarında da çeşitli tanımlamalar yapılmaktadır. Avrupa Komisyonu'nun 95/46/EC sayılı direktifinin 29. maddesi çerçevesinde oluşturulan dokümanda kişisel verinin tanımı dört unsurun tanımı üzerinden gidilerek yapılmıştır. Bu dört unsur sırasıyla; herhangi bir bilgi, ilişkin/ilişkili olma, tanımlanan ya da tanımlanabilir olma ve gerçek kişi olmadır (Ünsal, 2013: 99). Benzer şekilde 12.12.2012 tarihli raporda Bilgi Komiser Ofisi tarafından yapılan tanımlama da öncelikle unsurların tanımlanması ve bu unsurların aşama aşama oluşturulan sorulara verilen cevaplarla şekillenmesi yöntemine dayanmaktadır. Daha açık bir ifade ile öncelikle ortada bir bilgi var mı yok mu sorusuna cevap aranmakta, daha sonra bu bilginin gerçek kişiye ait olup olmadığı sorgulanmaktadır. Bu şekilde birkaç soruya verilen yerinde cevaplarla kişisel verinin var olup olmadığı ortaya konulmaktadır (The Information Commissioner's Office, 2013).

Ülkemizde ise hali hazırda kişisel verilerin korunmasına ilişkin yasal bir düzenleme olmamakla birlikte son yıllarda artarak devam eden yoğun çalışmalar neticesinde Başbakanlığa sunulan taslak metinde kısa bir tanımlama yapıldığı görülmektedir. Taslak metnin 3. maddesinde yer alan tanıma göre kişisel veri "belirli veya belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler" olarak tanımlamaktadır (Kanun Taslağı m. 3/a). Bu çalışmanın tamamlandığı süre zarfında hazırlanan bu kanun tasarısının Türkiye Büyük Millet Meclisi'nin (TBMM) gündeminde olduğu görülmektedir (Güler ve Ergül, 2014).

Farklı şekilde tanımlanabilen kişisel veri; bir kişiyi belirleyen ya da makul bir yöntem kullanılarak bir kişinin belirlenmesini sağlayan veya dolaylı olarak kişiyi belirleyen veri ve bilgilerle bağlantısı olan bütün diğer veriler olarak tanımlanabilir. Bu tanımlardan da anlaşılacağı üzere kişinin ismi, adresi, kimlik numarası, doğum tarihi, telefon numarası ve fotoğrafı birer kişisel veri olarak tanımlanabilmektedir.

Esas olarak kişisel veri sınıfına giren diğer bir kavram ise hassas veridir. Genellikle kişisel veri ile karıştırılan hassas veri; kişisel veri içerisindeki kişiliğe ait sosyal verileri içeren ve kişinin yaşam tarzı, inançları, değerleri gibi konularda özel bilgileri barındıran verilerdir. AB Veri Koruma Yönergesinde ırksal ve etnik köken,

siyasi görüş, dini ve felsefi inanç, sendika üyeliği, sağlık durumu ve cinsel yaşam olarak sıralanan hassas verinin içeriği itibari ile işlenmesi, ifşa edilmesi toplumsal barış ve huzur açısından ciddi sıkıntılar yaratabilecektir (Civelek, 2011:21).

Yukarıdaki kısımda genel hatlarıyla ve kısaca açıklanan kişisel verinin korunması hukuk devletinin, kişisel hak ve hürriyetlerin vazgeçilmez olduğu idari yönetimlerin üzerinde durduğu hususların başında gelmektedir. Pek çok platformda ele alınan kişisel verilerin korunmasının farklı açılardan oldukça fazla yararı gözetilmektedir. Bu noktada kişisel verilerin korunmasının önemi aşağıda işlenmektedir.

1.2 KİŞİSEL VERİLERİN KORUNMASININ ÖNEMİ VE NEDENLERİ

Bireylerin kendilerini güvende hissedebilecekleri toplumların oluşturulmasında kişisel verilerin korunması büyük öneme sahiptir. Bireylerin kendilerine ait kişisel verilerin kim tarafından ve hangi amaçla kullanıldığını bilmemeleri toplumda huzursuzluk, endişe ve korku yaratır. Kişisel verilerin korunması sağlıktan ticarete, sosyal güvenlikten müşteri memnuniyetine pek çok alanda da büyük önem arz etmektedir. Bu önemin daha iyi anlaşılabilmesi, daha somut şekilde ortaya konabilmesi için kişisel verilerin korunmasının nedenlerinin bilinmesinin yararlı olacağı düşünülmektedir. Bu bağlamda kişisel verilerin korunmasının arkasında yatan temel nedenlerden önemli olanlara aşağıda yer verilmiştir.

1.2.1 Ekonomik ve Ticari Gelişmeler

Kişisel verilerin korunmasının arkasında yatan nedenlerin başında ekonomik, sosyal ve ticari gelişmeler gelmektedir. Ekonomik alanda para, mal ve hizmet dolaşımının her geçen gün biraz daha ile ilerlediği görülmektedir. Avro ve dolar gibi ortak para birim kullanım eğiliminin artması, genel olarak kişi başına düşen gelirin artması, ekonomik iyileşmeler gibi olumlu unsurların yanı sıra ülkeden ülkeye hızla yayılabilen ekonomik krizler, iktisadi durgunluklar ve mali çalkantılar gibi negatif hususların etkisinin hızlı bir şekilde toplumdan topluma yayıldığı bilinmektedir. Böyle bir konjonktürde ekonomik anlamda yapılan para, zaman ve gayret harcamalarının hak etmiş olduğu değeri elde etmesi için ekonomik sistemin

vazgeçilmez unsuru olan kişisel verilerin korunması büyük önem arz etmektedir (Hermalin ve Katz, 2006).

Benzer şekilde ticari alanda meydana gelen değişiklikler ve oluşan hızlı dönüşümlerle birlikte kişisel verilerin korunmasının büyük önem arz ettiği görülmüştür. Ticari alanda finansal kayıpların azaltılması, yüksek seviyedeki üretimin devam etmesi, yeni düzenlemelere uyum sağlanabilmesi ve müşteri beklentilerinin karşılanabilmesi gibi nedenler kişisel verilerin korunmasını gerekli kılmaktadır. Kişisel verilerin kaybolması ticari alanda doğrudan finansal kayba neden olabilmektedir. Daha açık bir ifade ile verilerin yok olması durumunda idari para cezaları gibi doğrudan mali kayıplar açığa çıkabildiği gibi, yatırımcıların firmaya olan güveninin kaybolması ya da müşterilerin güven eksikliği gibi nedenlerle rakip firmalara kayması durumlarında olduğu gibi dolaylı olarak da finansal kayıplar oluşabilmektedir (Gellman, 2002).

Ticari alanda kişisel verilerin korunmasını gerekli kılan diğer bir neden ise ulusal ya da uluslararası alanda yapılan ticari düzenlemelerdir. Birden çok ülkede aynı anda faaliyet gösteren uluslar üstü firmaların yaygınlaşması, elektronik iletişimin hızlanması, e-para uygulamalarının yaygınlaşması ve internet üzerinden yapılan ticaretin gelişmesi gibi nedenlerin bu alanlarda yeni yasal düzenlemeleri de beraberinde getirdiği bilinmektedir. Bu çerçevede ortaya konan düzenlemeler firmaların hangi verileri alabileceklerini, ne kadar ve nasıl muhafaza edeceklerini, bu verileri ne kadar süre ve hangi şartlar altında kullanabileceklerini düzenlemektedir. Dolayısıyla fiziksel ticari sınırların neredeyse kalktığı, dünyanın bir ucundan yapılan harcamaların başka bir ucundan anlık olarak izlenebildiği, saniyeler içerisinde bir tuşla yüklü para transferlerinin gerçekleştirilebildiği böyle bir ticari ortam kişisel verilerin korunmasını zorunlu kılmaktadır.

Yasal düzenlemeler kadar önemli olmamakla birlikte ticari alanda verilerin korunmasını gerekli kılan diğer bir neden ise üst seviye üretimin devam etmesidir. Doğrudan isim olarak bilinmese de kümülatif olarak ticari alandaki bir ürün ya da hizmete yönelik arz ve talebin bilinmesi üretimde verimlilik ve sürekliliği beraberinde getirir. Bu noktada ticari verilerin ya da kişisel verilen kaybolmasının

üretimde sürekliliği sekteye uğratacağı, arz talep dengesini bozarak maddi kayba neden olacağı ortaya konmaktadır (Acquisti, 2004).

Elektronik ticaretin hızla yayıldığı, ticari aktörlerin birbirlerine sıkı bağlarla bağlandığı günümüz ticari alanında müşteri beklentilerinin her gün değişerek arttığı görülmektedir. Ticaretin odak noktasını oluşturan müşteri memnuniyetinin sağlanması temelde güvene dayanmaktadır. Bir bilgisayar sisteminde milyonlarca müşterinin verisinin olması ve buradan birkaç tuşla geniş hacimli işlemlerin gerçekleşebiliyor olması firmaları veri güvenliği hususunda her zamankinden daha dikkatli olmaya zorlamaktadır. Sadece e-ticaret uygulamalarıyla sınırlı olmayan bu durumun geçerliliği borsada da kabul görmektedir (Beales, 2010).

1.2.2 Sosyal Ağların Yaygınlaşması

Ekonomik ve ticari alanda olduğu gibi sosyal alanda da açığa çıkan değişimin kaçınılmaz bir sonucu olarak kişisel verilerin korunmasının bir zaruret arz ettiği söylenmektedir. Sosyal ağlarda kişilere yönelik oluşturulan tahribatın etkisi, olumsuz bir algının kişide açmış olduğu yaranın derinliği çok büyük olmakta ve kolay kolay silinememektedir. Bilhassa twitter, facebook gibi sosyal ağların yaygınlaşması buralardan kişisel verilerin kötü niyetli sosyal ağ hırsızı kişiler tarafından amacı dışında kullanılması kişisel verilerin korunmasına yönelik yeni tedbirlerin alınmasını gerekli kılmaktadır. Akıllı cep telefonlarının insan hayatında kullanımının artması ile birlikte kişiler bu sosyal ağlarda meydana gelen gelişmeleri takip edebilmekte, anında müdahil olabilmektedir. Kısacası bu çemberde yer alan her bireyin sosyal ağda, fiziksel olarak belki hiç tanımadığı binlerce, hatta milyonlarca kişiyle etkileşim içinde olan birer elektronik izdüşümünün oluştuğu varsayılmaktadır. Böylesine geniş bir sosyal ortamda kişisel verilerin korunması gerekmektedir. Ayrıca bu sosyal ağlarda veri dolaşımı oldukça hızlıdır. Dolayısıyla bu alanda da kişisel verilerin muhafaza edilmesi ayrı bir önem taşımaktadır (Organisation for Economic Co-Operation and Development, 2010).

1.2.3 Sağlık Teknolojilerindeki İlerlemeler

Özellikle 2000'li yıllarından başından bu yana sağlık sektöründe hızlı ve keskin değişimler yaşanmaktadır. Hastane ve eczaneler başta olmak üzere bu sektörde sağlık

hizmeti sunanların kâğıt esaslı çalışma ortamından elektronik ortama yönelik geçiş yaptıkları görülmektedir. Medikal kayıtlardan sağlık sigortasına, alınan tedaviler ve ilaçlara kadar pek çok sağlık bilgisi artık elektronik ortamda tutulmaktadır. E-reçete, e-rapor gibi uygulamalar neticesinde kâğıt ortamındaki bilgiler elektronik ortama taşınmaktadır. Sağlık kartlarının geride kaldığı dönemlere nazaran içinde bulunulan zamanda avuç içi damar izi gibi değiştirilmesinin dahi zor olduğu bilgilerin tamamı elektronik ortamlarda yer alır hale gelmiştir. Yüksek tutarlarda işlem hacimlerinin gerçekleştiği, sağlık harcamaların her yıl arttığı böyle bir ortamda kişisel verilere toplu olarak kısa sürede ulaşmak mümkün hale gelmiştir (Hermalin ve Katz, 2006).

Elektronik ortamda kişisel verileri elde eden kötü niyetli kişiler tarafından sahte e-reçetenin yazıldığı, raporların düzenlendiği tespit edilmektedir. Bu noktada üzerinde durulması gerekli olan diğer bir husus ise sadece hastaların değil aile hekimi, doktor, eczacı gibi sağlık hizmet sunucularına ait kişisel verilerin korunmasının da zorunlu olduğudur. Sağlık hizmet sunucularının kişisel verileri, şifreleri elde edilerek yapılan dolandırıcılığın maliyeti oldukça yüksek olarak tahmin edilmektedir. 2012 yılı içerisinde yapılan çalışmalarda Amerikan vatandaşlarından yaklaşık 1,85 milyon kişinin sağlık verilerinin çalındığını ve çalınan bu verilerin kişi başına ortalama maliyetinin 22 Dolar 346 Sent, toplam maliyetinse 41.3 milyar Dolar civarında olduğunu ortaya konmuştur (Ponemon Institute, 2012).

Sağlık ekonomisi alanında faaliyet gösteren firmalar arası rekabet de kişileri yasal yollarla elde edilemeyen verilerin illegal şekillerle elde edilmesine yönlendirmektedir. Ar-Ge harcamalarının her geçen gün arttığı bir ortamda yatırımların doğru yerlere yapılması için firmalar da hasta verilerine ihtiyaç duymaktadır. Son zamanlarda ortaya konan raporlar sağlık ve medikal hırsızlığın arttığını ve bu eğilimlerin yükseleceğini göstermektedir (Organisation for Economic Co-Operation and Development, 2013). Bu hırsızlık ve yolsuzluğun önüne geçmek için özellikle alt yapı yatırımlarına önem verilmektedir. Örneğin ABD'de 2009 yılında hazırlanan kanun çerçevesinde Sağlık Bilgileri Teknolojisi için 20 milyar Dolar altyapı yatırımının yapılması kararlaştırılmıştır.

1.2.4 Verinin Ticari Meta Haline Dönüşmesi

Rekabetin arttığı, dünyanın küresel bir pazar haline geldiği piyasalarda firmalar yatırımlarını doğru bir şekilde yönlendirmek, karlarını artırmak ve maliyetlerini düşürmek gibi nedenlerle ayrı bir Ar-Ge bütçesi oluşturmaktadır. Sağlık, ulaşım, kozmetik başta olmak üzere pek çok farklı farklı alanda tüketici profilinin ortaya konarak piyasada doğru adımların atılmasının firmaların rekabet güçlerini artırdığı ve karını yükselttiği görülmüştür. Temel dinamiklerinin rekabet üzerine kurulduğu piyasalarda doğru ve sağlıklı verilerin elde edilmesi büyük önem arz etmeye başlamıştır. Bu durumun doğal bir sonucu olarak kişisel verilerin ticari bire meta haline geldiği bilinmektedir. Firmalar daha fazla kar elde etme, rekabet piyasasında üstün olma gibi nedenlerle kişisel verileri elde etme uğrunda illegal yollara da başvurur hale gelmiştir. Bu çerçevede kişisel verilerin güvenli bir şekilde muhafaza edilmesi kaçınılmaz hale gelmiştir (European Commission, 2010).

1.2.5 Bilim ve Teknik Alanlardaki Yenilikler

Kişisel verilerin korunmasını gerekli kılan bir diğer neden ise bilim ve teknik alanlarında meydana gelen yeniliklerdir. Bu alanlardaki yenilikler sayesinde bilgisayar ortamına aktarılmaya başlanan veriye ulaşmak için fiziksel olarak aradaki mesafe önemsiz bir hal almıştır. Örneğin, dünyanın bir ucunda küçük bir köyde ikamet eden bir kişi illegal bir yolla bir firmanın, bir kurumun ya da bir ülkenin bilişim sistemini felce uğratabilmektedir. Siber saldırılarla ya da farklı yöntemlerle çok kısa bir sürede milyonlarca kişinin verilerine ulaşarak maddi ve manevi tahribatlı büyük zararların doğmasına neden olunabilir. Elli yıl kadar önce sadece istihbarat birimlerinin yoğun çalışmalarla ulaşabileceği kişisel bilgilere artık facebook ya da twitter gibi sosyal ağ sitelerinden ulaşılabilmektedir.

Kısacası yukarıdaki başlıklarda da değinildiği üzere, kişisel verilerin korunmasının nedenlerinin temelinde aslında bilim ve teknik alandaki yeniliklerin yattığı ifade edilebilir. Dolayısıyla verilerin çalınması, yasal olmayan bir amaç doğrultusunda işlenmesi, ticari bir meta olarak alınıp satılması gibi nedenler kişisel verilerin korunmasını zorunlu kılmaktadır. Bu çerçevede oluşacak bir veri hırsızlığı ve dolandırıcılığının yüksek tutarda finansal maliyeti olmaktadır. Örneğin 2006

yılında ABD'de gazilere ait kişisel verilerin bulunduğu bir dizüstü bilgisayarın çalınması sonucu Gazi İşlemlerin Kurumu gazi ve askeri personele 20 milyon dolar ödemek zorunda kalmıştır. Çalınan bu verilerin kötü niyetle kullanıldığının ispatı dahi yapılamamış olmasına rağmen kurumun katlanmak zorunda olduğu finansal yük oldukça büyüktür. Benzer şekilde Avrupa Sağlık Hizmetleri Dolandırıcılık ve Yolsuzluk Ağı tarafından hazırlanan rapora göre AB ülkeleri tarafından vatandaşlara sunulan sağlık hizmetleri için ayrılan 1 trilyon Avroluk bütçenin yaklaşık yıllık 56 milyar Avrosu yolsuzluk ve dolandırıcılık sonu erimektedir. Bu rakam dünya genelinde 180 milyar Avroya ulaşmaktadır.

1.3 KİŞİSEL VERİLERİN KORUNMASINDA İZLENECEK TEMEL İLKELER

Genel olarak bir süreç olarak ortaya konan kişisel verilerin korunmasında tavsiye edilen çeşitli süreçlerden bahsedilmektedir. Yapılan uluslararası literatür taramasında AB tarafından hazırlanan direktif ya da yasal düzenlemelerde, OECD tarafından hazırlanan metinlerde ve farklı ülkelerce uygulanan düzenlemelerde kişisel verilerin korunması sürecinde farklı ilkelerden bahsedildiği görülmektedir (Cate vd., 2014). Bu ilkeler bazı metinlerde yedi, bir takım makale ve kaynaklarda sekiz ilke olarak ele alınmaktadır. OECD tarafından 1980 yılında ortaya konan ilkeler şöyle sıralanabilir; veri toplamanın sınırlı olması, veri kalitesi, amacın belirliliği, verinin kullanımının sınırlı olması, verinin güvenliği, açıklık, bireyin katılımı, hesap verebilirlik (Organisation for Economic Co-Operation and Development, 2013). Bu çalışma kapsamında ise farklı kurum ve düşünürler tarafından farklı zamanlarda ortaya konan ilkeler dört ana kategori altında ele alınmıştır.

1.3.1 Hukuki İşlem İlkesi

Kişisel verilerin korunması ilkelerinin ilki ve en önemlilerinden biri hukuki işlem ilkesidir. Esasında diğer ilkeler çerçevesinde atılacak adımların yasal dayanağının olması ve meşru çerçevede kişisel verilerin korunmasının sağlanması dolaylı da olsa temelde bu ilkeye dayanmaktadır. Bu ilke kapsamında toplanacak verilerin yasal bir zemine dayandırılması, yine yasal bir çerçevede kullanılması, depolanması ve yok edilmesi amaçlanmaktadır. Kuralların ve kanunların ihlali durumunda başvurulacak

uygulama ve yaptırımların da neler olduğu bu ilke kapsamında açıkça ifade edilmektedir. Yine bu ilke doğrultusunda demokratik zeminde özel hayatın gizliliği ve ihlal edilemezliği hazırlanacak kanuni metnin de sınırlarını belirlemektedir. Kamu yararının ve bireylerin haklarının öncelikli olduğu toplumlarda hazırlanacak olan kişisel verilerin korunmasını amaçlayan kanun ve düzenlemelerde hukuki işlem ilkesi gereğince meşru bir amaç hedeflenmekledir. Ayrıca bu ilke gereğince kişisel verileri talep etmeye, toplamaya, kullanmaya ve yok etmeye yetkili kılınan birim ve kurumlara yönelik olarak kişilerden ihtiyaç duyulan oranda ve içerikte veri toplamaları hususunda düzenlemelerin getirilmesi gerektiği ortaya konmaktadır. Diğer taraftan kişilerin rızası da bu ilkenin önemli unsurlarından biri olarak kabul edilmektedir. Kişilerin bilgisi ve rızası olmadan verilerin toplanması ve kullanılması büyük sakıncalar barındırmaktadır. Bu sakıncaların başında hukuki düzenin zedelenmesi gelmektedir (Council of Europe, 2014).

1.3.2 Veri Kalitesi İlkesi

İlkelerden bir diğeri olan veri kalitesi ilkesinin daha ziyade verilere ilişkin olduğu görülmektedir. Bu ilke kapsamında öncelikli olarak ilgili verilerin toplanmasının gerekli olduğu hususu vurgulanmaktadır. Toplanan bu verilerin güncel olması ve gerekli durumlarda güncellenebilmesi gerektiği ileri sürülmektedir. Yine bu ilke kapsamında toplanan verilerin doğru ve amacına uygun şekilde kullanılmasının önemli olduğu belirtilmektedir. Veri kullanım esnasında gerekli veriye ilişkin gerekli kontrollerin yapılması ve kullanıldıktan sonra verilerin kısa sürede silinmesi de bu ilke çerçevesinde gerçekleşmektedir. Bütün bunların yanı sıra verileri elde tutma hakkının sınırlandırılması gerektiği hususu da veri kalitesi ilkesinin doğal bir yansıması olarak açığa çıkmaktadır (European Commission, 2012).

1.3.3 Adil İşleme İlkesi

Üçüncü ilke, kişisel verilerin işlenmesine yönelik adil işleme ilkesidir. Bu ilke temelde veri sahibi ile kişisel veriyi işleyecek kullanıcı arasındaki ilişkiye dayansa da şeffaflık hususu ön planda yer almaktadır. Şeffaflık ile hangi verilerin işleneceği, hangi amaçla, ne zaman ve kim tarafından işleneceği veri sahibine bildirilir. Veri işleme esnasında kanunun özel izni dışında herhangi bir işlem yapılmayacağı kabul

edilir. Adil işleme ilkesi çerçevesinde üzerinde durulan diğer bir husus da taraflar arasında güven tesisidir. Bu noktada veri işleyecek olanlar veri sahibine yazılı olarak gerekli dokümanları sağlamakla mükelleftirler. Aksi bir durum yoksa kullanım amacındaki sınırlar kullanıcılar tarafından aşılamaz. Aksi takdirde öngörülen yaptırımların uygulanacağı bildirilmektedir. Ayrıca bu ilke kapsamında veri sahibi kişiler istedikleri zaman işleme sürecinde verilerine ulaşabilmektedirler (Council of Europe, 2014).

1.3.4 Hesap Verebilirlik İlkesi

Veri öznelerinin veri işleyicilerine karşı yukarıdaki ilkeler çerçevesinde hesap sorabilmelerinin gerekliliği bu ilkenin kabul görmesinin önemli nedenlerinden biri olarak açığa çıkmıştır. Hesap verebilirlik veri işleme esnasında güven ve sağlamlığın sağlanması amacıyla işleyici tarafından aktif bir şekilde başvurulması gerekli olan bir ilkedir. İşleme esnasında gerekli önlemlerin alınması ve talep edildiği zaman anında yapılan iş ve işlemlerin önceden belirlenmiş olan kural ve yasalara uygun olduğunu gösterir belgenin ibraz edilmesi veri işleyenin sorumluluğundadır. Talep edildiğinde yapılan işlem ile yasalar arasındaki uygunluğun gösterilmesi gerekmekte olup bu sorumluluk veri işleyene aittir. Ayrıca diğer ilkelere uygunluğun sağlanmasından da hesap verebilirlik ilkesi gereğince verileri işleyen sorumludur (Organisation for Economic Co-Operation and Development, 2013) .

Yukarıda da görüldüğü üzere farklı ülke, kurum ve uluslararası kuruluşlar tarafından farklı ilkeler benimsenmekle birlikte temel olarak bu ilkeler dört kategoride ele alınabilmektedir. Bunlardan ilkinin hazırlık sürecine, ikincisinin kişisel veriye, üçüncüsünün bu verilerin işlenme sürecine ve dördüncüsünün ise süreç sonrasındaki sorumluluğa yönelik olduğu ifade edilebilir.

1.4 ULUSLARARASI DÜZENLEMELERDE KİŞİSEL VERİLERİN KORUNMASI

Gelişen teknolojiye paralel olarak başvurulan yeni uygulamalarla birlikte başta uluslararası kuruluşlar olmak üzere pek çok ülkenin kişisel verilerin korunması hususunda ve bilgi güvenliği çerçevesinde yeni yasal dayanaklar oluşturmaya başladıkları görülmektedir. Bu bağlamda kişisel hak ve özgürlüklere yüksek düzeyde

önem veren demokratik ülkelerde ve uluslararası kuruluşlarda gerekli adımlar atılmaktadır. Bu kısımda uluslararası düzenlemelerden bir kaçına değinilecektir.

1.4.1 Avrupa Konseyi 108 Sayılı Sözleşmesi

Uluslararası arenada bağlayıcılığı olan ilk düzenlemenin Avrupa Konseyi tarafından 1981 yılında çıkarılan "*Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair*" 108 sayılı Sözleşmesinin olduğu bilinmektedir (Sevimli, 2006). Avrupa Konseyi bu Sözleşmeyi 28 Ocak 1981 tarihinde hazırlamıştır. Hazırlanan bu sözleşme üye devletlerce imzalanmıştır. Türkiye de bu sözleşmeyi 1985 yılında imzalamıştır. Avrupa Konseyi tarafından yürürlüğe konan 108 sayılı Sözleşme üye devletleri bağlayıcı niteliktedir.

Bu sözleşme, imzası bulunan ülkelerin iç hukuklarında geçerlilik kazanmakla kalmamış aynı zamanda ülkelerin pek çoğu kendilerine ait gerekli yasal düzenlemeleri yapmıştır. Ülkemizde ise gerekli yasal zeminin olmaması nedeniyle sözleşme uygulanmamaktadır. Sözleşmenin temel gayesinin üye ülkelerde yaşayan herkesin kişisel verilerinin otomatik bilgi işlemeye tabi tutulması karşısında özel yaşam haklarını, temel hak ve özgürlüklerini güvence altına alarak toplumsal refah ve güveni yükseltmek olduğu söylenebilir. Bu çerçevede üye devletlerdeki gerçek kişilerin uyrukları, vatandaşı olduğu ülke ya da ikametgâhlarının önemli olmadığı bir anlayışın sergilendiği görülmektedir (Greenleaf, 2008:3).

1999 yılında Sözleşmede bazı değişiklikler yapılmıştır. Bu değişikliklerle birlikte ele alındığında sözleşmenin kişisel verilerin meşru ve yasal yoldan elde edilmesini ve işlenmesini talep ettiği ifade edilebilir. Aynı zamanda doğru ve güncel verilerin aşırıya gidilmeden talep edilmesi, işlenmesi ve belirli bir zaman sonra yok edilmesi gerektiği hususlarına da sözleşmede yer verilmektedir. Genel olarak yukarıda sayılan temel ilkeler çerçevesinde hareket edilmesi gerektiğini vurgulayan sözleşme ülkeler tarafından dikkate alınır temel kilometre taşlarından biri haline gelmiştir. Kişisel verilerin uluslararası transferi mevzusuna da yeni bir bakış açısı getiren sözleşmeye ek protokollerle yeni bir şekil verilmiştir (Atak, 2010:98).

1.4.2 Avrupa Birliği 95/46/EC Sayılı Direktifi

1995 yılında "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin korunması ve Bu Tür Verilerin Serbest Dolaşımı Direktifi" Avrupa Parlamentosu ve Konseyi tarafından kabul edilmiştir. Kişisel mahremiyet başta olmak üzere bireylerin haklarının ve özgürlüklerinin korunması hakkındaki bu Direktifte belirtilen esasların, Kişisel Verilerin Otomatik İşlenmesine İlişkin Bireylerin Korunması Hakkındaki 28 Ocak 1981 tarihli 108 sayılı Avrupa Konseyi Sözleşmesinde belirtilenleri güçlendirici ve genişletici nitelikte olduğu belirtilebilir. Kişisel verilerin üye devletlerde farklı şekilde işlenmesi hususunun AB seviyesindeki birtakım ekonomik faaliyetlerin takibi için bir engel oluşturabileceği, rekabeti bozabileceği ve Birlik hukuku kapsamında makamların sorumluluklarını yerini getirmesini engelleyebileceği ihtimaline binaen böyle bir Direktif Avrupa Birliğince kabul edilmiştir (The European Parliament and The Council of The European Union, 1995).

Kabul edildiği tarihte yürürlüğe giren Direktif ile AB üyesi olmayan ülkelerin AB üyesi ülkelerden veri transferi yapabilmesi için Direktifte belirtilen ilkelere uyarak "Güvenli Ülke" konumuna gelmiş olmaları şartı aranmaktadır. Verinin kaynağını bilme, yanlış verileri düzeltme, hukuk dışı işlemlere karşı başvuru hakları ile doğrudan pazarlama yöntemleri amacıyla kişisel verilerin elden ele dolaşmasına izin verilmemesini ve hassas verilere ilişkin düzenlemeleri içeren Direktifin en önemli özelliklerinden biri zorlayıcı olmasıdır. Daha açık bir ifade ile AB mevzuatının içinde yer alan direktife uymak zorunlu olduğu gibi, AB üyesi ülkelerle ilişkiye geçerek veri transferi gerçekleştirmek için AB üyesi olmayan ülkelerin de eşdeğer koruma sağlama zorunlulukları 95/46/EC sayılı Direktif ile getirilmiştir (Mantelero, 2012:4).

1.4.3 Avrupa Birliği Temel Haklar Şartı

Fransa'nın Nice şehrinde 7 Aralık 2000 tarihinde düzenlenen konferansta Avrupa Parlamentosu, Konseyi ve Komisyonu Temel Haklar Şartı'nı kabul etmiştir. Temel Haklar Şartı, temel hakları daha anlaşılır bir şekilde formüle etme ve temel haklara daha seçkin bir yer verme imkânı sunmaktadır. Temel Haklar Şartı'nın kabulü, AB'nin meşruiyetini güçlendirmekte, temel hakları Birlik vatandaşları için "görünür

kılmakta" ve temel hak korumasının düzeyini yükseltmektedir. Ayrıca Şart, AB Anayasası yönünde atılmış önemli bir adım teşkil etmektedir (Öhltnger, 2000). Sosyal değişimler ve bilimsel ve teknolojik gelişmelerin ışığında, temel hakların korunmasının, bu haklara bir Şartta yer vererek değerlendirilmesinin gerekliliği Temel Haklar Şartı'nın kabulünü zorunlu kılan nedenlerin arasında olduğu ifade edilebilir (Metin, 2001:37). Şartın "Özgürlükler" başlıklı bölümünde kişisel verilerin korunması ile ilgili bir düzenlemeye yer verildiği görülmektedir. Bu çerçevede kişisel verilerin korunmasının bir hak olduğu, bu verilerin kişinin rızası dahilinde belirli amaçlarla ve meşru yolla kullanılacağı ifade edilmiştir. Ayrıca kişilerin kendisi hakkında toplanmış verilere ulaşma ve bunları düzelttirme hakkına sahip olduğu belirtilirken bu süreçte bağımsız makamlarca denetlemelerin yapılacağından da bahsedilmektedir.

1.4.4 OECD

108 sayılı Avrupa Konseyi Sözleşmesi kabul edilmeden birkaç ay önce OECD tarafından bilginin serbest dolaşımının engellenmesi ve gizlilik ve mahremiyetin muhafaza edilmesi amacıyla sekiz farklı ilke yayımlandığı görülmektedir. Bu ilkelerin üye ülkelere kişisel verilerin korunmasına yönelik alacakları tedbir ve gerçekleştirecekleri yasal düzenlemelerde rehberlik etmesi öngörülmektedir. Bu yönüyle bu dokümanın tavsiye niteliğinde olduğu söylenebilir. Bu ilkelerin başında veri toplamanın sınırlı olması, verilerin kaliteli olması, veri işletmeciliğinde amacın belirli olması ve verinin kullanımının sınırlı olması gelmektedir. Diğer ilkeler ise verinin güvenliğinin sağlanması, açıklık, veri sahibinin aktif katılımı ve hesap verebilirliktir (Organisation for Economic Co-Operation and Development, 2013).

OECD tarafından hazırlanan bu düzenlemelere küresel bazda eleştiriler getirilmektedir. Bu eleştirilerden ilki hiç kuşkusuz yasal bir zeminin olmamasıdır. Bu yönüyle 108 sayılı sözleşme hukuksal bir zeminde yer alırken rehber ilkeler tamamen tavsiye niteliğindedir ve bağlayıcılığı bulunmamaktadır. Bir diğer eleştiri ise OECD tarafından hazırlanan bu rehberin sadece kişisel veriyle sınırlı olması hususudur. 108 sayılı sözleşmede sadece kişisel veri ile sınırlı olmayıp özel yaşam hakkı, temel hak ve özgürlükler gibi unsurlar da işlenmektedir (Hustinx, 2014).

1.4.5 Birleşmiş Milletler (BM)

Kişisel verilerin korunması alanında BM bünyesinde de uluslararası düzenlemelerin yapıldığı görülmektedir. Bu bağlamda 1990 yılında üye ülkelerce "*Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler*" adını taşıyan bir belge kabul edilmiştir. Burada vurgulanması gerekli olan husus esas amacın üye ülkeleri kişisel verilerin korunması alanında yasal düzenleme yapmaya teşvik etmek olduğudur. Dolayısıyla BM tarafından kabul edilen bu belgenin de OECD tarafından benimsenen ilkeler gibi yaptırımı olmayan tavsiye niteliğinde ilkeleri barındırdığı görülmektedir. Bu belgede doğru verinin güvenli bir şekilde toplanması, amacın belirliliği, ayrımcılık yapmama, gereksiz verinin talep edilmemesi, verilerin sınır ötesi transferi ve yasallık gibi ilkelere değinilmektedir (Rue, 2013).

Yukarıda kısaca açıklanan kişisel verilerin korunması alanında yapılan düzenlemelerin yanı sıra doğrudan ya da dolaylı olarak veri güvenliğini ilgilendiren uluslararası düzeyde farklı düzenlemelerden de bahsetmek mümkündür. Bu bağlamda 1997 yılında Uluslararası Çalışma Örgütü (ILO) tarafından hazırlanan "*İşçilerin Kişisel Verilerinin Korunması*" çalışması (International Labour Office,1997) ve Afrika Birliği (AU) tarafından 2012 yılında hazırlanan "*Siber Güvenlik ve Kişisel verilerin Korunması Sözleşmesinden*" söz edilebilir (African Union, 2012).

1.5 TÜRKİYE'DE KİŞİSEL VERİLERİN KORUNMASI

Türkiye'de kişisel verilerin korunmasına yönelik doğrudan kanuni bir düzenleme bulunmamaktadır. Türkiye daha önce de belirtildiği üzere 108 sayılı Avrupa Konseyi Sözleşmesi imzalamış olsa da henüz onaylamamıştır. Benzer şekilde diğer uluslararası düzenlemeleri de iç hukukuna uyumlaştıran bir reform çalışması da henüz uygulamaya geçirmemiştir (Kılınç, 2012:96). Diğer taraftan çeşitli kanun metinlerinde kişisel verilerin korunmasına yönelik bazı hususlara değinildiği görülmektedir. Bu düzenlemelere aşağıda kısaca değinilmektedir.

1.5.1 1982 Anayasası'nda Kişisel Verilerin Korunmasına Dair Hükümler

Genel olarak kişisel verilerin korunması hakkı kişilik hakları altında değerlendirildiğinden, dolaylı da olsa bu yönde Anayasa ve diğer özel kanunlarda çeşitli hükümler bulunmaktadır.

1982 Anayasasında kişisel verilerin korunmasıyla ilişkilendirilebilecek bazı ilke, hüküm ve unsurlar bulunmaktadır. Bu unsurların başında insan onuru, hukuk devleti ilkesi, bireyin maddi ve manevi varlığını geliştirme hakkı, özel yaşamın gizliliği ve korunması, konut dokunulmazlığı, haberleşmenin gizliliği, dini ve vicdani kanaatleri açıklamaya zorlanamama ile düşünce ve kanaatleri açıklamaya zorlanamama hususları gelmektedir (Türkiye Cumhuriyeti Anayasası, 1982). Anayasanın 20'nci maddesinde; "*Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hakimin onayına sunulur. Hakim, kararını el koymadan itibaren kırk sekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar*" hükmü yer almaktadır. Bu madde doğrudan kişisel verilerle ilgili bir düzenleme olmamakla birlikte 2010 yılında gerçekleştirilen 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun'un 2'nci maddesi ile Türkiye Cumhuriyeti Anayasasının 20'nci maddesine aşağıdaki fıkra eklenmiştir (Türkiye Cumhuriyeti Anayasası, 2010:5).

"*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.*" Bu hükmün

getirilmesi ile kişisel veriler hakkında Anayasa'da doğrudan bir hüküm bulunur hale gelmiştir. Ayrıca bu düzenleme uluslararası yasal düzenlemelerin iç mevzuatımıza uygun şekilde işletileceği yönünde olumlu bir adım olarak değerlendirilmektedir (Kılınç, 2012:1109).

1.5.2 Türk Medeni Kanunu

Kişisel verilerin korunması, kişilik haklarının korunması kapsamında değerlendirildiğinden özel hukukta bu konuda genel olarak kişilik hakları kapsamında bir koruma ve düzenleme olduğu söylenebilir. Türk Medeni Kanunu'nun "Kişilik" bölümünde yer alan bazı düzenlemeler kişisel verilerin korunması hususuyla ilişkilendirilebilir. Örneğin "*Vazgeçme ve Aşırı Sınırlamaya Karşı Kişiliğin Korunması*" hususundaki 23. maddede kişilik haklarından vazgeçilemeyeceği ve kişinin aleyhine haklarında herhangi bir sınırlama yapılamayacağı belirtilmektedir. Yine Aynı Kanunun 24. maddesi de kişisel hakları hukuka aykırı saldırılara karşı koruma altına almıştır. Saldırılara karşı kişiliğin korunabilmesinin yolu kişilik haklarına yönelik hukuka aykırı bir ihlalin olması gerekliliğidir.

Son olarak 4721 sayılı Medeni Kanun'un 25. maddesinde dava hakkı düzenlenmiştir. İlgili maddenin sağladığı hak ile kişilik haklarına saldırıda bulunulan kişinin mahkeme yoluyla olası saldırı tehlikesinin engellenmesini, devam eden ihlalin durdurulmasını veya saldırı sona erse bile devam eden etki nedeniyle hukuka aykırı işlemin tespitini talep edilebilmektedir.

1.5.3 Borçlar Kanunu

Medeni Kanun'da olduğu gibi Borçlar Kanunu'nda da kişisel verilerin korunması ile ilişkilendirilebilecek hükümler bulunmaktadır. 6098 sayılı Borçlar Kanunu'nun "*Haksız Fiillerden Doğan Borç İlişkileri*" başlıklı ikinci ayrımında yer alan düzenlemelere göre temel hak niteliğinde olan kişisel verilerin korunması hakkının ihlali durumunda tazminat hakkı doğabilecektir. Dolayısıyla bu noktada bir yaptırımın varlığından bahsedilebilir. Benzer şekilde Kanun'un 419. maddesi uyarınca işveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. Özel kanun

hükümleri saklıdır. Dolayısıyla söz konusu maddenin, işçilere ait kişisel verilerin korunması konusunda yapılmış özel bir düzenleme niteliğinde olduğu söylenebilir.

1.5.4 Türk Ceza Kanunu

765 sayılı mülga Türk Ceza Kanununda herhangi bir hüküm ve yaptırım bulunmamakta iken 2005 yılında yürürlüğe giren yeni 5237 sayılı Türk Ceza Kanunu'nda kişisel verilerin korunması ile ilişkilendirilebilen çeşitli hükümler bulunmaktadır. Bu bağlamda özel hayatın gizliliği hususunun 5237 sayılı Türk Ceza Kanunu'nda yer aldığı görülmektedir. Özellikle ceza davasının açılabilir hale gelmesi kişisel verilerin korunması anlamında oldukça önemlidir. Benzer şekilde 5237 sayılı Türk Ceza Kanunu'nda haberleşmenin gizliliğini ihlali, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğinin ihlali, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme, nitelikli haller, verileri yok etmeme ve şikâyet hususlarına yer verilmiştir (Türk Ceza Kanunu, 2004).

Yukarıda da değinildiği gibi Anayasa ve özel kanunlarda kişisel verilerin korunmasıyla ilgili dolaylı bir şekilde ilişki kurulabilen hükümler yer alıyor olsa bile hali hazırda bu alanı doğrudan ilgilendiren bir "Kişisel Verilerin Korunması Kanunu" mevcut değildir. Medeni Kanun, Ceza Kanunu ve Borçlar Kanunu'nun yanı sıra 4875 sayılı İş Kanunu ve 4982 sayılı Bilgi Edinme Hakkı Kanunu'nda da benzer hükümlerin bulunduğu görülmektedir. Uluslararası düzenlemeler ışığında iç mevzuatta gerekli ve yeterli yasal düzenlemelerin yapılmadığı da bilinmektedir. Bu durum güvenlik, bilgi güvenliği, mahremiyet, risk açısından çeşitli sonuçlar doğurmaktadır. Bu hususlar ikinci bölümde detaylı olarak ele alınmaktadır.

İKİNCİ BÖLÜM

BİLGİ GÜVENLİĞİ VE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Bilgi güvenliği ve bilgi yönetimi konuları, içinde bulunduğumuz bilgi toplumunda üzerinde en çok çalışılan alanların başında gelmektedir. Bu alanları daha iyi anlamak için öncelikle bilgi, veri, enformasyon gibi farklı kavramların tanımlanması gerekmektedir.

Veri, enformasyon ve bilgi kavramları, üzerlerinde uzun yıllar tartışılmış farklı kavramlardır. Süregelen tartışmalara rağmen bu kavramların anlamları ya da tanımları hususunda mutabakat oluşturulamamıştır. Özellikle Türkçe ele alınan kaynaklarda anlam kargaşasının yaşandığı görülmektedir. Bu kargaşanın en önemli nedeni ise bu farklı üç kavramın zaman zaman birbirinin yerine kullanılması olarak belirlenmiştir (Yılmaz, 2009:98).

Ulusal ve uluslararası literatürde yüzlerce farklı tanımın yer almasına rağmen en çok kabul gören tanıma göre veri; olayları, nesneleri ve bunların özellikleri ile arasındaki ilişkileri temsil eden ve aynı zamanda sınıflama, düzeltme, hesaplama gibi farklı işlemlerle işlenebilen sembollerdir (Kalseth, 2001:169). Burada verinin çoğu zaman tek başına bir anlam ifade etmeyeceği fakat bir sistem içerisindeki yeri, üstlenmiş olduğu görev ve taşımış olduğu anlamla birlikte gerçek değerini yansıtabileceği anlaşılmaktadır.

Benzer şekilde enformasyon kavramı da farklı şekillerde tanımlanmaktadır. Davenport ve Prusak (2001) enformasyonu bir ileti olarak algılayarak "genellikle belge şeklinde ya da görsel ve işitsel mesaj" biçiminde tanımlamaktadır. Yine Yılmaz (2009) enformasyonu kısaca "anlam kazandırılmış veya yüklenmiş veri" olarak tanımlamaktadır. Yapılan farklı tanımlar çerçevesinde enformasyon; verilerin bir formül, denklem ya da anlamlı dinamikleri olan bir sistem içerisinde yer alan ve sınıflandırma, özetleme, değiştirme ve düzeltme gibi farklı işlemlerle anlamlı hale gelen bir bütün olarak tanımlanabilmektedir (Acar, 2008:59).

Enformasyon sürecinde ham madde olarak alınan veriler işlenerek anlamlı bir çıktı oluşturulur. Veri ve enformasyon ile yakından ilişkili olan bilgi farklı şekillerde tanımlanmaktadır. Farklı tanımlar ve bilginin özellikleri dikkate alınarak genel bir tanımlama yapmak mümkündür. Sözlük anlamıyla bilgi, insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bilgi, malumat; öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek gibi farklı anlamlara gelmektedir (TDK Türkçe Sözlük). Bazen sonuç olarak, bazen çıktı olarak, bazen enformasyon olarak ele alınan bilgi hususunda Barutçugil ise (2002:7) "insanın etrafında olup bitenleri tam ve doğru olarak kavramasını sağlayan kişiselleştirilmiş enformasyon" tanımlamasını yapmaktadır.

Diğer bir tanımı ile bilgi; en basit anlamıyla belirsizliği gideren, bilinmezi bilinebilir kılmada yararlanılan, karar vericilere doğru karar verme amacıyla doğru zamanda ve doğru yerde sunulan, aynı zamanda ham olmayan işlenmiş, değerlendirilmiş, kişiselleştirmiş enformasyon süreci ve bu süreç sonucu açığa çıkan birikim ve tecrübedir (Israel ve Perry, 1990:11). Bu çerçevede; doğru zamanda, doğru vasıtayla, doğru bir şekilde bilginin doğru kişiye ulaşarak doğru kararların alınması için bilgi güvenliğinin tesis edilmesi gerekmektedir.

Özellikle son zamanlarda yaşanan teknolojik iyileşme ve gelişmelerle birlikte bilginin hem kendisi hem de enformasyon ve ham halde bulunan veri kolaylıkla bir yerden bir yere taşınabilmektedir. Aynı zamanda çok kısa sürede işlenebilmekte ve illegal yollarla ele geçirilebilmektedir. Bütün bunlar birlikte düşünüldüğünde bilgi güvenliğinin sadece bireyler için değil kurum, kuruluş ve devletler için ne kadar büyük bir önem arz ettiği anlaşılmaktadır. Son elli yılda dijital teknolojinin de açığa çıkmasıyla birlikte artık bilgi kolayca toplanabilmekte, işlenebilmekte, depolanabilmekte ve ağlar aracılığı ile bir yerden bir yere rahatlıkla iletilebilmektedir (Sadowsky vd., 2003:62).

Küresel ağların yeryüzünde yer alan bilgi sistemlerinin birbirleri ile olan iletişim ve etkileşimini aktif hale getirmesi ve yaygınlaştırması ile birlikte yukarıda değinilen bilgi güvenliğinin önemi artmıştır. En basit tabirle bilgilerin sistem içerinde korunması ya da bir yerden başka bir yere güvenli bir şekilde taşınması, işlenmesi ve

sağlıklı bir şekilde yok edilmesi olarak tanımlanabilen bilgi güvenliği, son yılların en popüler konuları arasında yer almaktadır (Awad, Hassanien ve Baba, 2013:249).

Değişen koşullarla birlikte bilgi günümüzdeki en önemli zenginlik kaynağı haline gelmiştir. İnsanoğlu doğası gereği zenginlik kaynaklarını elde etmeyi, muhafaza altında bulundurmayı ve gerektiğinde ihtiyacı ölçüsünde kullanmayı arzu etmektedir. Hatta son yaşanan WikiLeaks, casusluk dosyaları ve dinleme skandallarının da gösterdiği üzere illegal yolla elde edilen bilgiler devletlerin bir birine karşı kullandıkları şantaj aleti haline gelmiştir (Žižek, 2014). Bilgiyi elde etme gayretinin hatta bu yolda bilgi hırsızlığının zamana hükmetmekte olduğu böyle bir ortamda bilgi güvenliğinin sağlanması en önemli konu haline gelmiştir.

Bu çerçevede bu bölümde ilk olarak bilgi güvenliği tanımı yapılacak, daha sonra tarihsel gelişimi ve önemi üzerinde durulacaktır. Ardından bilgi güvenliği yönetim sistemi detaylı bir şekilde ele alınacaktır.

2.1 BİLGİ GÜVENLİĞİ KAVRAMI, TARİHSEL GELİŞİMİ VE ÖNEMİ

2.1.1 Bilgi Güvenliği Tanımı

Bilgi güvenliği; bilgiye erişimin sağlanması, iletişim kanallarıyla bozulmadan, başkalarının istilasına uğramadan, değiştirilmeden güvenli bir şekilde kaynaktan alıcısına taşınması ve devam eden süreçte muhafaza edilerek gerektiğinde güvenli bir şekilde yok edilmesi şeklinde tanımlanabilir (Tekerek, 2008:132). Bu tanımlamadan da yola çıkılarak, bilgi güvenliği ile ilgili üzerinde durulması gerekli olan birkaç husus vardır. Bunlardan ilki; bilgi güvenliğinin bir süreçten ibaret olduğudur. Diğer bir ifade ile bilgi güvenliği sadece elde edilen bilgilerin başkalarından, özellikle kötü niyetli ve farklı emeller peşinde olan kişilerden korunması olarak algılanmamalıdır. Bilginin elde edilmesi aşamasında güvenliğin sağlanması oldukça önemlidir. Yasal yollardan emniyetli bir şekilde bilgi elde edilmelidir. Aksi takdirde illegal yollarla, hırsızlıklarla ya da yasal dayanağı olmayan gizli dinleme ve takiplerle elde edilen bilgi daha ilk aşamada güvenlik açısından sıkıntılıdır. Benzer şekilde bilgi edinme süreci içerisinde sadece bilginin değil aynı zamanda bilginin aktarıldığı veya

iletildiği iletişim kanallarının güvenliğinin sağlanması da bilgi güvenliğinin unsurlarıdır.

Diğer bir husus ise elde edilen ve kullanılan bilgilerin ortadan kaldırılması ya da yok edilmesindeki güvenlik açısından gösterilecek hassasiyettir. Bu noktada yok edilmesi gerekli olan bilgilerin geri dönüşümü imkânsız olacak şekilde ortadan kaldırılması gerekmektedir. Özellikle elektronik ortamda tutulan bilgi ve verilerin belli bir süre sonra geri dönüştürülmesinin imkânsız olacak şekilde güvenli bir şekilde ortadan kaldırılması gerekmektedir. Örneğin; kariyer meslek sınavı açan bir kamu kurumunun toplamış olduğu ve elektronik ortamda kayıtlı olan bilgi, belge ve verilerin sınav tamamlandıktan sonraki süreçte güvenli bir şekilde tamamen ortadan kaldırılması gerekmektedir. Aksi takdirde kariyer mesleğe adım atmış olan bu kişilere ait bilgiler tekrar elde edilirse kötü niyetli kişilerce kullanılarak istenmeyen sonuçların doğmasına neden olunabilir.

Bilgi güvenliği alanında en önemli hususlardan bir başkası ise gerek kamu gerekse özel sektördeki her kurumun elinde tuttuğu bilgi varlıklarını net bir şekilde tespit ve tertip etmesi gerektiğidir. Yapılan çalıştaylarla dışarıdan ya da içeriden gelebilecek tehdit, tehlike ve riskler ortaya konmalı, bilgi varlıklarının korunmasında mevcut zafiyetler ele alınmalı ve bilgi güvenliği çemberi oluşturulmalıdır. Yapılacak bu ve benzeri çalıştayların kurumsal bilgi güvenliğinin tesis edilmesinde kilit rol oynadığı ortaya konmuştur (Güzel, 2011:158).

2.1.2 Bilgi Güvenliği Tarihsel Gelişimi

Bilgi güvenliğinin tarihi oldukça eskilere dayanmaktadır. Türk Dil Kurumu (TDK) Türkçe Sözlüğünde "gizli yazılar, şifreli belgeler bilimi veya incelemesi" şeklinde tanımlanan kriptoloji, esasında bilgi güvenliği çerçevesinde oluşturulan bir bilim dalı ortaya çıkmıştır. Milattan Önce (MÖ) 1900'lü yıllarda Mısırlı kâtipler tarafından yazılan kitabelerde standart dışı işaretlere rastlanmış olsa da, MÖ 60'lı yıllarda Sezar (Julius Ceaser) askeri anlamda şifreli metinleri kullanan ilk kişi olarak tarihe geçmiştir. En eski bilimsel kripto analiz eserinin ise ünlü Yunan bilim adamı AlKalkashandi tarafından 1412 yılında kaleme alındığı bilinmektedir (Stalling, 1995).

En temelde bilginin güvenli bir şekilde alıcıya aktarılması olan kripto ile bilgi bilinir bir formdan şifreleri bilmeyenler için bilinmez bir forma aktarılmaktadır. Özellikle askeri ve diplomatik alanda etkin bir şekilde kullanılmaktadır.

Bilgi güvenliği tarihi her ne kadar MÖ'ye kadar dayansa da esasında bilgi güvenliği bilgisayar sisteminin güvenliği ile başlamıştır. Diğer bir ifade ile 1920'lerde iletişimde kullanılan kodların şifrelenmesi, çözülmesi ve güvenliği için icat edilen Enigma'nın fiziksel, donanım ve yazılım güvenliğinde kullanılması ile birlikte bugünkü anlamda bilgi güvenliği başlamıştır. 1930'lu yıllarda şifreleri kırılmış olan Enigma yerine II. Dünya Savaşı sırasında daha karmaşık ve daha güvenli yeni sistemler oluşturulmuştur. Özellikle 1960'lı yıllarda daha önce ABD'de askeri amaçla geliştirilen ve ARPA olarak bilinen The Defense Advanced Research Projects Agency (DARPA) bu alanda yoğun mesai harcamıştır. Bu çalışmalar sonucunda internetin kurucusu olarak bilinen Larry Roberts ARPANET olarak adlandırılan ve bugünkü internetin ilk çekirdeğini oluşturan projeyi tamamlamıştır (Beranek ve Inc, 1981).

Soğuk savaşın devam ettiği yıllarda ARPANET ayrı bir önem kazanmıştır. Ayrıca çevreleme politikası çerçevesinde belirlenmiş olan stratejilerin gizlilik içerisinde gerçekleştirilmesi oldukça büyük önem arz etmiştir. Bu doğrultuda büyük güçler haberleşme ve bilgi güvenliğinin sağlanması gayesiyle önemli çalışmalar yapmışlardır. Bu çerçevede ARPA tarafından 1978 yılında "*Koruma Analizi: Sonuç Raporu*" yayımlanmış ve güvenlik sisteminin kırılganlığı ortaya konmuştur (Loewenstein, 2015). 1980'li yıllarda ise bilgi güvenliği için verilerin tek bir merkezden korunması terkedilmiş ve bir çeşit bilgisayar ağı oluşturulmuştur. 1990'lı yıllarda ise kurulan bu bilgisayar ağları birbiri ile bağlanarak internetin açığa çıkmasına yardımcı olmuştur. Bugün ise internet bu bilgisayar ağlarının güvenli olmayan bir şekilde birbiri ile devam eden bir iletişim halinde yer aldığı bir alan haline gelmiştir. Özellikle 1990'lı yılların sonu ve takip eden yıllarda pek çok ülkenin kişisel verilerin korunması alanında kanun çıkarmasıyla birlikte bilgi güvenliği ayrı ve önemli bir çalışma alanı olarak ortaya çıkmıştır. Son yıllarda ise bilgi güvenliğinin yanı sıra "bilgi yönetimi" ve "kayıt yönetimi" alanları da üzerinde

çalışılan ve pek çok ülkenin büyük önem atfettiği çalışma alanları arasında yerini bulmuştur (Lomas, 2010:188).

2.1.3 Bilgi Güvenliğin Önemi

"Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet" (TDK Türkçe Sözlük) olarak tanımlanan güvenlik kavramı geniş bir alanı kapsamaktadır. Dış politikadan spora, ticaretten taşımacılığa, eğitimden sağlığa birçok alanda emniyetin tesis edilmesi toplumsal yaşamın vazgeçilmezlerindendir. Teknolojinin, iletişimin ve internetin hızla ilerlemesiyle birlikte çoğu işlem elektronik ortamda yapılır hale gelmiştir. 2013 yılı sonu itibarıyla 2,8 milyar internet kullanıcısı bulunmaktadır. 2000 yılında 360 bin olan bu rakamın çok kısa sürede 3 milyar kişiye dayanması teknolojik ilerlemedeki hızı yansıtmaktadır (Miniwatts Marketing Group, 2014). Benzer şekilde, 2013 yılında oldukça hızlı bir şekilde genişleyen ve 1,2 trilyon Avro olan e-ticaret hacminin 2015 yılında 1,5 trilyon Avro olması öngörülmektedir (Sezgin, 2013).

Bilimsel ve teknolojik ilerlemenin oldukça yüksek seviyelerde olduğu günümüz bilgi toplumlarında gerçek ya da tüzel, ulusal ya da uluslararası kurum ve kuruluşlar internete ve teknolojiye bağımlı hale gelmiştir. Bütün bunların doğal bir sonucu olarak yapılan her e-ticarette ya da internet kullanımında bilgi güvenliği kavramını daha da ön plana çıkaracak şekilde sisteme veriler girilmekte, bilgi akışı, depolanması ya da yok edilmesi gibi işlemler yürütülmektedir. Bilgi güvenliğinin sağlanması ile iş ve işlemlerin insanlar tarafından daha rahat ve güvenli bir şekilde gerçekleştirilmesiyle, kurumlara ve piyasalara olan güven artacaktır.

Rekabetin bu denli yüksek olduğu piyasa ortamında firmaların en büyük varlıklarından biri kuşkusuz sahip oldukları bilgilerdir. Örneğin, bu rekabet ortamında hacklenen bir firmanın sahip olduğu bilgilerin internette dolaşması o firmayı maddi ve manevi olarak büyük zararlara uğratacaktır. Müşterilerine ait bilgilerin, mali yapısının, finansal kalem ve dinamiklerinin paylaşılması nedeniyle müşterilerin firmaya olan güveni sıfırlanacak, açılan davalar ile firma önemli düzeyde yıpranacaktır.

Göz önünde bulundurulması gerekli olan bir diğer husus ise tesis edilen bilgi güvenliğinin teknolojik ilerleme devam ettiği müddetçe güncellenmesi gerektiğidir. Diğer bir ifade ile mevcut durumda bilgi güvenliğinin tam olarak oluşturulmuş olması ve %100 güvenin sağlanmış olması tek başına belli bir anlam ifade etmeyebilir. Esas olan devam eden süreçte teknolojik ve bilimsel ilerlemeye paralel olarak bilgi güvenliği için oluşturulan güvenlik çemberinin güncellenmesidir. Aksi takdirde ilerleyen sürede tehditlere açık bir hedef haline gelmesi kaçınılmazdır.

2.2 BİLGİ GÜVENLİĞİ İLKE VE PARAMETRELERİ

Bir disiplin olarak ele alınan bilgi güvenliği kapsamında korunması öngörülen bilgi, temel olarak bir değere sahip olma, kaydedilebilme, alıcı tarafından alınabilme ve var olma gibi özellikleri bünyesinde barındırmaktadır (Zins, 2007:532). Bu özellikleri taşıyan bilginin güvenliğinin sağlanması amacıyla benimsenen bilgi güvenliği yönetiminde dikkate alınması gerekli olan çeşitli parametre ve ilkeler vardır. Bu noktada, yapılan literatür taramasında çeşitli kaynakların (Koç (2008), Güzel (2011), Tekerek (2008), UNINETT (2010), Stamp (2005) bilgi güvenliği ilkeleri adı altında erişilebilirlik, bütünlük ve gizliliği ele aldığı görülmüştür. Bir takım farklı kaynaklarda ise bu unsurların birer bilgi güvenliği parametresi olarak ele alındığı tespit edilmiştir. Bu çalışmada adı anılan unsurlar birer parametre olarak açıklanırken bilgi güvenliği ilkeleri ayrı başlık altında ele alınacaktır.

2.2.1 Bilgi Güvenliği İlkeleri

Bilgi güvenliğinin alanında genel kabul gören üç temel ilke vardır. Bu ilkeler aşağıda başlıklar halinde gösterilmiştir (Gelbstein ve Kamal, 2002).

2.2.1.1 Tam Güvenlik Sağlanamaz

Güvenlik sistemleri ve bu çerçevede oluşturulan araç ve gereçler dikkate alındığında kusursuz ya da % 100 güvenliğin sağlanamadığı söylenebilir. Her sistemin ve her aracın bir şekilde devre dışı bırakıldığı, saldırılar karşısında yetersiz kaldığı gözlenmektedir. Özellikle son yıllarda teknolojik ilerlemelerle birlikte güvenlik anlamında fiziksel korumanın yanı sıra bir de yazılım eklenmiştir. Zamanla bu yazılımların da kusursuz olmadığı ortaya çıkmıştır (Denning, 1998).

Bilgi güvenliği çerçevesinde oluşturulan bu yazılımlar dikkate alındığında unutulmaması gerekli olan bazı hususlar vardır. Bu hususlardan ilki; yeni yazılımın yeni açık anlamına geldiğidir. Ayrıca önceki yazılım hataları tam olarak düzeltilemez. Düzeltilse bile yapılan düzeltmeler tam olarak yüklenemeyebilir. Son olarak ise düzeltmelerin yeni açıklar içermesi muhtemeldir.

Bütün bunlar düşünüldüğünde güvenlik yönetiminde bilgi güvenliği anlamında kusursuz bir korumanın sağlanamayacağı söylenebilir. Ayrıca kurulan bir güvenlik sisteminin etkinliği sadece güvenlik açığı ortaya çıktığında tespit edilebilir. Ayrıca tespit edilen bu açık ve zayıflıklar yeni düzenlemelerle onarılabilir ki yukarıda da bahsedildiği üzere her onarım yeni bir açık anlamına gelmektedir. Dolayısıyla bilgi güvenliği alanında % 100 güvenlik sağlanamadığı gibi kusursuz bir güvenlik sistemi oluşturulduğuna dair" düşünceler en büyük zayıflıklardan biridir.

2.2.1.2 Risk ve Harcamalar Dengelenmelidir

Diğer güvenlik sistemlerinde olduğu gibi bilgi güvenliği sağlamaya yönelik alınan tüm tedbir ve önlemlerin yegane amacı başta kişinin kendisi olmak üzere kişi mülkiyetinin korunmasıdır. Gerekli önlemler alınırken alınan kararı etkileyen iki unsurdan birincisi potansiyel güvenlik riski algısı diğeri ise kullanıcıların güvenlik riski algısı karşısında kabul ettiği sınırlamalardır. Alınan güvenlik önlemleri kullanıcı kişilerin kullanımını belli ölçüde sınırlandırırken bir de maliyet yüklemektedir (Gelbstein ve Kamal, 2002).

Dolayısıyla yapılacak olan güvenlik harcamalarında bir denge kurulmalı ve kusursuz bir güvenliğin sağlanamayacağı ve potansiyel risk algısının zamanla değişebileceği unutulmamalıdır. Ayrıca güvenlik için alınacak önlemlerin kişiden kişiye ve zamana göre değişen tehlike algısı çerçevesinde değişmesi ve bu durumda harcamaların tekrar eden harcamalar haline gelmesi kaçınılmaz olmaktadır (International Business Machines, 2008).

2.2.1.3 Güvenlik ve Meşakkat Dengelenmelidir

Yukarıda da ifade edildiği gibi güvenlik alanında kusursuzluk mümkün olmamakla birlikte daha fazla güvenlik için alınan her tedbir, atılan her adım özellikle son

kullanıcıya yeni bir külfet getirmektedir. Örneğin hırsızlardan korunmak için bahçe duvarına, bahçe kapısına, bahçenin içerisine, dış kapıya ve buraların muhtelif yerlerine asma kilit, sürgülü kilit, şifreli kilit gibi ardı arkası gelmeyen güvenlik önlemleri alınabilir. Fakat burada dikkat edilmesi gerekli olan husus son kullanıcı pozisyonundaki kişinin bütün bu önlemleri ve kilitleri aktif hale getirmesinin uzunca bir zaman ve zahmet gerektirdiğidir. Dolayısıyla bilgi güvenliği için de geçerli olan bu hususta güvenlik ve katlanılacak olan zahmet ve meşakkat arasında denge kurulmalıdır (Gelbstein ve Kamal, 2002).

2.2.2 Bilgi Güvenliği Parametreleri

Bilgi güvenliğine yönelik çeşitli tehditler vardır. Bunlardan bir kısmı içeriden bir kısmı ise dışarıdan kaynaklanmaktadır. Dışarıdan gelebilecek tüm tehditlerin bertaraf edilmesi ve önlerinin alınması bilgi güvenliğinin sağlanması için gerekli fakat yeterli olmayabilir. Dolayısıyla içeriden, kullanıcılardan gelebilecek tehditler de dikkate alınmalıdır.

Özellikle son yıllarda tehditlerin büyük çoğunluğunun içeriden geldiği görülmektedir. Bu çerçevede bilgi güvenliği alanında genel kabul gören üç parametre olan erişilebilirlik, gizlilik ve bütünlük önemli hale gelmektedir. Bunların yanında bazı metinlerde kimlik tespiti, değer barındırma, kayıt tutma ve reddedilememe gibi parametreler de yer alıyor olmasına rağmen bu çalışmada çoğunluğun kabul ettiği üç esas parametre kısaca açıklanacaktır (Peltier, 2005:38).

2.2.2.1 Erişilebilirlik

Bilgi sistemlerindeki en önemli unsurlarından biri ihtiyaç duyulduğu zamanda kullanıcılara gerekli bilginin sağlanmasıdır. Bilgi sistemlerinde bilgiye ulaşabilmek oldukça önemli olmakla birlikte arzulanan ya da öngörülen zaman zarfında ulaşmak erişilebilirlik özelliğinin bir gerekçesi olarak bilinir. Bilgi güvenliği kapsamında erişilebilirlik hizmeti ile sisteme içeriden ya da dışarıdan gelebilecek tehditler engellenir ve kullanıcılara istenen zamanda istenilen bilgi güvenli bir şekilde sunulur.

Erişilebilirliğin sağlanması için güvenlik duvarları, koruyucu yazılımlar gibi fiziksel önlemler alınabilirken bilinçsiz kullanıcı, eğitimsiz personel, yazılım hataları

ve felaketler gibi sistem için tehdit unsurları barındıran hususlar vardır. Ayrıca erişilebilirlik genel olarak rakam ya da oranlarla ifade edilebilen ve performans ölçümü yapılabilen hususlardır. Örneğin "sistem, bir yılda kullanıcının talep ettiği bilgiyi % 99.5 oranında sağlamıştır" şeklinde ölçülebilir sonuçlar ortaya konulabilmelidir (Gelbstein ve Kamal, 2002)

2.2.2.2 Bütünlük

Bütünlük bilgi sisteminin köşe taşını oluşturmaktadır. Çünkü bir bilgi bütün halde kullanılamıyorsa ve o halde muhafaza edilemiyorsa sağlıklı bir bilgi güvenliği sisteminden söz edilemez. Bilgi güvenliği için bilinen/kabul edilen en iyi yöntemlerin sıralandığı ISO 17799 standartlarında bütünlük; *"bilgi ve işlem metodunun tamamının ve doğruluğunun muhafaza edilmesi eylemi"* olarak tanımlanmaktadır (ISO 17799, 2005). Burada bilginin bütünlük parametresini sağlıyor olması ile o bilginin tam olduğu, kaynaktan hedefe giderken ya da depolanırken herhangi bir değişim ve bozulmaya uğramadığı, eksik bir unsuru barındırmadığı ve daha önceden belirlenen prosedüre uygun olarak güvenli bir şekilde elde edilebildiği anlaşılmaktadır (Tekerek, 2008:133).

2.2.2.3 Gizlilik

ISO 17799'da *"sadece erişim yetkisi tanınan kişilerin bilgiye ulaşabilmesinin sağlanması"* olarak tanımlanan gizlilik parametresi bilgi güvenliği sisteminde önemli bir yer tutmaktadır. Temel olarak gizli bilginin gizliliğinin muhafaza edilmesi ile bu parametre sağlanmış olmaktadır. Burada genel dinamikleri ile bilgi güvenliği sistemi içerisinde başarılması en kolay parametre olarak algılansa da en önemli ve en çok tehdit edilen husustur.

Sistemi hem içeriden hem de dışarıdan tehdit eden pek çok unsur olmaktadır. Gizlilik ile bilginin oluşturulmasından depolanmasına, taşınmasından işlenmesine kadar bütün evrelerde sadece yetkili kişilerin yetki sınırları içerisinde bilgiye ulaşmasının, kullanmasının, işlemesinin ve depolamasının sağlanması amaçlanmaktadır. Gizliliğin sağlanması için şifreleme, yetkilendirme gibi yöntemler kullanılsa da tehditler her zaman var olmaya devam etmektedir (Peltier, 2005:39).

2.3 BİLGİ GÜVENLİĞİ YÖNETİMİ

Jellinek tarafından insan, toprak ve iktidar unsurlarının bir araya gelmesiyle oluşan bir varlık olan devlet (Gözler, 2007), toplumun en temel kurumlarından biri olarak ortaya çıkan, belirli işlevlerle donatılan ve farklı boyutları olan çok yönlü bir sosyal olgu olarak tanımlanabilmektedir (Zabunoğlu, 1973). Yukarıda kısa tanımı yapılan devletin, devleti oluşturan insanların, bu insanlara ait kişisel hak ve hürriyetlerin, can ve mal emniyetinin, kamu düzeninin, kişisel veri ve bilgilerin korunmasını da kapsayan güvenlik kavramı ve algısı değişkenlik göstermektedir. Özellikle 11 Eylül terörist saldırısının, başta Amerika Birleşik Devletleri (ABD) ve Avrupa ülkeleri olmak üzere pek çok devletin güvenlik dinamiklerinin ve güvenlik algısının değişimini zorunlu kıldığı ifade edilebilir (Yılmaz, 2011).

Güvenlik algısına paralel olarak devletlerin tehdit, saldırı ve tedbir algılarının da değiştiği söylenebilir. Özellikle içinde bulunduğumuz bilgi ve teknoloji çağında tespit edilen saldırıların çoğunluğunun bilgi ve kişisel verilere yönelik olduğu görülmektedir. Son zamanlarda medyaya da yansıyan WikiLeaks Olayı (Fenster, 2012:768) ve HSBC skandalı bilgi güvenliği ve kişisel verilerin korunmasının sadece devlet bazında değil uluslararası alanda da ne kadar önemli olduğunu ortaya koymaktadır. Benzer şekilde sağlık verilerinin korunamaması, bu alanda bilgi güvenliğinin etkin yönetilememesinin doğal bir sonucu olarak dünya genelinde ekonomik değeri milyar dolarların üzerinde olan veri hırsızlığı ve dolandırıcılık olayları ortaya çıkmaktadır. Yapılan araştırmalar dünya genelinde 1997-2007 yıları arasında % 5,59 olan sağlık alanında ortalama dolandırıcılık ve veri hırsızlığının 2008-2011 yılları arasında % 25 oranında bir artışla % 6,99'a yükseldiği görülmektedir. Bu durum ise ülkelerin bilgi güvenliği ve verilerin korunmasına daha fazla pay ayırmalarını zorunlu kılmıştır. Aynı araştırmaya göre, ABD'de sağlık alanındaki dolandırıcılığın ülke bütçesine olan maliyetinin yıllık 90 ila 210 milyar Dolar arasında değiştiği tahmin edilmektedir (Evans vd., 2014).

Bu çerçevede, Microsoft Başkan Yardımcısı Thompson tarafından bir hedeften ziyade bir süreç olarak tanımlanan güvenliğe ve güvenlik yönetimine ayrı bir önem atfedilmesi gerektiği açıktır (Wallace ve Baker, 2007:38).

Diğer taraftan bilgi teknolojilerinde meydana gelen süratli ilerlemeler, daha çok bilginin depolanmasına ve kolayca bir yerden başka bir yere taşınmasına imkân sağlamıştır. Bütün bunlara paralel olarak siber saldırıların çeşitlenmesi ve öngörülemez bir hal alması ile birlikte bilgi güvenliğinin sağlanması için kurum ve kuruluşlarda yeni bir yönetim anlayışının benimsenmesi zorunlu hale gelmiştir. Bilgi güvenliği yönetimi sadece kurumsal olarak değil aynı zamanda kişisel olarak da ele alınabilir. Bu noktada çalışmamızda kurumsal anlamda bilgi güvenliği yönetimi ele alınacaktır (Information Security Policy Council, 2012).

Kurum ve işletmelerde çağdaş yönetim teknikleri altında bilgi güvenliği yönetimi yeniden ele alınırken dikkat edilmesi gerekli olan birkaç önemli husus vardır. İyi oluşturulmuş bir süreç analizi bu hususların başında gelmektedir. Özellikle kamu kurumlarında idarenin sürekliliği ilkesinin genel bir sonucu olarak iş süreçleri sağlıklı bir şekilde oluşturulmalı ve ortaya çıkan değişiklikler çerçevesinde güncellenmelidir. Bu şekilde bilgi ve veri akışı net bir şekilde ortaya konarak hassas noktalar belirlenebilir. Ayrıca iş süreçlerinin sağlıklı bir şekilde analiz edilmesi sistem içerisinde bilgi güvenliği yönetimini kolaylaştıracaktır (Anderson, 2006:17).

Bir diğer önemli nokta kurum içerisinde iş süreçleri belirlendikten sonra bilgi güvenliği yönetimi çerçevesinde bir strateji belgesinin oluşturulmasıdır. Bu strateji belgesi çalışması esnasında paydaş ve müşterilerle bir araya gelinerek risk alanları tespit edilerek gerekli önlemler ve yeni stratejiler oluşturulabilir. İş süreçlerinin analiz edilmesi ve strateji belgesinin oluşturulması tek başına yeterli olmayıp bu aşamaların devamında kurumların teşkilat anlamında bu belgeye ve kısaca bilgi güvenliği yönetimine sahip çıkması sağlanabilir. Bilgi güvenliği yönetiminin sahiplenilmesi doğrultusunda atılacak ilk adım kurum içerisinde farkındalık oluşturmaktır Oluşturulan bu farkındalıkla birlikte kurum çalışanları bilgi güvenliği yönetimi hususunu ve bu doğrultuda atılacak adımları, izlenecek stratejileri benimseyecek ve sahiplenecektir. Zamanla oluşan farkındalığı verilecek eğitimlerle pekiştirmek bilgi güvenliği yönetiminin tamamlayıcı unsurlarındandır. Bu eğitimlerin periyodik olarak düzenlenmesinin hem çalışanlar hem de yöneticiler açısından daha sağlıklı olacağı ifade edilebilir (Fey vd., 2012).

Bilgi güvenliği yönetiminde önemli hususlardan bir diğeri de verilerin tasnif edilmesidir. Gerekli güvenlik önlemlerinin alınması, siber saldırılarının engellenmesi ve veri muhafazasının sağlanması kadar önemli olan bu husus yönetim açısından oldukça ehemmiyetlidir. Tasnif edilmemiş bir bilgi ve verinin yönetimi oldukça zor olup gerektiğinde kullanılması için ulaşılması güçtür. Ayrıca tasnif edilmemiş bilgi ve veriye ulaşmak büyük bir zaman kaybına neden olabilmektedir. Yine kurumsal anlamda bilgi güvenliği yönetiminin sağlanması için kurum içinde bilgiye ulaşım ve veriyi kullanım amacıyla personel arasında gerekli yetkilendirme yapılması bu sürecin yönetimini olumlu yönde etkileyecektir (Hennessy, 2009). Gerekli eğitimi almış, bilgi güvenliği yönetimini sahiplenmiş kişilerin bilgi kullanımı konusunda yetkilendirilerek sorumluluk yüklenmesi bilgi güvenliği yönetimi açısından oldukça önemlidir.

Bilgi güvenliği yönetimi çerçevesinde kısaca ele alınan bu hususların resmi bir belgeye dayandırılması yönetim açısından fevkalade mühimdir. Bu durum bir yandan çalışanlara güven vermekte diğer yandan da izlenecek strateji ve politikaların oluşması esnasında bir pusula görevi görmektedir.

Ana hatlarıyla kurumsal anlamda bilgi güvenliği yönetiminde bulunması gerekli olan hususlara kısaca değindikten sonra son olarak bilgi güvenliğinde kabul görmüş genel ilkelere değinilecektir.

2.4 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ VE GÜVENLİK ALANLARI

İlk kez 1998 yılında BSI (British Standards Institute) tarafından yayınlanan ve BS 7799-2 standardında kullanılan Bilgi Güvenliği Yönetim Sistemi (BGYS) organizasyonlara bilgi ve veri yönetiminin sistematik bir şekilde ele alınması hususunda yol göstermektedir. BSI tarafından ortaya konan standartlar izleyen yıllarda Uluslararası Standartlar Kurumunca (ISO) kabul edilmiş ve uygulamaya konulmuştur. Gelinen noktada ise bilgi güvenliği yönetimi alanında en çok başvurulan standardın, "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardı olduğunu söylemek mümkündür. Bu standartlar esasında bilgi güvenliği yönetim sürecinin başarılı bir şekilde gerçekleşmesi

amacıyla işletilmektedir (Önel ve Dinçkan, 2007). Bu noktada ifade edilmesi gereken önemli bir husus ise bilgi güvenliği yönetim içeriğinin, etki alanının ve unsurlarının kurumdan kuruma ve kişiden kişiye değişebildiğidir. Örneğin Tudor'a (2001) göre bilgi güvenliği yönetiminde beş unsur vardır ve bunlar;

- Güvenlik organizasyonu ve altyapı,
- Güvenlik politika, standart ve prosedürleri,
- Güvenlik esasları ve risk değerlendirmeleri,
- Güvenlik bilinci ve eğitim programları,
- Uygunluk.

Tudor tarafından beş başlık altında sıralanan yukarıdaki güvenlik alanlarının ISO belgelerinde daha farklı başlıklar altında ele alındığı görülmektedir. Bilgi güvenliği yönetim alanındaki bu güvelik alanları aşağıda kısaca açıklanmaktadır.

2.4.1 Güvenlik Politikası

İçinde barındırdığı tavsiye ve kaidelerle bilgi güvenliğinin sağlanmasına ilişkin süreç yönetimini güçlendiren güvenlik politikalarının amacı bilgi güvenliği yönetimine yön verirken ilgili kanun ve yasal düzenlemelere uygun olarak gerekli desteğin verilmesidir. Bu bağlamda bilgi güvenliği konusunda yönetimin bakış açısını, onayını ve desteğini yansıtan güvenlik politikası belgesinin hazırlanarak iç ve dış tüm paydaşlara duyurulması büyük önem arz etmektedir. Bu belgenin özellikle organizasyon içerisinde çalışanlar tarafından benimsenmesi için belge hazırlama süreci iyi organize edilmeli ve çalışanların görüş ve önerileri dikkate alınmalıdır. Ayrıca hazırlanacak bu belge genel kurumsal doküman, belge, ilke ve kaidelere uygun olmalıdır (Pehlivan ve Marttin, 2007:51).

Oluşturulacak güvenlik politikasının ve belgenin personel güvenliğinden fiziksel güvenliğe, pratik uygulamalardan ve teknik alanlara kadar pek çok konuyu açık, net ve anlaşılır bir şekilde ortaya koyması oldukça önemlidir. Ayrıca organizasyonun her kademesinin güvenlik politikalarını benimsemeleri ve bu oluşturulan belgen sorumlu bir yöneticinin mevcudiyeti de işin ciddiyetinin ortaya konması bağlamında büyük önem arz etmektedir. Son olarak hazırlanan güvenlik

politikası ve belgesi organizasyon içinde ve dışında genel uygunluk ve etkinliğin sağlanması için belirli aralıklarla gözden geçirilmeli ve gerekli görüldüğünde değiştirilmelidir (Doğantimur, 2009).

2.4.2 Organizasyonel Güvenlik

Bilgi güvenliği yönetiminde karşılaşılan güvenlik alanlarından ikincisi olan organizasyonel güvenlik ile Kurum içerisinde bilgi güvenliği yönetimi alanında yürütülen iş ve işlemleri kolaylaştıracak bir yönetim yapısının oluşturulması amaçlanmaktadır. Bilgi güvenliği yönetimi çerçevesinde uygulama ve kontrollerin yapıldığı, görev dağılımının belirlendiği ve sorumluluğun dağıtıldığı bir yönetim yapısının organizasyonlara bilgi güvenliği yönetim alanında kolaylıklar sağlayacağı belirtilmektedir. Ayrıca iş süreçlerinin analizinin de yönetimi daha etkin hale getireceği ifade edilmektedir. Bu çerçevede gerekli olması durumunda kurum içerisinde bilgi güvenliği danışma birimi ile koordinasyon birimi oluşturulabilir. Organizasyonel güvenlik kapsamında kurulacak olan bilgi güvenliği yönetim birimlerinin kurum dışındaki dış paydaşlar ve üçüncü taraflara da bakan bir yönünün olması yönetimin hem içeride hem de kurum dışında daha etkin ve başarılı olmasına yardımcı olacaktır (ISO/IEC-17799, 2005).

2.4.3 Varlık Sınıflandırması ve Denetim

Bilgi güvenliği yönetimindeki bir başka unsur, kurum içerisinde envanter çalışması yapılarak mevcut varlıklar ortaya konulması gerekliliğidir. Daha sonra bu varlıklar makul bir sınıflandırmaya tabi tutulmalıdır. Burada temel amaç farklı değere sahip varlıkların bilgi güvenliği yönetim kapsamında uygun koruyucu önlemler çerçevesinde ele alınmasıdır. Bu noktada varlıklar çalışanlara zimmetlenebilir. Benzer şekilde zilyetliğin de oluşturulması tartışılabilir. Bu noktada, organizasyon içerisindeki farklı varlıklara uygulanacak güvenlik yönetiminin ve koruyucu tedbirlerin derecesinin yönetim tarafından belirlenmesi ve sorumlu kişilerin atanmasının bilgi güvenliği yönetiminin etkinliğini artıracağı vurgulanmaktadır (Doğantimur, 2009).

2.4.4 Personel Güvenlik Alanı

ISO belgelerinde belirtilen bilgi güvenliği yönetimde bir diğer önemli alan personeldir. Bilgi güvenliği alanında hırsızlığı, dolandırıcılığın ve hataların önüne geçebilmek için personelin işe alınmadan önce başlanarak ayrıldıktan sonraki süreci de içine alan geniş bir zaman diliminde uygulanması gerekli olan kurumsal politikalar ortaya konmaktadır. Bu doğrultuda personel işe alınmadan önce başta kendisi olmak üzere yakın akrabaların da güvenlik soruşturulmasında titizlikle geçmesi öngörülmektedir. İşe alım esnasında ise açık, net ve anlaşılır bir dille oluşturulan yazılı hukuki doküman, belge ve sözleşmelerin taraflarca imzalanmasının gerekli olduğu düşünülmektedir (The Office of the Australian Information Commissioner, 2013).

İşe başladıktan sonraki aşamada ise işe alınan personele yönelik düzenlenecek eğitim ve çeşitli faaliyetlerle personelde bilgi güvenliği farkındalığının oluşturulması ve müteakiben gerekli donanımın edinilmesinin bu alanda atılması gerekli olan önemli adımlardan biri olduğu vurgulanmaktadır. Bu esnada hem kurumun tüzel kişiliğinin, hem çalışan personelin hem de üçüncü tarafların rol ve sorumluluklarının belirtilmesi önem arz ettiği bilinmektedir. Ayrıca görev ve sorumluğu dışında ortaya konan davranışlar ile kurumsal ekipmanın amacı dışında kullanılması durumlarında oluşan disiplin suçları ve bunlara yönelik daha önceden belirtilen yaptırımların kararlılıkla uygulanması bilgi güvenliği yönetimini etkin hale getirecektir.

Son olarak personel güvenliği alanında işten ayrılan, çıkarılan ya da emekli olan personelin fiziksel olarak kurumuyla bağlantısı kopmuş olsa dahi bilgi güvenliği alanında risk teşkil etmektedir. Dolayısıyla daha önceden taraflarla taahhüt edilen edim ve eylemlerle güvenlik yönetimindeki bu risk ortadan kaldırılabilir (ISO/IEC-17799, 2005).

2.4.5 Fiziksel ve Çevresel Güvenlik

Bilgi güvenliği yönetiminde fiziksel ve çevresel güvenlik alanında gerekli önlemlerin alınması gerekli olup özellikle sel, yangın, deprem gibi doğal afetlerin yanı sıra insan kaynaklı saldırılar sonrası oluşacak hasarın önlenmesinde oldukça önemlidir. Bu doğrultuda kurumsal bina depreme dayanıklı olmalı, gerekli testlerden geçmiş

bulunmalı ve yangın merdiveni, acil durum alarmı, erken uyarı sistemi, depo ve sığınak gibi unsur ve üniteleri içermelidir. Aynı zamanda çevresel güvenliğin tesisi için kurum dışı duvar, kontrol noktaları, kartlı geçiş esasında çalışan turnikelerin olması büyük önem arz etmektedir. Ayrıca varlık envanteri çalışması sonucunda gerekli görülmesi durumunda şifreli giriş, parmak izi okumalı giriş gibi bazı ünitelere ayrı bir güvenlik sistemi kurulabilir. Son olarak fiziksel ve çevresel güvenliğin kurum içerisindeki ekipmanları da kapsadığı unutulmamalı ve bu amaçla gerekli tedbirler alınmalıdır (Doğantimur, 2009).

2.4.6 İletişim ve Operasyonel Yönetim

Bu alanda temel amaç bilgi ve verinin doğru ve güvenli bir şekilde aktarılmasıdır. Dolayısıyla haberleşme ve iletişim yönetiminde dikkat edilmesi gereken bazı önemli hususlar vardır. Bunların başında iletişim ve haberleşmede uygun prosedürlerin belirlenmesi gelmektedir. Ayrıca belirlenen bu prosedürler yazılı bir doküman haline getirilerek hem personelin hem de üçüncü tarafların bilgi edinmeleri sağlanmalıdır. Bunların yanı sıra donanım ve ağ güvenliğinin sağlanması hususlarında özel kontrol ve izleme yöntemleri geliştirilmelidir. Son olarak bilgi güvenliği yönetiminde iletişim alanında gerçekleşecek test ve iyileşmelerin parça parça farklı zamanlarda yapılması sağlanmalıdır. Böylelikle uygulamalardan kaynaklanacak riskin azaltılabileceği belirtilmektedir.

2.4.7 Erişim Kontrolü

Bilgi ve veriye ulaşımın, onu elde etmenin kontrol altına alınması gayesiyle erişim kontrolü alanında ayrı bir güvenlik tedbirlerinin alınması gerektiği düşünülmektedir. Bu tedbirler hem kullanıcı bazında hem de ağ bazında olabilir. Yetkilendirilmiş kullanıcıların kayıt olması ve kendilerine bir şifre oluşturması bu bağlamda yapılan uygulamalardan bir kaçıdır. Benzer şekilde ağ erişimi de sınırlandırılmalı ve belli prosedürlere bağlanmalıdır. Böylelikle bilgi güvenliği yönetimi alanında sıklıkla karşılaşılan yetkisiz erişim, izinsiz erişim kontrol altına alınabilir. Erişim kontrolünde ayrıca kurumda kullanılan ekipmanların da erişim amacıyla sisteme tanıtılmasının yapılması tanıtılmamış ekipmanlara kısıtlama getirilmesi gerekmektedir (ISO/IEC-17799, 2005).

2.4.8 Sistemlerin Geliştirilmesi ve Sürekliliği

Bu alan bilgi güvenliği yönetiminde kullanılan sistemin iç güvenliği ile alakalı uygulamaları kapsamaktadır. Diğer bir ifade ile güvenliğin sistem içerisine, yazılıma ve işleyişine yerleştirilmiştir. Güvenliğin sistem içerisine yerleştirilmesindeki amaç ise bilgi ile verinin gizlilik ve bütünlüğünün muhafaza edilerek uygun yöntemlerle sistem içerisinde aktarımının sağlanmasıdır. Bunun için ise sistem ve yazılımların iç işleyişlerine oto kontrol sağlayacak güvenlik uygulamalarının yüklenmesi gerekmektedir. Böylelikle bilgi akışında meydana gelecek sızıntıların ve hataların engelleneceği düşünülmektedir (Doğantimur, 2009).

2.4.9 İş Sürekliliği Yönetimi

Bilgi güvenliği yönetiminde diğer bir önemli alan ise iş sürekliliği yönetimidir. Burada temel amaç kurumun ya da organizasyonun acil duruma cevap verme kapasitesinin artırılmasıdır. Yangın, sel, deprem gibi acil durumlarda bile kurumun kritik işlemleri devam ettirebilmesi beklenmektedir. Bu çerçeve kurumdan beklenen ise yapılacak analizlerle zayıf noktaların ve risklerin tespit edilmesi, rol, görev ve sorumlulukların yer aldığı ve her aşamasının adım adım oluşturulduğu acil durum eylem planının oluşturulmasıdır. Böylelikle acil durumlarda dahi asgari iş ve işlemler güvenli bir şekilde devam edebilecektir (Kaberia, 2010).

2.4.10 Uyumluluk

Uyumluluk alanı başlığı, kurumsal bağlamda oluşturulacak sistem, yazılım ve ekipmanın önceden belirlenmiş olan kanun ve düzenlemelere uygun olması gerektiği hususuna dikkat çekmektedir. Ayrıca kanun ve düzenlemelerin yanı sıra belirlenmiş olan ve kabul edilen politika ve standartlara da uygun bir güvenlik yönetiminin oluşturulması önem arz etmektedir. Aksi takdirde oluşacak aykırılıkların sistemin sürdürülebilirliğini ve uyumluluğunu olumsuz yönde etkileyeceği belirtilmektedir (ISO/IEC TR 18044, 2010).

2.5 BİLGİ GÜVENLİĞİ YÖNETİM TEORİLERİ

Bilgi güvenliği yönetimi alanında etkinliğin artması, güvenliğin tam anlamıyla sağlanması ve ideal bir yönetimin kurulması doğrultusunda ortaya konan çeşitli

teoriler görülmektedir (Kayem ve Meinel, 2013). Bu teoriler kısaca aşağıda ele alınmaktadır.

2.5.1 Güvenlik Politikası Teorisi

Her ne kadar bilgi güvenliği yönetimi alanında güvenlik politikası teorisi önemli bir yer tutsa da bu güne kadar üzerinde hem fikir olunan ve uzlaşı sağlanmış bulunan bir teori bulunmamaktadır. Gerek içerik ve yöntem gerekse prosedürler bakımından farklılaşan bu teorilerin temel bazı noktalarda benzeştiği de görülmektedir. Bunlar:

- Bilgi güvenlik ihtiyaçlarının planlanması,
- Organizasyon yapısının oluşturulması,
- Bir politika taslağının oluşturulması ve uygulamaya konması ve
- Uygulamaya konan bu politikaların düzenli olarak gözden geçirilmesidir.

Yukarıda zikredilen ana hususları içeren bir güvenlik politikasının başarıya ulaşacağı öngörülmektedir (Puhakainen, 2006).

2.5.2 Risk Yönetim Teorisi

Risk yönetim teorisinde amaç bilgi güvenliğine yönelik riskleri makul bir seviyede kontrol altında tutmaktır. Risk yönetim teorisine göre kurumsal risk analizi ve değerlendirmesi sonucu bilgi güvenliği alanındaki zayıf noktalar ve tehditler tahmin edilip değerlendirilebilir. Bilgi güvenliği yönetiminde bir süreç olarak ele alınan risk yönetiminin kritik noktası risk değerlendirmesidir. Çünkü iyi bir risk değerlendirmesi ile kurumların hem en uygun ve maliyet etkinlik açısından en etkin stratejiyi belirleyebilecekleri öne sürülmektedir. Ayrıca kurumsal risk analizi şemasının oluşturulmasının bilgi güvenliği yönetimine yardımcı olacağı da ifade edilmektedir (Reid ve Floyd, 2001:335).

2.5.3 Kontrol ve Denetim Teorisi

Kontrol ve denetim teorisi savunucularına göre kurumlar öncelikle bilgi güvenliği kontrol sistemleri kurmalılar. Bu sistem uygulamaya konduktan sonraki aşamada ise sistemin performansını ölçmek üzere denetim mekanizmaları oluşturulmalıdır. Bilgi

güvenlik kontrol sistemi ile yasal olmayan durum, saldırı ve tehditlerin önlenebilir, tespit edilebilir ve düzeltilebilir bir hale geleceği vurgulanmaktadır. Bu noktada oluşturulacak kontrol sistemleri de önleyici kontrol sistemi, tespit edici kontrol sistemi ve düzenleyici kontrol sistemi olarak üçlü bir yapıda kurgulanıp uygulamaya konmasının yararlı olacağı belirtilmektedir. Ayrıca sistemin performansının ölçülebilmesi ve gerekli adımların atılabilmesi için düzenli aralıklarla bilgi denetimlerinin yapılmasının gerekliliği teorinin ana argümanlarından bir olduğu belirtilmektedir (Weber, 1999).

2.5.4 Yönetim Sistemi Teorisi

Kurumların ve organizasyonların "Bilgi Güvenliği Yönetim Sistemi Dokümanı" oluşturmasının ve uygulamaya koymalarının önemine vurgu yapan yönetim sistemleri teorisine göre bilginin kontrolü ve korunması bu belgenin rehberliği ile gerçekleşebilecektir. Teoriye göre oluşturulacak doküman şu altı adımı içermelidir:

- Güvenli politikasının tanımlanması,
- Bilgi güvenliği yönetim sistemi dokümanının kapsamının belirlenmesi,
- Risk değerlendirilmesinin üstlenilmesi,
- Risk yönetiminin gerçekleştirilmesi,
- Kontrol alanlarının belirlenerek kontrol uygulamalarının yapılması,
- Uygulanabilirlik beyanının hazırlanması,

Ayrıca teoride güvenlik çevresinin iyi araştırılmasının ve güvenlik standartlarının sağlıklı bir şekilde belirlenerek bilgi güvenliği tanım ve risk değerlendirilmelerinin etkin bir şekilde yapılmasının zorunluluğu vurgulanmaktadır (Hong vd., 2003:106).

2.5.5 Olasılık Teorisi

Kurum içerisinden ya da dışarıdan gelebilecek bir takım tehdit ve saldırıların önlenmesi, tespit edilmesi ve düzeltilmesi bir çeşit olasılık yönetimidir. Bu açıdan olasılık teorisini savunanlara göre bilgi güvenlik yönetimi de esasında bir çeşit olasılık yönetiminin bir parçası, bir uzantısıdır. Bu bağlamda, olasılık teorisi

kurumsal hedef ve amaçlara zamanında ve etkili bir şekilde ulaşabilmek için durumsal değişkenler ile çevresel faktörlerin doğru bir şekilde tanımlanmasının ve bu çerçevede doğru hareketin gerçekleştirilmesinin gerektiğini savunur (Luthan ve Stewart, 1977:186).

Olasılık teorisine göre bilgi güvenliği yönetimi esnasında çevresel ve teknolojik değişkenler ile yönetimsel farklılıkların tamamı ele alınıp değerlendirilmelidir. Genel olasılık yaklaşımı bilgi güvenliği yönetiminde de uygulanmaya konulmuş ve bu alanda Von Solms ve diğerleri (1994) tarafından bir bilgi güvenlik modeli oluşturulmuştur. Beş farklı güvenlik seviyesi üzerinden oluşturulan bu modelde risk yönetimi, kontrol ve denetim gibi diğer modellerin ortaya koymakta olduğu birikimlerden de istifade edildiği görülmektedir (Hong vd., 2003:112).

Bilgi güvenlik yönetiminin son derece büyük bir önem kazandığı günümüzde kurum ve kuruluşlar etkin bir yönetimin oluşturularak içerden ya da dışarıdan gelebilecek tehdit ve saldırıları önlemek, kontrol altına almak ve gerekli iyileştirmeleri yapmak amacıyla farklı yöntemler uygulamaktadırlar. Bu alanda ortaya konan teoriler kısaca yukarıda açıklanmıştır. Fakat bilgi güvenliği yönetimi bu teorilerle sınırlı olmayıp uygulamada farklı yol ve yöntemlere de rastlamak mümkündür (Young ve Leveson, 2014:33).

2.6 BİLGİ GÜVENLİĞİ YÖNETİMİNDE YAPILAN HATALAR

Bilgi güvenliği yönetiminde sıklıkla yapılan hatalar vardır. Bu hatalar içeriden ya da dışarıdan gelebilecek tehdit ve saldırılar için kapı aralamaktadır. Ayrıca düşülen bu hatalardan ders alınmaması diğer kurumlarda da bilgi güvenliği yönetimini risk altına sokmaktadır (Perrin, 2008). Basie ve Rossouuw (2004) bilgi güvenliği yönetiminde sıklıkla düşülen hataları kısaca şu şekilde sıralamaktadırlar:

- **Bilgi güvenliği yönetiminin genel yönetimin bir parçası olduğu hususunun göz ardı edilmesi:** Özellikle üst düzey yöneticilerin bilgi güvenliği yönetimine gereken önemi vermemesi ve risk yönetimi,

personel yönetimi gibi diğer farklı yönetimlerle bilgi güvenliği yönetimi arasında gerekli olan bağın kurulamaması kurumların bilgi güvenliği yönetim alanında yapmış olduğu en önemli hatalardan biri olarak görülmektedir. Oysa katılımcı ve işbirliğine dayalı yönetimlerde bilgi güvenliği yönetimi genel yönetimin en önemli parçalarındandır (Basie ve Rossouuw, 2004:371).

- **Bilginin güvenliği hususunun sadece teknik bir konu olarak algılanması:** Kurumlar genellikle bilgi güvenliğini teknik bir alan olarak algılamaktadırlar. Oysa bilgi güvenliği için yönetici ve çalışanların farkındalığının artırılması, uygun politika ve stratejilerin belirlenmesi ve risk analizi gibi pek çok unsur gerekli olup bu unsurların teknik konudan ziyade yönetsel birer unsur olduğu unutulmamalıdır.

- **Bilgi güvenliği yönetiminin dar bir çerçevede ele alınması:** Bilgi güvenliği yönetimi çok boyutlu bir disiplindir. Bu gerçek göz ardı edildiğinde hataya düşülmüş olunmaktadır. Bilgi güvenliği yönetiminin teknik, politik, etik, yasal, insani, kurumsal ve uygulama gibi farklı boyutları bulunmaktadır. Dolayısıyla yöneticilerin kapsamlı ve sağlıklı bir politika oluştururken bilgi güvenliği yönetimini bütün boyutlarıyla ele alması kurumsal bazda hataya düşülmesini engelleyecektir (Susanto ve Muhaya, 2010:3).

- **Bilgi güvenlik planının tanımlanmış riskler üzerine inşa edilmemesi:** Bilgi güvenliğinin ana gayesi kurumsal bilgiye yönelik tehdit ve risklere yönelik önlemlerin alınmasıdır. Fakat kurumlar sahip oldukları değerleri ve etraflarındaki potansiyel riskleri doğru tespit edemezlerse hazırlayacakları güvenlik planları maddi ve manevi israftan öte geçmeyecektir. Dolayısıyla kurumlar etkin bir risk analizi yapmalı ve bu analize dayalı güvenlik planları hazırlamalıdır.

- **Diğer kurum ve kuruluşların tecrübelerinden yeteri kadar istifade edilememesi:** Bilgi güvenliği yönetimi alanında ulusal ya da uluslararası kurumlarca yaşanan tecrübelerden yararlanılmalıdır. Aksi takdirde aynı hataya düşme ihtimali oldukça yüksek olup yapılan maddi yatırımlar ve harcanan emek boşa gitmiş olur. Bu bağlamda yazılı dokümanların ve sözlü konferans ve toplantıların yakından takip edilerek yaşanmış tecrübelerden yararlanılması kuruma bilgi güvenliği yönetimi alanında faydalı olacaktır.

- **Kurumsal bilgi güvenlik politikasının olmaması:** Hem birim hem de alt birim bazında hazırlanacak olan bilgi güvenliği politikasına yol gösterecek, üst çatı rolünü üstlenecek, yazılı, kısa ve anlaşılır bir kurumsal bilgi güvenlik politikasının mevcudiyeti yönetimin etkinliğini artıracaktır. Fakat böyle üst ve bağlayıcı bir politika metninin eksikliği bilgi güvenliği yönetiminde hataya neden olacaktır (Thomson, 2006:8).

- **Bilgi güvenliği uyumluluk noktasında denetim ve izleme eksikliği:** Ölçülemeyen, izlenemeyen ve yeterli bir şekilde değerlendirilemeyen hususta iyi bir yönetim ortaya konamaz. Dolayısıyla bilgi güvenliği alanında uygulamadaki politikaların diğer politikalarla arasındaki ilişki ve etkileşimin izlenmesi, gerekli uyumluluğun sağlanması oldukça önemlidir. Aksi takdirde bilgi güvenliği yönetiminde hataya düşülmesi kaçınılmaz olacaktır.

- **Uygun bilgi güvenlik yönetim yapısının olmaması:** Bilgi güvenliği yönetim alanında başarılı olmak için uygun kurumsal yapının oluşturulması gerekli olup bu yapı içerisinde roller, sorumluluklar ve görevler açık ve net bir şekilde tanımlanmalıdır. Hesap verebilirlik hususu kurum içerisinde herkes tarafından paylaşılmalıdır. Aksi takdirde içine düşülecek hatada kurum bütün sorumluluk bilgi güvenliği yöneticisine yüklenecektir. Bu durumda ise yönetimin başarısız olması kaçınılmaz olacaktır(Basie ve Rossouuw, 2004:373).

- **Kullanıcılar arasında bilgi güvenliği farkındalığın öneminin göz ardı edilmesi:** Kurumun sağlamış olduğu bilişim teknolojileri alt yapısını kullananların bilgi güvenliği alanında yeterli derecede bilgilerinin olması gerekmektedir. Bu bilinç ve farkındalık oluşmamışsa kullanıcılar sebep olacakları bozulma ve risklerin ciddiyetini kavrayamaz ve bilgi güvenliği yönetimi başarılı olamaz.

- **Bilgi güvenliği yöneticisine gerekli araç-gereç, teknik altyapı ve yetkinin verilmemesi:** Bilgi güvenliği çok boyutlu ve karmaşık bir yapıya sahiptir. Bu bağlamda yöneticinin ihtiyacı olan araç-gereç ve yetki kendisine verilmelidir. İhtiyaç duyduğu teknik alt yapı oluşturulmalıdır. Diğer taraftan genelde uygulamalarda görüldüğü üzere bilgi güvenliği yöneticisi kurum üst yöneticisi tarafından atanır ve kendisine gerekli hareket alanı ve yetki sağlanmazsa bilgi güvenliği yönetimi başarıya ulaşamaz(Basie ve Rossouuw, 2004:373).

Bilgi güvenliği yönetiminde en sık rastlanan bu hataların dikkate alınmasının ve yöneticilerin bu hususları göz önünde bulundurarak karar vermelerinin ve gerekli adımları atmalarının bilgi güvenliği yönetiminde başarı ve istikrarı getireceği düşünülmektedir.

2.7 BİLGİ GÜVENLİĞİ YÖNETİMİNE YÖNELİK TEHDİTLER

Bilgi güvenliği yönetimi alanında başarılı olmak için yukarıda kısaca sayılan hatalara düşmemek oldukça önemli olmakla birlikte tek başına yeterli değildir. Bir yandan hatalara düşmemek gerekirken diğer yandan bilgi güvenliğine yönelik tehditlerin doğru bir şekilde analiz edilerek gerekli tedbirlerin alınması zorunluluk haline gelmiştir. Bu tehditler hem içeriden hem de dışarıdan olabileceği gibi aniden gelişen ya da yavaş yavaş ortaya çıkan tehditler de olabilir (Fibikova ve Mueller, 2012:14). Genel olarak donanım ve bilişim alt yapısındaki eksiklikler, yangın, sel, deprem gibi doğal afetler, yazılım hataları, insan kaynaklı hatalar ile yanlış tasarlanmış kurum politikaları ve yönetici hatalarından kaynaklanan tehditler bilgi güvenliği yönetimindeki her daim olan tehditler olarak algılanmaktadır (Whitman, 2003:94).

Diğer taraftan özellikle hızlı gelişen teknolojik yeniliklerle birlikte söz konusu tehditlerin içerik, boyut ve etkisinin de değiştiği görülmektedir (Devost, 2000:21). Özellikle içinde bulunduğumuz zaman diliminde ve önümüzdeki beş yıl içerisinde bilgi güvenli yönetimine yönelik olası tehditler kısaca aşağıda açıklanmaktadır.

2.7.1 Ulus-Devlet Destekli Casusluk Faaliyetlerinin Yaygınlaşması

Birkaç yıl öncesine kadar devlet destekli casusluk faaliyetleri gizli tutulabiliyordu. Fakat hızla gelişen teknoloji ve iletişim alanındaki yenilik ve ilerlemeler bu ve benzeri faaliyetlerin uzun süre gizli kalamayacağını göstermiştir. Çin örneğinde olduğu gibi hükümet destekli siber saldırıların diğer ulus devletlere de yayılabileceği öngörülmektedir. Dolayısıyla uluslararası arenada devletleri de bağlayacak yaptırımları içeren üzerinde mutabakatın sağlandığı yazılı dokümanların varlığı ile ulus-devlet destekli casusluk faaliyetlerinin ve bilgi güvenliğine yönelik başta siber saldırılar olmak üzere saldırı ve tehditlerin önünün alınabileceği düşünülmektedir.

2.7.2. İnternetin Jeopolitik Sınırlara Ayrılması

Özellikle son zamanlarda ulus devletlerin internet kullanımını kontrol altına alma gayesiyle çeşitli çalışmalar yürüttüğü görülmektedir. Bu bağlamda istenmeyen içerikleri barındıran internet sitelerin erişimi filtreme ile kontrol altına alınmaya çalışılmaktadır. Ayrıca yabancı casusların kolaylıkla erişemeyecekleri ve kendi iletişimlerini güvenli bir şekilde yapacakları hükümet kontrolünde olan ayrı bir internet ağının oluşturulması çalışmalarının devam ettiği görülmektedir. Hali hazırda söylev üzerinde olan internetin jeopolitik sınırlarla bölümlenmesi ve erişimin bu sınırlara göre izne bağlanması hususu bilgi güvenliği yönetim alanındaki diğer önemli bir tehdit olarak görülmektedir (Meinrath, 2013). Oysa saldırılar karşısında endüstriyel sektörler arası bilgi paylaşım alanında gerekli olan işbirliği ve koordinasyonun oluşturularak istikrarlı bir şekilde sürdürülmesi yeterli olup jeopolitik ağ parçalanmalarına ihtiyaç duyulmayacaktır.

2.7.3. Büyük Veriler

Teknolojinin hızla ilerlemesi, hareket ve iletişimin artmasına paralel olarak her an devasa boyutta veri açığa çıkar hale gelmiştir. Bu verilerin elde edilmesi, analize tabi tutularak geliştirilip güçlendirmesinin kurumlar için bir lütuf olduğu söylenebilir.

Fakat artık terabayt, petabayt, eksabayt gibi birimlerle ifade edilen devasa büyüklükteki verilerin bilgi güvenliği yönetimi açısından bir tehlike taşıdığı söylenebilir (Zhou vd., 2014:64). Rekabetin ve ani manevra kabiliyetlerinin ön planda olduğu bir zamanda yeteri kadar hızlı olabilme adına büyük veriler diğer taraftan kurumlara yük getirmekte, kurumların hareket hızını yavaşlatmaktadır. Bunun yanı sıra büyük verilerin analiz edilmesi, anlamlandırılması, yönetim açısından oldukça zordur. Üstelik bu verilerin kaliteli veri olması gerekmektedir. Bilgi güvenliği yönetimi açısından büyük verilerin sağlıklı bir şekilde toplanması, taşınması, kontrol ve denetiminin verinin büyüklüğü nispetinde zorlaşacağı öngörülmektedir. Son olarak büyük verilerin veri hırsızlarının iştahını açtığı söylenebilir. Dolayısıyla "*büyük veri = büyük problem*" şeklinde bir ifade doğru olabilir.

2.7.4. Bilinçsizlik ve Kuşaklar Arası İletişim Problemi

Bilgi güvenliği yönetim alanındaki en büyük tehditlerden bir diğerinin bilinçsizlik ve kuşaklar arası iletişim problemi olduğu bilinmektedir. Bilgi güvenliği ve mahremiyet konusunda hem kurum çalışanları, hem veri kullanıcıları hem de yöneticilerin yeterli düzeyde bilinçli olması gerekmektedir. Maalesef bu konuda arzu edilen bilinç ve farkındalığın oluşturulamadığı görülmektedir (Peltier, 2005:41). Benzer şekilde yeni dijital nesil (Çamsarı, 2012:27) penceresinden mahremiyet, bilgi güvenliği ve kişisel verilerin güvenliği gibi konular farklı şekilde görülmektedir. Diğer bir ifade ile bilgi güvenliği konusunda nesiller arası farklı algı ve değerlerin oluştuğu görülmektedir. Dolayısıyla farklı jenerasyonların bilgi güvenliği konusunda uzlaşmaları bilgi güvenliği yönetim alanında oldukça önemlidir.

Bilgi güvenliği yönetimine yönelik tehditler yukarıda sayılanlarla sınırlı olmayıp özellikle gelişen teknoloji ve yeni uygulamalarla birlikte yeni tehditlerin de açığa çıktığı görülmektedir.

Modern kamu yönetimi anlayışı çerçevesinde bu kadar önemli olan bilgi güvenliği yönetimi ve kişisel verilerin korunması hususlarının kaçınılmaz bir sonucu olarak mahremiyet konusu karşımıza çıkarmaktadır. Çünkü kişisel verilerin muhafaza edilememesi ve bilgi güvenliğinin sağlanamaması durumlarında kişisel ya

da kurumsal mahremiyetin ihlali söz konusu olduğu bilinmektedir (Enyew, 2009). Dolayısıyla ilerleyen bölümde mahremiyet ve bu alanda etkin bir uygulama olarak kabul gören MED ele alınacaktır.

ÜÇÜNCÜ BÖLÜM

MAHREMİYET VE MAHREMİYET ETKİ DEĞERLENDİRMESİ (MED)

3.1 MAHREMİYET

3.1.1 Kavram, Tanım ve Tarihsel Gelişimi

İnsanlar kendilerine ait bir takım hususların başkaları tarafından bilinmemesini isteme eğilimindedirler. Bu noktada insanların hayatının iki tarafı olduğu ifade edilebilir. Bir tarafı herkese açıkken yani herkesin bildiği, gördüğü bir yan iken diğer tarafı başkalarının bilgisine kapalı ya da kişinin kendisi tarafından bilmesine izin veriler belli kişilerin bildiği ve özel olan taraftır (Salihpaşaoğlu, 2013:235). Özel hayat ile bütünleşmiş bir kavram olan mahremiyet ise TDK Türkçe Sözlüğünde "gizlilik" şeklinde tanımlanmaktadır (TDK, Türkçe Sözlük). Arapça "harem", "haram" köklerinden türetilmiş olan mahremiyet kelimesi diğer insanlar tarafından bilinmemesi gereken, herkesin bilmemesi gerekli olan anlamındadır (Yurtsever ve Buran, 2012:49).

İlk kez kamu alanı ile özel alan ayrımını açıklığa kavuşturma gayesiyle Aristotle tarafından kullanılan mahremiyet kavramının daha sonra John Stuart Mill ve diğer düşünürler tarafından da ele alındığı görülmektedir (DeCew, 2013). Felsefi olarak ele alınarak işlenen mahremiyet kavramının ilk kez 1890 yılında Warren ve Brandeis'in hazırlamış oldukları "Mahremiyet Hakkı" (Warren ve Brandeis, 1890:195) adlı eserde daha detaylı bir şekilde ele alındığı ve günümüzdeki mahremiyet hakkı alanındaki tartışma ve araştırmalara kaynaklık ettiği söylenebilir. Bu eserde mahremiyet *"bireyin yalnız bırakılma hakkı"* olarak tanımlanmıştır (Warren ve Brandeis, 1890:198).

İnsan Hakları Avrupa Sözleşmesi'nin "Özel ve Aile Hayatına Saygı Hakkı" başlıklı 8. maddesinde geçen;

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

2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzeninin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir."

İfadeleri de mahremiyet kavramının dayandırıldığı yasal maddelerin başında gelmektedir. Yalnız burada üzerinde tartışılan husus "özel" ve "kişisel" kavramları ile tam olarak nelerin ifade edildiği hususudur (Roagna, 2012).

Bu bağlamda kişisel bazda bazı insanların diğerlerine nazaran kendi özel yaşamlarına ya da kişisel hayatlarına daha fazla hassas yaklaştığı görülmektedir. Kişisel anlamda gözlemlenen bu husus toplumsal ya da kültürel anlamda da benzerlik göstermektedir. Diğer bir ifade ile bazı toplumların ve bazı kültürlerin diğerlerine göre özel ve kişisel alana diğerlerine göre daha fazla önem verdiği görülmektedir. Dolayısıyla mahremiyet kavramının bu kadar değişkenlik göstermesinin arkasında yatan nedenlerinden birinin de özel yaşam ve kişisel hayatların farklı şekillerde algılanması, ele alınması olduğu söylenebilir (Tahaoğlu, 2009:221).

3.1.2 Kişisel, Kurumsal ve Sosyal Mahremiyet

Yukarıda da ifade edildiği üzere kişilerin kendi başlarına faaliyetlerini sürdürdüğü, diğerlerinin rahatlıkla dokunamayacağı ve genellikle anayasal düzenleme ile koruma altına alınmış özel hayatları vardır. Bu alanın kişilerin kendilerini özgür hissetmelerini sağladığı söylenebilir. Kişiye özel olan bu alanda bireyler kendilerine ait olan ve 1995 yılında yayınlanmış olan AB direktifinde "*kim olduğu belli veya belirlenebilen bir gerçek kişiye ait tüm bilgilerdir. Belirlenebilen bir kişi doğrudan veya dolaylı olarak bir kimlik numarası referansından veya kişiye ait fiziksel, psikolojik, ekonomik, kültürel veya sosyal bilgilerden yola çıkarak tespit edilebilen bir kişidir"* şeklinde tanımlanan kişisel veri kavramı karşımıza çıkmaktadır (Duji, 1996:65). Kişisel verilerin mahremiyet içerdiği görülmektedir. Dolayısıyla kişisel mahremiyet olarak adlandırılabilen bu durum kişilerin içinde bulunduğu dinsel inanç, etnik köken, politik eğilimler, cinsel tercihler ve suç geçmişi gibi kişinin yaşam

şekline ilişkin olabilir. Benzer şekilde kişilere ait finansal kişisel veriler, biyometrik veriler ile sağlığa ilişkin veriler ve internet kullanımına ilişkin verilerinin de mahremiyet içerdiği ve doğrudan kişisel mahremiyetin söz konusu olduğu söylenebilir (Kavza, 2010).

Gerçek kişilerde olduğu gibi tüzel kişilerin de başkaları tarafından bilinmemesi istenilen özel alanlarının olduğu bir gerçektir. Bu noktada kurumsal maremiyet kavramı ortaya çıkmaktadır. Kurumsal mahremiyet kısaca kurumların özel bilgi ve verilerini içeren kurumsal alan şeklinde tanımlanabilir (Xu vd., 2011:803).

Kurumsal açıdan gizli kalması gerekli olan ve kullanımı kurumsal izne bağlı olan bütün bilgilerin Kurumsal mahremiyete girdiği ifade edilmektedir. Kurumun mali yapısı (piyasayı etkileyecek veriler), stratejik planlar (kritik amaç ve hedefleri içeren), performans programları (harcama ve ödenekleri gösteren) ve kuruma ait fiziki yapı, personel yapısı gibi bilgiler kurumsal mahremiyet çerçevesinde ele alınabilir (Kavza, 2010).

Bu noktada üzerinde durulması gerekli olan en önemli hususlardan biri de hiç kuşkusuz devlet mahremiyetidir. Daha açık bir ifade ile toplumun en temel kurumlarından biri olarak görülen devlete ait bazı bilgi ve veriler kurumsal mahremiyet açısından önemli olduğu söylenebilir. Milli Güvenlik Siyaset Belgesi diğer adıyla "kırmızı kitap" (Akay, 2009), devlet sırrı olarak adlandırılan hususlar ile devletteki istihbarat bilgilerin temel kurumların başında yer alan Devlete ait kurumsal mahremiyetin en önemli unsurlardan olduğu ifade edilebilir.

Kişisel ve kurumsal mahremiyetin yanı sıra hali hazırda tartışılmakta olan, özellikle facebook, twitter gibi sosyal ağların yaygınlaşmasıyla birlikte akademik alanda üzerinde sıklıkla konuşulan sosyal mahremiyet kavramının yeni bir kavram olduğu söylenebilir. Bu noktada Nissenbaum gibi düşünürler sosyal mahremiyet konusunun "kavramsal bütünlük" içerisinde ele alınması gerektiğini öne sürmektedirler (Nissenbaum, 2009). Dolayısıyla göreceli olarak yeni bir kavram olarak karşımıza çıkan sosyal mahremiyetin sağlıklı bir şekilde ele alınabilmesi için

hızla yaygınlaşan sosyal ağlar üzerindeki toplumsal içeriklerin açık ve net bir şekilde tanımlanması gerektiği öne sürülmektedir. Bunun yanı sıra "müsaade" unsurunun da kavramsal bütünlük ile ele alınarak işlenmesinin etkin bir sosyal mahremiyet tanımı yapılmasına yardımcı olacağı ön görülmektedir (Cohen, 2013).

3.1.3 Mahremiyet Hakkı

İlk defa 1890 yılında Warren ve Brandeis tarafından kullanılan mahremiyet hakkı kavramı üzerinde fikir birliği bulunmadığından tek bir tanımdan bahsedilmesi oldukça zordur. Yukarıda da ifade edildiği üzere Warren ve Brandeis tarafından yalnız bırakılma hakkı olarak tanımlanan mahremiyet hakkının daha iyi anlaşılması üzere ortaya çıkış dönemindeki gelişmelerin incelenmesinde fayda bulunacağı düşünülmektedir. 1800'lü yılların sonunda doğru artan nüfus ile birlikte Warren ve Brandeis de içinde yer aldıkları toplumsal yapının daha yoğun ve karmaşık bir hal aldığı gözlenmektedir. Yine aynı toplumda ve aynı dönemde Alexander Graham Bell tarafından telefonun icat edilmiş olmasının toplumsal hareketlilik ve yoğunluğu daha da artırdığı söylenebilir. Bunların yanı sıra yazılı ve sözlü basım ve yayımdaki ilerlemelerle birlikte artış gösteren dedikodu haberleri ve kişilerin özel hayatları ile alakalı haberler de mahremiyet hakkı kavramının belirtilen dönemde ortaya çıkmasının arkasında yatan önemli nedenlerden birkaçı olduğu ifade edilebilir (Glancy, 1979:11).

Warren ve Brandeis'in mahremiyet hakkı kavramını ortaya attıklarında bu hakkın genel hukuk düzenlemelerinin ve kabul görmüş genel yasaların bir unsuru olarak gördükleri söylenebilir. Bu düşünürlere göre mahremiyet hakkı kişilerin özel yaşamlarına ait kişisel veri ve bilgilerin istemedikleri kişilerle paylaşılıp paylaşılmaması noktasında izin verebilme durumudur. Kişilerin izin vermedikleri bilgilerin başkaları tarafından biliniyor olması ise kişiliği yaralayan bir durum olarak belirtilmektedir. Dolayısıyla Warren ve Brandeis'e göre kişinin psikolojik bütünlüğü mahremiyet hakkı ile korunma altına alınabilir aksi durumda kişinin psikolojik bütünlüğü bozulabilir (Glancy, 1979:17). Bu noktada mahremiyet hakkının ilk defa kullanımının arkasında yatan hukuksal nedenin kişinin psikolojik bütünlüğü ile alakalı olduğu söylenebilir.

Yasal bir kavram olan mahremiyet hakkının ilerleyen yıllarda Warren ve Brandeis'in tanımından farklı şekillerde ifade edildiği görülmektedir. Örneğin 1970'li yıllarda Westin mahremiyet hakkını *"bireylerin, grupların veya kurumların, diğerleriyle iletişime girdiklerinde kendileri hakkındaki bilgiyi ne zaman, nasıl, ne ölçüde vereceklerini belirleme yetkisi"* olarak tanımlamaktadır (Yüksel, 2009:278). Laurie'se göre ise mahremiyet hakkı, hem pozitif yükümlülükleri hem de negatif yükümlülükleri kapsar. Diğer bir ifade ile, mahremiyet hakkı, bir taraftan diğer insanların müdahalesinden muaf olma hakkını içerirken diğer taraftan uygun şartlar altında bir kimsenin özel hayatını yaşamasına yardım etme yükümlülüğünü de içerdiği söylenebilir (Laurie, 2002).

İnsanoğlunun saygınlığı ve temel insan hakları üzerinde yükselen mahremiyet hakkı kavramının zaman, mekân ve kültürel yapı açısından farklılık gösterdiği söylenebilir. Örneğin genel kabul gören mahremiyet hakkı tanımında yer alan "yalnız bırakılma" ifadesinin ne anlama geldiği; yalnız olmadan kastedilen fiziksel olarak mı yoksa ulaşılamamak anlamında mı yalnızlık kastedildiği hükmü açık değildir. Örneği somutlaştıracak olursak; bir şahıs tek başına bir adada da olsa buradan yapmış olduğu telefon konuşmaları, kurmuş olduğu diğer iletişim kanalları takip edilebilir, hatta kameralarla izlenebilir. Dolayısıyla burada yalnız ve tek başına bırakılan kişinin sahip olduğu mahremiyet hakkının çiğnenmediği söylenemez. Benzer şekilde bugün mahremiyet hakkı kapsamında olan bir husus ilerleyen zamanda bu kapsamdan çıkmış olabilir. Hatta bir kültür açısından mahremiyet hakkı kapsamında değerlendirilen bazı unsurlar farklı kültürlerde bu aynı kapsamda ele alınamayacağı ifade edilmektedir (Nissenbaum, 2009).

Mahremiyet hakkı konusunda diğer önemli bir hususun "kişinin rızası" olduğu gerçeğidir. Özellikle hızla yaygınlaşan sosyal medyada kişinin kendi rızasıyla duyurmuş olduğu özel bilgilerin mahremiyet hakkı çerçevesinde ele alınamayacağı belirtilmektedir. Benzer şekilde örneğin bir kavga esnasında taraflarca yüksek sesle ifade edilen kişisel bilgilerin oradan geçen üçüncü taraflarca duyulması, öğrenilmesi mahremiyet hakkının ihlali anlamına gelmediği bilinmektedir. Dolayısıyla mahremiyet hakkı kavramının kapsamının belirlenmesinde rızanın önemli bir unsur

olduğu ve mahremiyet hakkının farklı dinamikler etrafında oluşabileceği görülmektedir (Nissenbaum, 2009).

3.1.4 Mahremiyetin Farklı Boyutları

İlk olarak "yalnız bırakılma hakkı" olarak tanımlanan mahremiyet kavramının zaman ilerledikçe farklı şekillerde tanımlanarak ele alındığı görülmektedir. Westin'in mahremiyeti "kişisel uyum süreci" olarak tanımladığı görülmektedir (Spiekermann ve Cranor, 2009). Benzer şekilde 1975 yılında Altman'ın mahremiyet kavramını diğer insanların bilgilerine açık ya da kapalı olan alanın çerçevesinin oluşturulması süreci olarak kavramlaştırdığı bilinmektedir (Palen ve Dourish, 2003). Bu noktada yukarıda yapılan her iki tanımda da elektronik çevre ve teknolojik ilerlemelerin göz ardı edildiği görülmektedir. Fakat özellikle günümüzde e-pasaport, e-ticaret, biyometrik uygulamalar gibi e-uygulamalarla m-uygulamaların yaygınlaşması ile birlikte bireysel aktivitelerin büyük bir kısmı elektronik ortamlarda gerçekleşmeye başlamıştır. Bu çerçevede dolaylı olarak mahremiyet ihlalinin var olduğu bir dönemin yaşandığı söylenmektedir (Cranor, 2005).

Bu ve benzeri gelişmeler altında mahremiyet konusuna risk yönetiminin yanı sıra erişim kontrolleri hususlarını da kapsayan yeni yaklaşımlar kapsamında farklı bakışların ileri sürüldüğü görülmektedir. Bunlardan ilki mahremiyeti bir politik unsur olarak görmektedir. Politika aracı olarak mahremiyet çerçevesinde bilgi akışının güvenliğinin sağlanması temel esas olarak belirlenmektedir. İkinci yaklaşım ise mahremiyeti bir mühendislik tasarım aracı olarak görmektedir. Burada önemli olan geliştirilecek yazılım ve donanımlarla en az bilgi ile ihtiyacın giderilmesidir. Diğer bir ifade ile iş ve işlemlerin gerçekleştirilmesi çerçevesinde kişilerden talep edilen kişisel verilerin azaltılması gaye edinilmiş ve bu amaçla yeni yazılımların tasarlanmasının arzulandığı söylenebilir. İkinci yaklaşıma göre mahremiyet konusunun daha soyut olduğu kabul edilmektedir. Kullanıcıların beklentilerini de dikkate alan bu yaklaşımda verilerin toplanması, depolanması, transferi ve işlenmesi teknik çalışmalarda ayrıca dikkate alınmaktadır (Spiekermann ve Cranor, 2009:76).

Yukarıda bahsedilen yaklaşımların çeşitlenmesinin arkasında yatan en önemli nedenlerden birinin mahremiyetin iktisadi rasyonellik boyutunun varlığı olduğu

söylenebilir. Bir değişim değeri olan bilginin ticareti yapılan bir meta haline dönüşmüş olması bu durumu hızlandırmaktadır. Mahremiyet çerçevesinde iktisadi rasyonellik açısından alınan risk ile elde edilen kazancın iyi analiz edilmesi gerekmekte olup geliştirilecek stratejiler ona göre belirlenmelidir. Örneğin kredi kartının yaygınlaşmasının getirmiş olduğu kazanç ile mahremiyet ihlali riskinin yaratacağı kaybın etkin bir şekilde analiz edilmesi gerekmektedir (Dourish ve Anderson, 2006:328). Dolayısıyla teknoloji ilerlemeler ile gelişen e-uygulamalar, m-uygulamalar dikkate alındığında mahremiyetin farklı boyutlarının farklı şekillerde ele alındığı yaklaşımların çoğalması mümkün gözükmektedir.

3.2 MAHREMİYET YÖNETİMİ

Buraya kadar yapılan değerlendirmelerden de anlaşılacağı üzere üzerinde hem fikir olunan bilgi güvenliği ve mahremiyet tanımları bulunmamaktadır. Güvenlik ve mahremiyet arasında ilişkinin varlığı kabul edilse de farklı yazarlar tarafından konu farklı şekillerde ele alındığı görülmektedir. Bir kısım düşünürler bu iki kavramın aynı olduğunu öne sürerken bazıları da bir biriyle zıt olan ilişkili iki kavram olarak tanımlamaktadır (Herold, 2002:2).

Farklı yaklaşımların varlığına rağmen belirtilmesi gerekli olan birkaç husus vardır. İlk olarak; bu iki kavramın teknik alandan yasama alanına, kurumsal yatırımlardan personel politikasına kadar pek çok alanda atılacak adımların ve alınacak kararların odağında yer aldığı gerçeğidir. Hem güvenlik hem de mahremiyet çerçevesinde bilginin korunması ve izinsiz değiştirilmesinin önlenmesi hedeflerin başında gelmektedir. Ayrıca her iki kavramın da riskle doğrudan ya da dolaylı olarak ilişkili olduğu da bilinmektedir. Örneğin güvenli olarak tanımlamanın arkasında riskin az olduğu hususunun sosyal açıdan kabul edilebilir olması güvenliğin bir çeşit göstergesidir (Dourish ve Anderson, 2006:322).

Bu iki kavramın sahip olduğu benzerliklerin yanı sıra farklılıklardan da söz edilebilir. Örneğin Dourish ve Anderson'a (2006:320) göre mahremiyet genellikle sosyal bir olgu olarak algılanırken güvenlik daha teknik bir olgu olarak karşımıza çıkmaktadır. Genel olarak, güvenlik bir eylem iken mahremiyet bu eylemin başarılı

sonucu olarak görülebileceği gibi güvenliği bir strateji iken mahremiyeti bu stratejinin çıktısı olarak da tanımlamak mümkündür. Temelde ise güvenlik mühürlü bir zarfın tesis edilmesi iken mahremiyet bu zarf içindeki mesajın başarılı bir şekilde iletilmesi olarak tanımlanmaktadır (Herold, 2002:3).

Güvenlik ve mahremiyet konusundaki farklı yaklaşımlar dikkate alındığında genel kabul gören hususun yatırımlar güvenlik mekanizmalarını tesisi amacıyla yapılırken mahremiyetin muhafazası oluşturulan bu mekanizmalardan beklenmektedir (Anderson, 2006:21). Ayrıca bu faklı tanım ve farklı yaklaşımlara rağmen mahremiyet ve bilgi güvenliğinin etrafımızı kuşatan vazgeçilmez birer süreç olduğu kabul edilmektedir (Wallace ve Baker, 2007:41).

Bu çerçevede, hızlı bir değişimin yaşandığı günümüzde modern yönetim aracı olarak etki değerlendirmelerinin yaygınlaştığı ifade edilebilir. Özellikle yönetimde girdilerin iç dinamiklerle etkileşimini ya da dış faktörlerin etkilerinin doğuracağı olumsuz çıktıları öngörmek oldukça zordur. Dolayısıyla olumsuz çıktıların önlenebilmesi için uygulama öncesinde, uygulama esnasında ya da uygulama sonrasında geri bildirim şeklinde etki değerlendirmesi yapılabilmektedir (Rotmans, 2006:42). Bu etki değerlendirmelerine hem özel sektörde hem de kamu yönetiminde rastlamak mümkün olmakla birlikte her iki alanda da temel amacın sağlıklı politikaların geliştirilmesi, kaliteli çıktıların elde edilmesi olduğu bilinmektedir. Bu amaçla oluşturulacak etki değerlendirilmesinde iç ve dış dinamiklerin iyi analiz edilmesi, olumsuzluklar karşısında alınacak önlemlerin planlanması, stratejilerin sağlıklı bir şekilde belirlenmesi, alternatif stratejilerin oluşturulması gerekmektedir. Etki değerlendirme sürecinin amacına ulaşması için şeffaflık, etkin katılım, saydamlık ve açıklık ilkelerine bağlı kalınması iç ve dış paydaşlarla ortak akıl platformlarının düzenlenmesi önem arz etmektedir (Shaffer, 2013).

Bir sonraki kısımda, etki değerlendirme türlerine kısaca değinildikten sonra, çalışmanın temel konusunu oluşturan ve mahremiyet yönetiminin etkin araçlarından biri olan MED kapsamlı bir şekilde incelenecektir.

3.3 ETKİ DEĞERLENDİRMELERİ VE ÇEŞİTLERİ

TDK tarafından *"1. Bir şeyin nitelik ya da niceliği üstüne yapılan çalışma sonucu varılan yargı. 2. Aynı biçimdeki olayların, birtakım ölçünlere göre, önemini belirtme. 3. Türlü öğretim amaçlarının gerçekleşme oranını değişik yollarla ölçme ve ortaya çıkan sonuçlar üzerinde değer biçme"* (TDK Türkçe Sözlük) şeklinde tanımlanan değerlendirme esasında bir konunun nitelik ve nicelik yani kalite açısından ele alınarak yorumlanma süreci olarak betimlenebilir. Etki değerlendirmeleri ise kısaca mevcut ya da uygulamaya konması planlanan bir düzenlemenin, bir projenin ya da bir planın gelecekte açığa çıkacak olan etkilerinin ortaya konması ve olumsuz etkilerin de giderilmesi süreci şeklinde tanımlanabilir (Streatfield, 2009:136).

Tarihsel süreç içerisinde etki değerlendirmelerinin gelişim ve değişimine göz atacak olursak öncelikle "teknolojik değerlendirme" olarak ortaya çıktığı görülmektedir. İlk kez ABD'de kullanılan bu terim daha sonra diğer ülkelere de yayılmış ve Avrupa'da *Avrupa Parlemantosu Teknolojik Değerlendirme (EPTA)* ağı kurulmuştur (European Parliamentary Technology Assessment, 2009). Bilhassa enerji, nano-teknolojisi çerçevesinde yapılan sağlık hizmetleri ve e-devlet uygulamalarında teknolojik değerlendirmeden yararlanıldığı bilinmektedir. Daha sonra 1970'li yıllarda "etki beyanı" adı altında yöneticiler tarafından başvurulan etki değerlendirmelerinin 1980'li yılların ortalarında bugünkü adıyla yani "etki değerlendirmesi" olarak zikredildiği görülmektedir (International Association for Impact Assessment, 1999).

Modern yönetimde etkililiği her geçen gün biraz daha artan etki değerlendirmeleri sağlıktan ekonomiye, çevreden sosyal alanlara, iklimden teknolojiye birçok farklı alanda başvurulan bir süreç olarak karşımıza çıkmaktadır. Çevresel Etki Değerlendirmesi (ÇED), Stratejik Çevre Etki Değerlendirmesi (SÇED), Bütçe Etki Değerlendirmesi, Sağlık Etki Değerlendirmesi, Sosyal Etki Değerlendirmesi (SED), Mahremiyet Etki Değerlendirmesi (MED), Bütünleşik Etki Değerlendirmesi, İklim Etki Değerlendirmesi ve Düzenleyici Etki Analizi (DEA) etki değerlendirme türlerinden bir kaçıdır. Çalışmanın bu kısmında etki

değerlendirme türlerinden öne çıkan birkaç tanesine kısaca değinildikten sonra mahremiyet alanındaki etki değerlendirmeleri detaylı olarak incelenecektir.

3.3.1 Çevresel Etki Değerlendirmesi (ÇED)

Birinci Dünya Savaşı Öncesinde başlayan hızlı bir endüstrileşme ve şehirleşmenin doğal kaynakları tükettiği gözlemlenirken özellikle İkinci Dünya Savaşı sonrasında üzerinde yaşadığımız toprak, su ve çevrenin hızla kirletildiği ve tarım başta olmak üzere pek çok alanda problemlerin oluştuğu görülmüştür. Artan çevre bilinci kapsamında 1960'lı yıllarda ÇED konusunun gündeme geldiği görülmektedir. 1969 yılında ABD'de kabul edilen "Ulusal Çevre Politikası Yasası" ile birlikte ÇED'in resmiyet kazandığı ifade edilebilir (Clark ve Canter, 1997). 16 Haziran 1972 tarihli İnsan Çevresi Hakkındaki Birleşmiş Milletler Bildirgesinin 3-14 Haziran 1992 yılındaki Çevre ve Gelişim Hakkında Rio Deklarasyonu ile güçlendirildiği ve kabul edilen ilkelerle ÇED'in öneminin arttığı söylenebilir. Daha açık bir ifade ile 1970'lerin sonları ile 1980'lerin başlarında Brezilya, Çin, Filipinler ve Malezya gibi gelişmekte olan ülkelerin kendi ÇED'lerini oluşturdukları görülürken özellikle Rio Deklarasyonundan sonra Afrika ülkeleri dahil olmak üzere ÇED uygulamalarının hızla yayıldığı görülmektedir (Nugent, 2009:67).

Yukarıda kısaca tarihsel süreç içerisindeki gelişimi anlatılan ÇED'in farklı tanımları bulunmaktadır. Buna rağmen genel olarak ÇED; özel ya da kamu mercilerince uygulanması düşünülen proje, program, plan, faaliyetler ile bunlara ilişkin yatırımların içerisinde yaşadığımız çevreye doğrudan ya da dolaylı etkilerinin tüm artı ve eksileriyle birlikte ele alınarak incelenmesi süreci olarak tanımlanabilir. ÇED belirtilen plan, proje ve faaliyetlerin uygulama öncesinde yapılabildiği gibi uygulama esnasında ya da sonrasında da gerçekleştirilebilir. Temelde çevreyi etkileyecek olumsuzlukların önlenmesi ve ortaya çıkan negatif durumların ortadan kaldırılması ya da azaltılmasının amaçlandığı ÇED'de karar verici mercilerin hassasiyeti, süreci sahiplenmesi, etki değerlendirme sürecinin şeffaf ve açık bir şekilde yürütülmesi oldukça büyük önem arz etmektedir.

Çevre hukuku alanında kabul edilen genel yaklaşımın ve bu yaklaşım çerçevesinde kalkınmadaki sürdürülebilirliğin yakalanması için başvurulacak olan

ÇED'in farklı aşamaları olduğu bilinmektedir. Bu aşamalar; ön inceleme, kapsam belirleme, rapor hazırlama, rapor inceleme, karar ve denetim aşamalarıdır (Mutlu, 2011). Bu aşamaların etkin bir şekilde oluşturulması ekolojik dengenin muhafazasının sağlanmasında ve kaynak israfının önlenmesinde önemli olduğu kadar dolaylı olarak da sağlıklı bir çevre, sağlıklı bir yaşam ve sürdürülebilir bir kalkınma için de önemli olduğu vurgulanabilir (Mekuriaw ve Teffera, 2013).

3.3.2 Düzenleyici Etki Analizi (DEA)

Bir diğer etki değerlendirme çeşidi Düzenleyici Etki Analizidir. DEA kısaca hükümetlerin ya da sektörlerin uygulamaya koymayı düşündükleri plan, program, proje gibi düzenleyici işlemlerinin önceden analiz edilerek sosyal, ekonomik ve çevresel gibi çeşitli alanlarda ortaya çıkması muhtemel olumlu ya da olumsuz sonuçlarının belirlenmesi ve negatif çıktılarının azaltılması amacıyla yönetilen bir süreç olarak tanımlanabilir (Türkiye Ekonomi Politikaları Araştırma Vakfı, 2007). Farklı şekillerde de tanımlanabilen DEA'nın özellikle hükümetler tarafından başvurulmasının arkasında rasyonel politikaların geliştirilmesi, bürokrasinin politik açıdan kontrol altına alınması ve düzenleyici seçeneğinin yapısında yer alan fırsat değişikliğinin yakalanarak şeffaf ve açık bir idarenin oluşturulması amaçlarının yer aldığı söylenebilir (Radaelli ve Francesco, 2007).

İlk olarak 1975 yılında ABD'de kabul edilerek uygulanan DEA izleyen yıllarda Kanada, Meksika ve Avustralya gibi ülkelerde başarılı bir şekilde uygulanmış ve özellikle 2000'li yıllarda AB ülkeleri başta olmak üzere gelişmekte olan ülkelerin pek çoğunda hızlı bir şekilde yayılmıştır. Mevcut durumda dünya genelinde bazı ülkeler DEA'yı zorunlu tutarken bazıları bu zorunluluğu belli şartlara bağlamaktadır. Bunların yanı sıra hali hazırda uygulamanın bütün ya da kısmı olarak zorunlu olmadığı ülkelerin de mevcut olduğu görülmektedir. Türkiye'de ise DEA 17 Şubat 2006'da yayımlanan "Mevzuat Hazırlama Usul ve Esasları Hakkında Yönetmelik" ile yasal zorunluluk haline geldiği bilinmektedir (Güven, 2011:17). Altun'a (2011) göre başta kamu kurum ve kuruluşları olmak üzere farklı yapılarca etkin, güvenilir, başarılı politikalar oluşturulması, uygun stratejilerin belirlenmesi ve

ihtiyaç duyulan diğer düzenlemelerin hayata geçmesinde kilit rol oynayan DEA'nın temelde dört amacı vardır.

Bunlar:

- İdari düzenlemelerin fayda ve maliyetlerini de içeren gerçek etkilerinin anlaşılırlığının sağlanması,
- Çoklu politika amaçlarının bir araya getirilmesi,
- Şeffaflık ve danışma sürecinin iyileştirilmesi,
- İdarenin hesap verebilirliğinin arttırılması.

Sadece yukarıda sayılan amaçlarla sınırlı olmayan DEA'nın başarılı bir şekilde uygulanabilmesi için bazı ön şartların gerekli olduğu söylenebilir. Şeffaflık, profesyonellik, bağımsızlık, yeterli zaman, istek, sağlıklı bir veri tabanı ve uygun analitik teknikler varlığı aranılan ön şartlardan bir kaçıdır.

Jacops tarafından "küresel bir norm" ve McGarity tarafından ise "tuhaf bir yeni oluşum" şeklinde tanımlanan DEA'yı zorunlu hale getiren en önemli dış faktörün piyasadaki asimetrik bilgi olduğu ifade edilebilir. Çünkü karar mekanizmalarının etkinliğinin artması ve doğru politikaların ortaya konması asimetrik bilginin doğurmuş olduğu boşluğun giderilmesi ile mümkün olacağı bilinmektedir (Radaelli ve Francesco, 2007). Dolayısıyla başarılı bir şekilde uygulanan DEA dolaylı olarak yoksulluğun azaltılmasında, ekonomik kalkınmanın sağlanmasında ve ulusal ekonominin rekabet gücünün artırılmasında önemli rol oynadığı ifade edilebilir.

3.4 MAHREMİYET ETKİ DEĞERLENDİRMESİ

Mahremiyet konusunun toplumlar arası hızla yayıldığı görülmektedir. Özellikle bilgi ve iletişim teknolojilerindeki ilerlemeler ile sosyal ve ekonomik kurumların çoğalmasının bu yayılmayı hızlandırdığı söylenebilir. Bu durumun bir sonucu olarak, içinde bulunduğumuz çağda bilgi toplumlarından "mahremiyet toplumlarına" doğru bir değişimin varlığından bahsedilebilir (Lavanya vd., 2012:269). Bu noktada Ayn Rand tarafından ifade edilen *"medeniyet mahremiyet toplumuna doğru gerçekleşen*

bir ilerlemedir" (Max, 2011:1) ifadesinin mevcut gelişmelerle desteklendiği söylenebilir. Mahremiyet konusunun bu denli önem taşıdığı bir zamanda MED'in de ön plana çıktığı görülmektedir. Özellikle 1990'lı yılların ikinci yarısında USA, AB, Kanada, Avustralya, Hong Kong ve Yeni Zelanda başta olmak üzere pek çok gelişmiş ve gelişmekte olan toplumlarda uygulamaya konan MED çalışmanın bu bölümünde detaylı olarak ele alınmaktadır.

3.4.1 MED Kavramı ve Tanımı

Etki değerlendirme türlerinden olan ve bu çalışmanın ana konularından birini oluşturan "*Privacy Impact Assessment*" dilimize "*Gizlilik Etki Değerlendirmesi*" (ULTRANET, 2010) ya da "*Mahremiyet Etki Değerlendirmesi*" (Tataroğlu, 2013) şeklinde çevrilen etki değerlendirme yöntemi bu çalışmada MED olarak zikredilmektedir. Rasyonel yönetim tekniklerinin ve modern yönetim anlayışının doğal bir unsuru olarak görülen MED'in farklı tanımlarına rastlamak mümkündür. Bu noktada farklı tanımlara bakıldığında MED kavramının ÇED kavramı tanımından esinlenerek ortaya konduğu ve kısaca kişinin ya da kurumların mahremiyetini olumlu ya da olumsuz etkileyebilecek plan, proje, program ve uygulamaların önceden, uygulama esnasında ya da sonradan analiz edilerek mahremiyet üzerindeki etki ve sonuçlarının belirlenmesi süreci şeklinde tanımlandığı görülmektedir (United Nations Environment Programme, 2002).

Çok farklı tanımları yapılan MED kavramını ilk tanımlayanlardan biri Clarke olmuştur. 1998 yılında Clarke MED'i "olası mahremiyet ihlalini içeren bir öneri ya da planın potansiyel etki ve sonuçlarının ortaya konup incelendiği süreç" olarak tanımlamaktadır (Clarke, 1998:14). Bu noktada, MED kavramlarını ilk kullanan ülkeler başta olmak üzere çeşitli ulusal veya yerel bazda hazırlanan yasal, idari veya politik metinlerde yer alan kısa tanımlara değinilmesinin faydalı olacağı düşünülmektedir. Bu tanımlar aşağıda yer alan tabloda bir araya getirilmiştir.

Tablo 1: Farklı Ülkelerde Yer Alan Resmi Dokümanlarda Yapılan Farklı MED Tanımları

Ülke	Tanım
Yeni Zelenda	"bir önerinin mahremiyet üzerindeki etkilerinin değerlendirildiği sistematik bir süreç" (Clarke, 2009:130).
Kanada	"mahremiyet riskinin azaltılması ve tamamen bilgiye dayalı politikalaırn güçlendirilmesi için mahremiyetin tasarlanmış ya da gözden geçirilmiş programlarla birlikte ele alındığı uygun çerçevenin oluşturulması ve diğer yasal düzenlemelerle uyumluluk derecesinin tanımlanması"(Tancock vd., 2010).
Avustralya	"mahremiyet üzerindeki mevcut ya da olası etkilerin değerlendirilmesi ve bu etkilerin nasıl azaltılacağı hususlarının ortaya konması"
ABD	"mahremiyet koruma sisteminin diğer sistemlerle uyum içinde bütünleşmesinin sağlanması için tanımlanabilir biçimdeki bilginin nasıl toplandığı, depolandığı, korunduğu, paylaşıldığı ve yönetildiği hususlarının analiz edilmesi"(United States Department of Homeland Security, 2007)
İngiltere	"MED bilginin toplanması, işlenmesi ve yok edilmesinde mahremiyet risklerinin belirlenmesine yardım eden bir süreçtir. MED mahremiyet risklerinin belirlenmesine, problemlerin öngörülmesine ve gerekli çözümlerin ortaya konmasını sağlamaktadır."(Information Commissioner's Office, 2009)

3.4.2 MED'in Ortaya Çıkışı ve Tarihsel Gelişimi

MED'in çıkış noktasının tam olarak bilinmesi neredeyse imkânsızdır. Yukarıda da ifade edildiği gibi farklı isimler altında ve farklı amaçlarla başvurulan kavramlar zaman içerisinde MED olarak karşımıza çıkmaktadır. Özellikle endüstrileşmiş toplumlarda risk yönetimi çerçevesinde yeni bir teknoloji, idari süreç, hizmet ya da ürünün fayda analizinin önceden yapılması hem proje sahipleri hem de toplumun geneli için oldukça önemlidir. Çünkü özellikle son zamanlarda olumlu yanları ispatlanmamış sağlık ve teknolojik alanlardaki yenilikler tehlikeli olarak algılanmaktadır. Dolayısıyla toplumdaki bu değişiklikler MED'in ortaya çıkışını hızlandırmıştır (Clarke, 2004:21).

MED'in ortaya çıkışı noktasında farklı iddialar bulunmaktadır. Bunlardan ilki MED'in ilk olarak ABD'de ortaya çıktığı düşüncesidir. Buna göre 1974 yılında ABD'de Mahremiyet Yasasının kabulünden sonra "Mahremiyetin Korunması Çalışma Komisyonu" tarafından bir rapor hazırlandığı görülmektedir. Bu süreci uzantısında ise 1990'da "Veri Eşleşme Program Yasası" ile Maliye ile Sosyal Güvelik Kurumları arasındaki veri transferi üzerinde önemle durulan bir konu olarak ele alınmaya başlanıştır. MED'in ilk önce ABD'de ortaya çıktığı savını savunanlara göre 1990'daki bu yasanın MED mantığı ve anlayışı çerçevesinde hazırlanmıştır. Çünkü bu yasa maliyet-fayda analizinin yapılmış olmasını ve hangi metotların veri eşleştirmede kullanılacağı gibi bir takım hususları zorunlu kılmaktadır (Tancock, vd., 2010).

ABD ve Avustralya'da MED'in farklı form ve adlar altında 1990'lı yılların ikinci yarısında kullanıldığı öne sürürse de bu savın aksine akademik literatürde MED ifadesinin ilk kez Yeni Zelanda'da kullanıldığı görülmektedir. 1996 yılında Yardımcı Komiser Blair Stewart'ın hazırlamış olduğu raporda dile getirdiği MED ifadesi sonraki çalışmalarında da genişletilerek ele alınmış ve uzmanlar tarafından derinlemesine tartışılan bir konu olarak gelişmiştir (Stewart, 1996). Dolayısıyla her ne kadar MED kavramının ortaya çıkışı konusunda farklı savlar öne sürürse de Yeni Zelanda'da Blair Stewart 1996 yılındaki çalışmasının MED kavramının kullanıldığı ilk yazılı metin olarak kabul edildiği görülmektedir. Daha sonra özellikle son 15 yıldır MED Avusturalya ve Kanada başta olmak üzere AB ülkeleri ve gelişmekte olan ülkelerde hızla yaygınlaşmış ve üzerinde tartışılan bir konu halini almıştır. 2007 yılında İngiltere'de "Bilgi Komiserleri Ofisi" tarafından MED Rehberi hazırlanmıştır. Devamında ise ilk kez "Ulusal Politika Geliştirme Kurumu" tarafından ilk kez MED uygulandığı görülmektedir (Tancock, vd., 2010). İngiltere, İrlanda ve diğer AB ülkeleri ile MED uygulamasına başvuran ülkelerde MED kullanımını zorunlu kılan bir takım nedenler sayılabilir. Bu nedenlerin bir kısmı aşağıda sayılmaktadır.

3.4.3 MED'i Zorunlu Kılan Nedenler

MED'i gerekli kılan nedenlerin başında XX. Yüzyılın ikinci yarısının sonralarında hükümet ve organizasyonların faaliyet ve etki alanlarında meydana gelen değişiklik gelmektedir. Diğer bir ifade ile bu dönemde mahremiyet alanlarına devletin ve diğer kurum ve kuruluşların yoğun bir şekilde müdahil oldukları görülmektedir. Bu durumun toplumda oluşturmuş olduğu tepkinin doğal bir yansıması olarak vatandaşların kurum ve kuruluşların mahremiyet alanındaki aktivite ve faaliyetleri daha yakından takip etme isteklerinin yükseldiği görülmektedir (Bennett vd., 2007).

İkinci bir neden ise rasyonel yönetim anlayışının artan popülaritesidir. Özellikle rasyonel yönetimin üzerinde durduğu risk değerlendirme ve risk yönetim hususları MED'i gerekli kılmaktadır. Üçüncü bir husus ise mahremiyet ihlallerinin yargıya taşınmış olması MED'i gerekli kılan durumlardır. Özellikle artan teknolojik imkanlar ile mahremiyet ihlallerinin de arttığı ve bu durumun yargı taşınmasının da MED'i gündeme getirdiği görülmektedir. Yeni Zelanda'da MED ilk kez kullanan Stewart'ın da çalışmasının yargı alanında yaptığı bilinmektedir. Son olarak ise artan veri paylaşım ihtiyacının ve bu doğrultuda yapılan veri transferlerinin MED'i gerekli kıldığı söylenebilir. Bu paylaşım devlet kurumları arasında gerçekleşen ulusal veri paylaşımı olabileceği gibi sınır birimlerinde yapılan uluslararası veri paylaşımı gibi geniş ölçekli veri paylaşımı da gerçekleşebilmektedir (Tancock, vd., 2010).

3.4.4 MED'i Diğer Uygulamalardan Farklı Kılan Hususlar

Farklı ülkelerdeki dokümanlarda yer alan farklı tanımlar dikkate alındığında MED'i diğer bir takım sistem, aktivite ve süreçlerden farklı kılan çeşitli özelliklerin var olduğu görülmektedir. Bu özelliklerden ilki; MED'in kurumsal mahremiyet politikalarından farklı olarak uygulamada olan ya da uygulamaya konması düşünülen bir proje, program veya yeni bir girişim olduğu gerçeğidir. Diğer bir ifade ile benimsenen kurumsal mahremiyet politikaları kurumun var oluşundan sonuna kadar devam ederken MED yeni bir uygulama, plan, proje ya da program ile başlayan bir süreçtir (Information Commissioner's Office, 2014). İkinci olarak, MED ileriye dönük olarak çalıştırılmaktadır. Diğer bir ifade ile başlamış olan ya da başlanması planlanan bir program için başvurulan MED'den geriye dönük olarak yararlanılamaz.

Bu özelliği ile MED mahremiyet denetiminden ayrılmaktadır. Çünkü mahremiyet denetimi geriye doğru işlemektedir ve denetim sonucunda çeşitli yaptırımların uygulanması söz konudur (Shroff, 2007:17-23).

Üçüncü olarak MED tanımından da anlaşılacağı üzere geniş bir alanda etki göstermektedir. Diğer bir ifade ile sadece veri mahremiyeti, ya da kişi mahremiyeti gibi dar alanda etkili olmak yerine kişisel veri, kişisel iletişim, kurumsal veri ve kişisel davranış gibi geniş bir yelpazede kendini göstermektedir. Dolayısıyla MED'i sadece kişisel veri mahremiyetinin korunması hususunda çalışan bir süreç olarak görmemek gerekmektedir (Tancock, vd., 2010). Son olarak, MED sadece risk ve tehlike alanlarını belirleyen bir tespit aracı olmanın ötesinde problemleri önceden teşhis eden ve bu doğrultuda çözüm üreten, belirlenecek politikalara ve izlenecek stratejilere rehberlik eden bir enstrümandır.

3.4.5 MED'in Amaçları

MED uygulamasının gerçekleştirilmesinde çeşitli amaçlar olduğu bilinmektedir. Bu amaçlar organizasyonun büyüklüğü, kurumsal yapısı ve yönetim anlayışındaki farklılıklara göre değişebildiği gibi içinde bulunulan hukuki ve idari sistemin işleyişi ile toplumsal beklentilerdeki farklılıklara göre de değişebilmektedir. Buna rağmen genel olarak MED uygulamasının arkasında bulunan temel amaçlar aşağıda kısaca açıklanmaktadır (Information Commissioner's Office, 2014).

MED'in ilk amacının kişisel ya da kurumsal mahremiyet ihlallerinin engellenmesi olduğu ifade edilebilir. Özellikle kişisel verilerin çalınması, değiştirilmesi, yasal olmayan bir şekilde elde edilerek farklı amaçlar doğrultusunda işlenmesinin önlenmesi MED'in amaçlarından biridir. İkinci olarak; kişisel verilerin korunması yasası, insan hakları, anayasa gibi temel yasalarla ve alt mevzuatta öngörülen gereksinimlerin karşılanması arzulanmaktadır. Diğer bir ifade ile uygulanması düşünülen proje, faaliyet, program ya da düzenlemenin yasal gereksinimleri karşılayıp karşılamadığı MED ile ortaya konmakta ve gerekli değişiklikler yapılmaktadır. MED'in diğer bir amacı risk alanlarının tanımlanıp ortaya konmasıdır. Böylelikle yönetimde etkinlik sağlanmış olacaktır. Dördüncü amaç olarak pratikte ve uygulamada meydana çıkacak gereksiz harcamaların önüne

geçmek sayılabilir. Özellikle proje ödeneklerinin serbest bırakılmadan önce yapılması MED'in bu anlamda etkililiğini artıracaktır. Bir diğer önemli amaç; güven unsurunun başat rol oynadığı günümüz piyasalarında kurum ve kuruluşlar kendilerine duyulan güvenin pekişmesi ve sahip olduğu ün ve prestijin devam etmesini istemektedirler. Dolayısıyla MED sayesinde bu istekleri büyük oranda gerçekleşmiş olmaktadır. Bu amaçlara yönetime yol gösterme, izlenecek stratejilerin belirlenmesinde karar verici mercilere yardımcı olma, şeffaf ve hesap verebilir bir kurum olma gibi amaçlar da sayılabilir (Wright, 2012:56).

3.5 TEMEL MED UNSURLARI

Yukarıda da belirtildiği üzere tek bir MED kavramı olmamakla birlikte bir MED uygulamasında herkes tarafından kabul edilen temel ilke ve unsurlar da bulunmamaktadır. Bununla birlikte MED sürecinde yer alması gerekli olduğuna inanılan bazı temel unsurlardan bahsetmek mümkündür. Bu unsurlardan önemli olan birkaç tanesi kısaca aşağıda açıklanmaktadır.

3.5.1 Bir Süreç Olması

MED'i oluşturan temel unsurlardan ilki MED'in bir süreç olduğu gerçeğidir. MED belli bir zaman diliminde hazırlanıp tamamlanan bir rapor değildir. Bilakis MED bir proje öncesinde başlayan, proje devam ettiği sürece devam eden bir süreçtir. Diğer bir ifade ile MED'te temel gaye mahremiyetin muhafaza edilmesi, mahremiyet ihlallerinin önlenmesi ve etkilerinin azaltılması iken, mahremiyet ihlalleri ile veri hırsızlığının proje öncesi ve sonrasında dahi gerçekleşme ihtimallerine binaen MED de bir süreç olarak karşımıza çıkmaktadır. Bu süreç sonunda MED raporu hazırlanır ve hazırlanan bu raporun sürecin bir sonucu olarak algılanması gerekmektedir (Hert vd., 2012).

Bu sürecin ana aşamaları ise kısaca şu şekildedir (Wright ve Wadhwa, 2012:6):

- MED'in gerekliliğinin belirlenmesi
- ME uygulayacak olan bir ekibin oluşturulması
- Öneri aşamasındaki projenin tanımlanması

- Proje kapsamındaki bilgi akışının ve diğer mahremiyet etkilerinin analiz edilmesi
- İç ve dış paydaşlarla fikir alışverişinin düzenlenmesi
- Risk yönetimi
- Yasal uygunluk kontrolünün gerçekleşmesi
- Öneri ve tavsiyelerin formüle edilmesi
- MED raporunun hazırlanması ve yayımlanması
- MED kapsamındaki önerilerin uygulanması
- Dış denetimin gerçekleştirilmesi
- Gerekmesi durumunda MED'in yeniden değerlendirilmesi.

3.5.2 Ölçeklenebilir Olması

Hem özel sektörde hem de kamuda yer alan kurum ve kuruluşlar farklı boyut ve farklı ölçektedir. Ayrıca bu kurum ve kuruluşların mahremiyet ile bağları farklı boyutta ve veri korumacılığında farklı donanım ve tecrübelere sahiptirler. Dolayısıyla MED politikaları kurum ve kuruluşlara kendilerine uygun bir MED uygulama imkânı sunmalıdır. Bütün organizasyonlardan tek tip bir MED uygulamalarını beklemek imkânsızdır. Bu bağlamda MED'in ölçeği ve kapsamı uygulayıcı kuruma uygun olabilecek esnekliğe sahip olması oldukça önemli olmakla birlikte MED'in temel unsurlarındandır (Kelter vd., 2010)

3.5.3 Kişisel Verilerin Korunmasıyla Sınırlı Olmaması

MED'in diğer bir önemli unsuru sürecin sadece kişisel verilerin korunmasıyla sınırlanamamasıdır. Yukarıda da değinildiği gibi mahremiyet kavramının içerik ve kapsamının sabit olmadığı ortaya konan eserlerden anlaşılmaktadır. Örneğin Clarke'e göre mahremiyet dört kategoriden oluşmaktadır. Bunlar; kişisel mahremiyet, kişisel iletişim mahremiyeti, kişisel bilgi mahremiyeti ve kişisel davranış mahremiyetidir (Clarke, 2006:2). Solove ise mahremiyeti altı kategoriye ayırmaktadır. Ayrıca yer-mekan mahremiyeti ve duygu-düşünce mahremiyeti gibi mahremiyetin farklı boyutlarının da ele alındığı görülmektedir (Solove, 2002). Dolayısıyla mahremiyetin farklı boyut ve kategorilerde ele alındığı unutulmamalı.

Mahremiyetin farklı boyutlarının ortaya konduğu bu noktada önemli bir tartışma daha açığa çıkmaktadır. Tartışma konusu olan mahremiyet ve verilerin korunması arasındaki ilişki hakkında farklı argümanlar ileri sürülmektedir. Bunlardan ilki mahremiyetin veri korumacılığını kapsadığı düşüncesidir ve mahremiyeti üst çatı olarak görmektedir. Diğer taraftan ise veri korumacılığının mahremiyeti kapsadığını ve esas üst çatının veri korumacılığı olduğu düşüncesi de desteklenmektedir(Hert ve Gutwirth, 2003). Dolayısıyla MED'in sadece kişisel verilerin korunmasıyla sınırlı tutulmayıp mahremiyetin farklı boyutlarıyla birlikte oluşturulması gerekmekte olup bu çerçevede ise terminolojinin açık, net bir şekilde oluşturulması gerekmektedir.

3.5.4 Hesap Verilebilirliği Sağlaması

Bilgi ve iletişim teknolojileri alanında etkili bir veri koruma için hesap verme temelleri üzerine inşa edilen mekanizmalardan bahsedilebilir. Bu mekanizmalarda dar anlamda hesap verilebilirlik alınan önlem ve uygulamalar olmakla birlikte neden bu önlem ve uygulamaların alındığının izahı daha bir önem taşımaktadır. Oysa MED'de hesap verilebilirlik daha geniş ve daha farklı ele alınmaktadır. Diğer bir ifade ile bir taraftan MED kurum ve kuruluşlarda hesap verilebilirlik ilkesinin oluşup yerleşmesine katkıda bulunurken diğer taraftan MED uygulamasının başarılı bir şekilde noktalanabilmesi için kurum ve kuruluşlarda hesap verilebilirlik ilkesinin etkin bir şekilde işlemesi gerekmektedir. Dolayasıyla MED'in en önemli unsurlarından biri olan hesap verilebilirlik kavramı geniş bir yelpazede ele alınmalı ve diğer unsur ve mekanizmalarla etkileşimi net bir şekilde belirlenmelidir (European Commission, 2010).

3.5.5 Şeffaflık

Demokrasinin en önemli gerekliliklerinden biri olan şeffaflık MED uygulamalarının da vazgeçilmez unsurlarındandır. Özel sektör ve kamuda farklı seviyelerde algılanan şeffaflık yukarıda zikredilen hesap verilebilirlik unsurunun ikizi konumundadır. Daha açık bir ifade ile her adımı şeffaf olan bir süreç hesap verilebilirlik açısından başarılı olarak yürütülmüş bir süreç olarak algılanmaktadır (Demirkıran vd., 2011:176).

MED'de şeffaflık iki farklı noktada ele alınabilir. Bunlardan ilki MED sürecinde oluşturulan "süreç şeffaflığıdır" ikincisi ise birbiri ile ilişkili olan bilgilerin açıklanmasında ortaya çıkan "ifşa şeffaflığıdır". İfşa şeffaflığında ise özellikle paydaşların sürece aktif katılımı ve süreç sonrasında MED raporunun yayımlanması oldukça büyük önem arz etmektedir. İlk olarak paydaşların sürece aktif bir şekilde katılmaları ve taraflar arası fikir alış verişinin gerçekleşmesi MED sürecinin sağlıklı bir şekilde işlemesini sağlayacaktır. Özellikle risk analizinin objektif bir şekilde gerçekleşmesinde paydaşların rolü yadsınamaz. Böylelikle risk alanları daha net bir şekilde ortaya konacak ve bunların etkileri doğru bir şekilde tanımlanacaktır (Hert vd., 2012). Ayrıca temel haklar çerçevesinde paydaşların görüş ve önerilerinin alınması karar alma sürecinin adil bir şekilde noktalanmasına yardımcı olacaktır. Bütün bunlara ek olarak paydaşların etki katılımı MED de şeffaflık ilkesini de güçlendirecektir (Wright ve Hert, 2012:462).

İfşa şeffaflığında diğer bir önemli husus MED raporunun yayımlanmasıdır. Şeffaflık unsurunun gerekliliği olan bu durumda kurum ve kuruluşun iç ve dış paydaşlar nezdinde oluşturmuş olduğu güvenirlik pekişecektir. Fakat kurum ve kuruluşlar MED sürecinde şeffaflık ilkesi çerçevesinde hareket ederken "devlet sırrı" ve "hassas verilere" yaklaşımlarında hem mevzuat hem de etik kurallar çerçevesinde gerekli hassasiyeti göstermeleri gerekmektedir. Bu noktada veri tasnifinin yapılması şeffaflık ilkesinin işletiminde faydalı olacaktır (Hert vd., 2012).

3.5.6 Risk Yönetimi ve Mevzuat Uygunluğunun Kontrolü

MED'i oluşturan unsurlardan bir diğeri hiç kuşkusuz risk yönetimi ve yasal uygunluğun kontrolüdür. Bu çerçevede ilk olarak risk değerlendirmesinin yapılması ve belirlenen risklerin azaltılması gerekmektedir. İkinci olarak ise yasal uygunluğun kontrolü gerçekleştirilmelidir. Yasal uygunluk kontrolünde amaç uygulanan MED'in diğer mahremiyet ve veri koruma kanunlarına aykırı olmadığının ortaya konmasıdır. MED ile uygulamada olan mevzuat uyumlu olmalı ve aralarında bir ahenk oluşturulmalıdır. Bu noktada Risk yönetimi daha geniş bir kavram olmakla birlikte uyumluluk kontrolü ile aralarında bir etkileşimin olduğu unutulmamalı (Information Commissioner's Office, 2014).

3.5.7 Denetim ve Gözden Geçirme

Denetim ile MED uygulamasında başvurulması gerekli olan dış denetim unsuru kastedilmektedir. MED sürecinin ve süreç sonunda hazırlanan raporun bağımsız akredite edilmiş dış denetçiler tarafından denetlenmesi ve uygulamanın belirli periyotlarda gözden geçirilmesi MED'in önemli unsurları arasındadır. Bu ilkenin hesap verilebilirlik ilkesi ile el ele gittiği ve birbirlerini tamamladıkları ifade edilebilir (Hert vd., 2012).

3.6 MED'İN FAYDALARI VE MED UYGULAMASININ NEDENLERİ

MED uygulamalarının pek çok faydası bulunaktadır. Bu faydaları ekonomik, sosyal ve toplumsal faydalar altında sınıflara ayırmak mümkün olmakla birlikte kişiye yönelik, Kuruma yönelik, üçüncü taraf ve topluma yönelik faydalar şeklinde de tasnif etmek mümkündür. Fakat çalışmamızda bu faydalara kısaca değinileceği için maddeler halinde ifade etmenin daha yararlı olacağı düşünülmüştür. MED'in faydaları şu şekilde sıralanabilir (Wright, 2012:58)

- MED sayesinde risk alanlarının tanımlanması ve etkin bir risk yönetiminin gerçekleştirilmesi sağlanmış olur.

- MED ile gereksiz harcamaların önü alınmış olunur. Özellikle piyasa sürecinde yapılan müdahalelerin proje öncesinde yapılan müdahalelere nazaran çok daha maliyetli olduğu bir dönemde MED uygulaması proje bütçesi tekrar gözden geçirilmiş gereksiz harcamalar engellenmiş olmaktadır.

- MED ile risk alanlarının önceden tespit edilmesi Kuruma alınması gerekli olan önlemler ve çözümler için yeteri kadar zaman ve kaynak imkanı bulma fırsatı verecektir. Aksi takdirde uygulama esnasında sorunun tespit edilmesi ve gerekli çözümün ortaya konması için hem zaman, hem ekipman hem de maddi kaynak imkanı bulunmayabilir.

- MED vatandaşlara hangi kişisel verilerinin ne zaman, kim tarafından, hangi amaçlarla kullanılacağı, bu verilerin nerede ve nasıl korunup hangi yolla yok edileceği hakkında gerekli bilgiyi vererek vatandaşlarda MED düzenleyen

kuruma karşı güven duygusunun oluşmasına yardımcı olmaktadır (Van vd., 2012:121).

- Genellikle bir erken uyarı sistemi olarak tanımlanan MED potansiyel mahremiyet problemlerinin önceden belirlenmesini ve yüksek tutarda harcamalar yapılmadan önce gerekli tedbirlerin alınmasını sağlar.

- Her türlü önleme rağmen mahremiyet ihlali, verilerin çalınması ve kötü niyetli amaçlar doğrultusunda kullanılması durumunda MED sonucu hazırlanmış olan rapor sayesinde MED uygulayan kurumun yasal mevzuata uygun hareket ettiği, mahremiyet ihlalini önlemek için gerekli adımları attığı ortaya konmaktadır. Böylelikle kurumun güvenirlik, saygınlık ve prestij kaybı azaltılmış olur (Stewart, 1999).

- MED mahremiyet konusuna sistematik bir yaklaşımın ortaya konmasını sağlar. Özellikle karar alma sürecinde fikir alışverişinin sağlanmasına ve kurum içi iletişim kopukluklarının ortadan kalkmasına yardımcı olur.

- MED disipline edilmiş bir süreç olduğu için bu süreçte şeffaflığa ayrı bir önem verir. MED düzenleyen kurum ve kuruluşlar mahremiyet konusundaki şeffaflık hususundaki hassasiyetlerini ortaya koymuş olmaktadırlar. Böylelikle toplumdaki itibar ve güvenirlikleri artmaktadır (David, 2000).

- MED düzenleyen kurumlar kişisel mahremiyet konusunun kurumsal öncelikleri arasında olduğunu belirtmekte ve kendinden hizmet alanların yanı sıra kendi personeline de mahremiyet konusunun önemini aktarmaktadır. Böylelikle MED sürecinde kurumsal değerlerin çalışanlar tarafından tasdik edilip kabullenilmesi de sağlanmış olur (Cavoukian, 2005).

- MED sürecinde kurum iç ve dış paydaşlarla iletişime açık olduğunu ortaya koymaktadır. Paydaş analiz çalışmaları bu durumun en önemli göstergelerindendir.

- MED uygulaması projelerin daha uzun ömürlü olmasına yardımcı olur.

Yukarıda sayılan faydalarının yanı sıra MED uygulaması yargı yükünün azaltılmasında da önemli bir rol üstlenmektedir. MED ile birlikte risk alanları önceden belirlenip gerekli tedbirler alındığından uygulama esnasında yürütmenin durdurulması ya da tazminat gibi davaların açılma olasılığı da en aza indirgenmiş olmaktadır. Örneğin, Sosyal Güvenlik Kurumu (SGK) tarafından 2013 yılında özel sağlık hizmet sunucularında kullanılması zorunluluk haline getirilen Avuç İçi Damar İzi Tarama Sisteminin yürütmesi Danıştay İdari Dava Daireler Kurulu tarafından durdurulmuştur. Devam eden süreçte 03/04/2015 tarihli Resmi Gazetede yayımlanan Anayasa Mahkemesi'nin 2014/180 Esas, K.2015/30 sayılı ve 19/03/2015 tarihli kararı ile Danıştay İdari Dava Daireler Kurulu tarafından verilen yürütmeyi durdurma kararları kaldırılmıştır. Dolayısıyla MED uygulamaları bu ve benzeri dava sayısını azaltacağı gibi maddi ve manevi tazminatların da önüne geçecektir (Sosyal Güvenlik Kurumu, 2015)

MED'in faydalarını ortaya koymakla birlikte Kurumları MED yapmaya iten nedenler de kendiliğinden açığa çıkmış bulunmaktadır. Fakat organizasyonlar açısından yeni ya da mevcut uygulama, hizmet veya çıktılardaki potansiyel risklerin tanımlanması MED sayesinde gerçekleştirilebilmektedir. Ayrıca Organizasyonlar piyasada güven tesis etmek, eğer sahiplerse borsada işlem gören kıymetli kâğıtların değer kazanması için MED'e başvurabilmektedirler. Bütün bunların yanı sıra güvenlik zafiyeti olan, aciz, istikrarsız, başarısız, risk yönetimini gerçekleştiremeyen bir organizasyon imajı vererek bu durumun doğuracağı sosyal ve ekonomik zorluklarla karşılaşmamak için kurum ve kuruluşlar MED yapmaktadırlar.

MED'in faydaları ve organizasyonları MED uygulamasına iten nedenler genel olarak yukarıda sıralanmaktadır. Bu noktada faydalar ve MED yapma nedenlerinin yukarıda sayılanlarla sınırlı olmadığının ve her bir organizasyonun kendine özgü yarar ve nedenlerinin bulunduğunun belirtilmesi gerekmektedir. Diğer bir ifade ile bazı şirketlerin, MED yapmalarında kendilerine has sebepleri vardır. Örneğin Nokia'nın mahremiyet değerlendirmesi yapma konusunda dört nedeni vardır.

Bunlar (Wright, 2012):

1. Mahremiyet şartlarının uygulanmasını ölçmek, mevcut statüyü kavramak (riskler, kontroller, temel nedenler, vs.);
2. Yeni projelerin mahremiyet şartlarını takip edip etmediğini öğrenmek;
3. Yetkililer ve tüketicilerin bilgi istekleri için bir veri ambarı işlevi görmek;
4. Genel bir farkındalık oluşturmak.

Kurumsal bir diğer örnek olarak Vodafone'nun da mahremiyet etki değerlendirme konusunda bir takım nedenleri bulunmaktadır. Bunlar (Wright, 2012):

1. Hesap verilebilirliğin bir unsuru olarak, MED işleminin uygun yapıldığını göstermek;
2. Uygulama sonrası inceleme için bir temel sağlamak;
3. MED uygulama sürecine dahil olmayan bir kişi veya ekip tarafından üstlenilen objektif ve tarafsız bir değerlendirme olan denetim için bir temel sağlamak;
4. Proje sırasında kazanılan bilginin gelecek MED ekipleri ve kurum dışından diğer kişilerle paylaşılabilir olmasına olanak veren "kurumsal hafıza" sağlamak.

Görüldüğü üzere pek çok farklı faydası sıralanan MED'i uygulanabilir kılan nedenler de kurumdan kuruma farklılık arz etmektedir.

3.7 MED'İN AŞAMALARI

Yukarıda genel olarak faydaları, amacı, tarihsel gelişimi, ilkeleri anlatılan MED'in uygulanmasında farklı aşamaların olduğu görülmektedir. Bu durum ülkeden ülkeye, proje ya da MED uygulanacak olan plan, program, yeni bir uygulamanın ölçeğine ve etkisene göre farklılık arz etmektedir (Spiekermann ve Oetzel, 2012). Buna rağmen genel olarak bir MED sürecinin aşağıda kısaca açıklanan aşamalardan oluştuğu ifade edilebilir (Information Commissioner's Office, 2012).

3.7.1 MED İhtiyacının Ortaya Konması

MED sürecinin ilk ve başlangıcı uygulanacak proje, program, plan, politika ya da reform gibi yeni uygulamada MED'e ihtiyaç olduğunun ve gerekliliğinin ortaya konmasıdır. Bu ihtiyaç Kurumun olağan proje yönetimi tarafından ortaya konabileceği gibi veri koruma uzmanları tarafından da gerçekleştirilebilmektedir. Bu süreçte özellikle yeni uygulamanın niçin düşünüldüğünün ve hangi amaçları gerçekleştirmek için planlandığı sorularının cevap bulması gerekir. MED'in bu aşamasında en önemli rolü üst yönetim üstlenmektedir. Mahremiyet uzmanlarından ya da proje yöneticilerinden gelecek bildirimleri değerlendirip karar verecek olan üst yöneticiler böylelikle MED sürecini başlatmış olacaklardır (Office of The Information Commissioner, 2015).

3.7.2 Bilgi Akış Şemasının Oluşturulması

MED'in en önemli aşamalarından biri olan bilgi akış şemasının tam olarak oluşturulup ortaya konması mahremiyet risklerinin net bir şekilde belirlenmesine yardımcı olacaktır. Aksi durumda mahremiyet riskleri açık bir şekilde belirlenemediği için risk yönetiminde de başarısızlıklar kaçınılmaz olacaktır. Dolayısıyla bilgi akış şemasının oluşturulması bu kapsamda hangi kişisel bilgilerin kimlerden, ne zaman, nasıl ve kim tarafından toplanacağının yanı sıra bu bilgilerin nerede, ne kadar bir süre için, kim tarafından ve nasıl depolanacağı belirtilmeli. Ayrıca bu verileri kimlerin işleyeceği, bu verilere kimler tarafından erişileceği, transferlerinin nasıl sağlanacağı ve ne zaman, kimler tarafından, nasıl yok edileceğinin net bir şekilde bu aşamada ortaya konması gerekmektedir (The Office of the Australian Information Commissioner, 2014).

3.7.3 Mahremiyet ve İlgili Riskleri Tanımlanması

MED'in diğer bir önemli aşaması mahremiyet ve ilgili risklerin tanımlanması aşamasıdır. Kurumlar MED oluştururken hem kendi kurumsal yapı ve oluşumunu hem de vatandaşları tehdit edebilecek mahremiyet ve ilgili riskleri net bir şekilde tanımlamalıdır. Örneğin bireyler için yanlış veri ya da güvenlik ihlali olması, kurumlar için ise itibarın zedelenmesi, finansal maliyetler ya da veri güvenliğinin kırılması gibi hususlar göz önünde bulundurularak riskler tanımlanmalıdır. Bu

tanımlama sürecinde kurumlar risk yönetim metodolojilerini kullanabilecekleri gibi mevcut proje yönetimi kapsamında da yönetim imkânlarından faydalanabilirler (Information Commissioner's Office, 2012).

MED sürecinin en önemli aşamalarından olan bu aşamada hem doğrudan hem de dolaylı olarak kişisel mahremiyeti, projenin yasal uyumluluğunu, kurumsal işleyişi ve saygınlığı tehdit edebilecek unsurlar masaya yatırılır. Proje, program ya da planın insan hakları, sektörel etik kuralları ve diğer iletişim mevzuatlarına uygunluğunu engelleyecek riskler ortaya konmalı. Bu noktada mahremiyet ve ilgili risklerin tanımlanmasının sübjektif yani kişiden kişiye değişebildiği unutulmamalı. Dolayısıyla farklı kesimden iç ve dış paydaşlarla bir araya gelinerek onların da görüş ve önerilerinin dikkate alınması süreci daha sağlıklı kılacaktır. Dolayısıyla hem bu aşamada hem de bir sonraki aşamada iç ve dış paydaşlarla ortak akıl platformlarının organize edilmesi kaçınılmaz görünmektedir. Bu platformlarda sadece risklerin tanımlanması yeterli görülmemeli aynı zamanda bu risklerin şiddet ve seviyelerinin de ortaya konması alınacak önlemler açısından büyük ehemmiyet arz etmektedir. Çünkü çoğu projede belirli düzeylerdeki risklerin varlığını kabul etmek gerekir ve bunların mahremiyet konusunda da etkileri görülebilir (Wright ve Wadhwa, 2012:7).

3.7.4 Mahremiyet Çözümlerinin Tanımlanması ve Değerlendirilmesi

Belirlenen risklerin tanımlanasından sonra bu risklerin ortadan kaldırılması, azaltılması ya da başka bir alana transferinin gerçekleştirilmesi MED sürecinin önemli bir parçasını oluşturmaktadır. Bu aşamada özellikle yukarıda değinilen iç ve dış paydaş ortak akıl platformlarını etkili kullanmak gerekmektedir. Bu etkili kullanım sayesinde mevcut kaynaklar, öngörülen proje, program ya da planın muhtemel maliyeti net bir şekilde ortaya konabileceği gibi henüz başlangıç aşamasında olan çalışma için sağlıklı bir Güçlü Yanlar-Zayıf Yanlar-Fırsatlar-Tehditler (GZFT) analiz çalışması yapılabilecektir (Garfinkel vd., 2005:37).

3.7.5 MED Çıktılarını Kayıt Altına Almak ve Sonlandırmak

Bir önceki aşamada gerçekleştirilen ortak akıl platformlarında belirlenen riskler ve bu risklerin kabul edilebilir olup olmadıkları, sorunlar ve çözüm önerileri bu aşamada kayıt altına alınarak rapora dökülür. MED sonucunda hazırlanan bu rapor

sürecin en önemli çıktılarından biri olarak kabul edilir. Bu rapor aynı zamanda şeffaflık ilkesine verilen önemin en somut göstergesi olduğu gibi vatandaşların bilgilendirilmesi hususunun da en önemli mihenk taşıdır (Wright vd., 2011).

MED raporu, süreci ve mahremiyete ilişkin riskleri azaltmak için atılan adımların neler olduğunu özetlemelidir. Rapor ayrıca belirlenen riskleri azaltmak ya da varlığını kabul etmek için ne tür kararların alındığını içermelidir. Bu noktada raporun basılması ve ulaşılabilir bir yerde yayımlanması idarenin almış olduğu bir karar neticesinde gerçekleşmesi idarenin sürece vermiş olduğu önemin yansıtılması açısından önem arz etmektedir. Esasında geniş kapsamlı, önemli ve maliyeti yüksek proje, program, plan ya da yeni düzenlemelerin tamamında MED süreci bütün olarak idare tarafından alınan kararlar çerçevesinde resmi olarak yapılması MED'in etkinliğini artıracaktır (Stoneburner vd., 2002). Bu aşamada hazırlanacak rapor için üzerinde fikir birliği sağlanmış örnek bir şablon bulunmamakla birlikte genel olarak giriş, projenin tanımlanması, veri akışı ve mahremiyet ilişkisi, ortak akıl platform çıktıları, risk değerlendirmesi, yasal uygunluk, sonuç ve öneriler ile gerekmesi durumunda kaynakça kısımlarının mevcut olması arzulanmaktadır (Hert vd., 2012).

3.7.6 MED Çıktılarının Entegre Edilmesi

Bu aşamada MED sonucunda ulaşılan çıktı ve eylemler proje, plan, program ya da düzenlemeye entegre edilmelidir. Özellikle büyük Projelerin uygulaması boyunca çeşitli aşamalarda MED'e dönüş yapmak gerekli olabilir. MED süresince yapılan değerlendirmeler sonrasında devam eden projede öngörülen değişikliklerin yapılması diğer bir ifade ile MED sonuçlarının projeye yansıtılması gereklidir. Çünkü MED çıktılarının proje, plan, program ya da yeni düzenlemeye entegre edilmesi sürecin etkililiği ortaya koymaktadır. Aksi durumda MED süreci sadece formaliteden yapılmış bir değerlendirme olarak kalacaktır ki bu durumda da hem kişilerin, hem kurumların hem de toplumun güveni kaybolacaktır (Information Commissioner's Office, 2012).

3.7.7 Gözden Geçirme ve Denetimin Gerçekleştirilmesi

MED sürecinin son aşaması gözden geçirme ve denetim aşamasıdır. Bu aşamada daha önceki aşamada yapılanlar gözden geçirilir. Özellikle önerilerin projeye

uygulanıp uygulanmadığı hususu, süreç esnasında belirlenen risklerin kabul edilebilir bir seviyeye indirgenip indirgenmediği hususu bu aşamada dikkate alınır. Bu çalışma sonucunda bir "gözden geçirme raporu" düzenlenmesi beklenir. Ayrıca daha öncede ifade edildiği gibi MED bir süreç olup bu sürecin en uzun aşaması ise bu son aşamadır. Çünkü proje devam ettiği sürece MED gözden geçirilecek ve gerekli görülmesi durumunda yenilenecektir. Özellikle proje, plan, program ya da düzenlemede önemli değişikliklerin varlığı MED'in yenilenmesini zorunlu kılacaktır. Ayrıca denetim olarak hem iç denetimin hem de bağımsız dış denetimin yapılması MED'i daha etkin ve güvenilir kılacaktır (Hert vd., 2012).

3.8 FARKLI ÖLÇEKLERDE MED UGULAMALARI

Kurum ve kuruluşlar başvuracakları yeni uygulamanın, proje ve programın içerik, kapsam ve büyüklüğüne göre farklı derinlikte ve farklı ölçeklerde MED uygulaması yapabilmektedir. Özellikle toplumun geniş kesimini ilgilendiren, bünyesinde kapsamlı kişisel verileri barındıran, maliyeti oldukça yüksek proje, program ya da yeni uygulamalarda derinlemesine yapılacak MED sayesinde emek ve harcamaların boşa gitmesinin önüne geçilecektir. Benzer şekilde küçük ölçekli projelerde ise daha yüzeysel bir MED yapılarak bu sürecin hem zaman hem de finansal açıdan tasarruf sağlanmış olacaktır. Bu çerçevede genel olarak dört farklı derinlik ya da ölçekte MED uygulamasının varlığından bahsedilebilir. Bunlar sırasıyla tam ölçekli MED, Yarım Ölçekli MED, Mahremiyet Yasalarına Uygunluğun Kontrolü ve Veri Koruma Kanununa Uyguluğun Kontrolüdür. Aşağıda kışça açıklanacak olan bu farklı MED uygulamalarının aktif bir şekilde başvurulduğu görülmektedir (Falconer, 2012:4).

3.8.1 Tam Ölçekli MED

Özellikle büyük ve kapsamlı projelerde başvurulan tam ölçekli MED'de amaç mahremiyet risk alanlarının net bir şekilde belirlenmesi ve dış paydaşların aktif katılımlarının sağlanarak gereksiz harcama ve mali israfın önüne geçmektir. Uzun dönemleri kapsayan projelerde tam ölçekli MED'in kurum ve kuruluşlara büyük kolaylıklar sağlayarak projenin sağlıklı bir şekilde devam edip sonlanmasında yardımcı olduğu ifade edilebilir (Oetzel vd., 2011). Modern yönetim anlayışı çerçevesinde karar verici merciler açısından hangi proje, program ya da

uygulamalarda tam ölçekli MED'e başvurulacağının belirlenmesi hususunda karşılaşılan sorunu çözmek amacıyla bazı sorular oluşturulmuştur. Eğer proje, program veya uygulama aşağıdaki durumların tamamını bünyesinde barındırıyor ise o zaman tam ölçekli MED uygulanması gerekmektedir (Information Commissioner's Office, 2012).

Bu noktada sorulması gerekli olan sorular kısaca:

1. Proje, daha önce anonim olan, bilinmeyen işlemleri tanımlanabilir, bilinebilir hale getiriyor mu?
2. Proje, tanımlayıcılara izinsiz kimlik tespiti ya da kimlik doğrulama imkanı veren yönetim sürecini içeriyor mu?
3. Proje, mahremiyet saldırıları için önemli bir potansiyel içeren yeni veya ileri teknoloji kullanımı içeriyor mu?
4. Proje, karşılaştırılabilir veri korumaya tabi olmayan üçüncü kişilere herhangi bir ifşayı içeriyor mu?
5. Proje, bireyler üzerindeki veri hacimlerini artırıyor mu?
6. Proje, hassas veriler için yeni bir veri işleme süreci içeriyor mu?
7. Proje, mevcut mevzuat haricinde veri işlemeyi içeriyor mu?
8. Proje, bireylerin artan oranda katılımını içeriyor mu?
9. Proje, çok taraflı kurumsal kullanımı gerekli kılıyor mu?
10. Proje, yeni ya da artan veri eşleştirmeyi içeriyor mu?

Eğer yukarıda yer alan sorulara "evet" cevabı veriliyorsa bu durumda tam ölçekli MED yapmak daha yararlı olacaktır.

3.8.2 Yarı-Ölçekli MED

Tam ölçekli MED için sorulan soruları içermeyen proje, program ya da uygulama için yarı-ölçekli MED uygulaması veya diğer uygulamalar yapılabilir. Özellikle zaman ve kaynak açısından büyük yatırım yapılmasının gerekli olmadığı durumlarda başvurulan yarı- ölçekli MED uygulamalarında risk alanları tam ölçeklideki kadar net ve ayrıntılı bir şekilde ortaya konamamaktadır. Yarı-ölçekli MED ile daha ziyade mahremiyet alanındaki büyük risk tespit edilebilmektedir. Diğer yandan karar alma mekanizması tam ölçekli MED'e göre daha hızlı çalışmaktadır (Oetzel vd., 2011).

Yarı-ölçekli MED uygulamasının yapılmasına karar vermeden önce aşağıdaki soruların cevabının bilinmesi önem arz etmektedir. Bu noktada sorulması gerekli olan sorular kısaca (Information Commissioner's Office, 2012):

1. Proje, belirsiz ya da tatmin edici olmayan veri kalitesi güvence süreç ve standartlarını içeriyor mu?
2. Proje, öncesine nazaran veriye daha rahat ulaşılmasını sağlayan ifşa araçlarını beraberinde getiriyor mu?
3. Proje, belirsiz ya da tatmin edici olmayan veri güvenlik düzenlemelerini içeriyor mu?
4. Proje, belirsiz ya da maliyetli veri muhafaza düzenlemelerini içeriyor mu?
5. Proje, belirsiz ya da fazla müsamahakâr veri erişim veya ifşa düzenlemelerini içeriyor mu?

Eğer yukarıda yer alan sorulara "evet" cevabı veriliyorsa bu durumda yarı-ölçekli MED yapmak daha yararlı olacaktır. Yarı-ölçekli MED hem süre, hem de işleyiş açısından daha etkin olmakla birlikte yukarıda da belirtildiği üzeri mahremiyet risklerinin derinlemesine tespit edilmesi açısından tam ölçekli MED'e göre daha zayıftır.

3.8.3 Mahremiyet Yasalarına Uygunluğun Kontrolü

Yarı- ölçekli ve tam ölçekli MED uygulamasında yer alan soruları içermeyen proje, program ya da uygulamaların temelde var olan ulusal ya da uluslararası mahremiyet yasalarına uygunluğunun dikkate alındığı bu MED uygulamasında özellikle hukuki alanda açılması muhtemel mahremiyet ihlali davaların önüne geçilmiş olacaktır. Bilhassa elektronik iletişim, e-ticaret gibi mahremiyet hususunu doğrudan düzenleyen yasalara uygunluğun kontrolü bu aşamada önem arz etmekte olup bu uygunluk kontrolünün mali yükü yarı-ölçekli ve tam ölçekli MED ile kıyaslanmayacak kadar küçüktür (Falconer, 2012:7).

3.8.4 Veri Koruma Kanununa Uyguluğun Kontrolü

Projenin en önemli unsurlarından biri bireyler üzerinde güven tesisinin oluşturulmasıdır. Bu güvenin sağlanması için en temel husus proje, program ya da uygulamanın mahremiyet açısından veri koruma kanununa uygunluğunun kontrol

edilmesidir. Mahremiyet yasalarına uygunluğun kontrolünde olduğu gibi veri koruma kanununa uygunluğun kontrolünde de proje sürecinin, sonuçlarının ve proje gerekliliklerinin proje sahibi kurumlar tarafından ele alınması ilgili kanunlarla uyumluluğunun ortaya konması oldukça büyük öneme sahiptir (Information Commissioner's Office, 2012).

3.9 GELECEKTEKİ MED UYGULAMALARI

ABD, Yeni Zelenda, Kanada ve AB ülkeleri gibi pek çok gelişmiş ve gelişmekte olan ülkelerde uygulanan MED'in önümüzdeki yıllarda yaşayacağı değişim ve ilerlemeler hususunda çeşitli öngörüler ortaya konmaktadır. Bu öngörülerden ilki Otomatik Karar Destekleme Sistemlerinin (OKDS) MED uygulamalarında kullanılmasının kaçınılmaz olduğudur. Bu çerçevede Mahremiyet Uzmanlık Sistemi gibi çeşitli sistemlerin geliştirilerek MED uygulamalarında doğru kararların zamanında alınması sağlanmış olacağı öne sürülmektedir. Özellikle karar alma, izleme ve raporlama gibi süreçlerin Otomatik Karar Alma Sistemi yardımıyla etkin bir şekilde uygulanmasıyla daha başarılı MED çalışmalarının gerçekleşmesinin kaçınılmaz olduğu öngörülmektedir (Tancock, vd., 2010).

İkincisi ise gelecekteki yıllarda hali hazırda yerel ya da ulusal yetki sınırları içerisinde uygulanmakta olan MED'in sınır ötesi diğer bir ifade ile uluslararası bir boyuta taşınacağıdır. Özellikle sınırların neredeyse kaybolduğu ve dünyanın küresel bir köy haline geldiği günümüzde idari yetki alanları noktasında karışıklıklar çıkabilmektedir. Örneğin İngiltere'den Avustralya'ya sefer düzenleyen Fransa gemisinde yolculuk yapmak isteyen bir Amerikalı vatandaşın Almanya seyahat firmasından kredi kartıyla bilet alması durumunda kişisel verilerin elde edilmesi, işlenmesi ve korunması hususlarında ülkelerin yetki alanlarının net olmadığı görülmektedir (Homeland Securtiy, 2014).

Sonuç olarak yerel ve ulusal sınırlar içerisinde uygulanan MED'in yetersiz olduğu sınır ötesi iş ve işlemlerde mahremiyetin yeterli bir şekilde tanımlanması ve gözden geçirilmesi gerekmekte olup kişilerin güvenle iş ve işlemlerini yürütebilmesi için uluslararası bir MED uygulamasının oluşturulup yaygınlaştırılması

gerekmektedir. Bu bağlamda farklı ülkelerden mahremiyet uzmanlarının olduğu bir mahremiyet değerlendirme ekibinin oluşturulması ve üçüncü ülkelerden bağımsız uzmanlar tarafından dış denetim ve kontrolünün yapılacağı bir uluslararası MED uygulamasının kaçınılmaz olduğu ileri sürülmektedir (Karol, 2001:5). Dolayısıyla yakın gelecekte MED uygulamalarında öngörülen değişikliklerden önemli olarak görülen iki tanesi yukarıda ele alınmıştır.

SONUÇ VE ÖNERİLER

Bilişim ve teknolojideki ilerlemelere paralel olarak toplumlarda güvenlik algısı da değişmektedir. Yeni güvenlik algısının oluşmasında özellikle 11 Eylül saldırıları, WikiLeaks Olayı ve modern kamu yönetim anlayışındaki değişikliklerin başat rol oynadığı söylenebilir. Değişen bu güvenlik anlayışı çerçevesinde üzerinde en çok tartışılan ve önem verilen konuların başında bilgi güvenliği ve kişisel verilerin korunması hususlarının geldiği ifade edilebilir. Özellikle son zamanlarda yaşanan teknolojik iyileşme, e-uygulamaların yaygınlaşması, dijital teknolojideki ilerlemelerle birlikte artık bilgi kolayca toplanabilmekte, işlenebilmekte, depolanabilmekte ve ağlar aracılığı ile bir yerden bir yere rahatlıkla iletilebilmektedir. Bu durum bir taraftan veri ve bilgi hırsızlarının iştahını artırırken diğer taraftan hem kişileri, hem devletleri hem de ulusal ve uluslararası kurum ile kuruluşları bilgi güvenliğinin sağlanması ve kişisel verilerin korunmasında gerekli tedbirleri almaya sevk etmektedir.

Diğer taraftan, içinde bulunduğumuz bilgi çağında küresel ağların yeryüzünde yer alan bilgi sistemlerinin birbirleri ile olan iletişim ve etkileşimini aktif hale getirmesiyle birlikte küresel bir köy olarak adlandırılan yenidünya düzeninde kişisel ya da kurumsal bilgilere kolayca erişilebilmektedir. Bu durumun doğal bir sonucu olarak küresel medeniyetin bilgi toplumundan mahremiyet toplumuna doğru ilerlediği ifade edilmektedir. Dolayısıyla hem kişisel mahremiyete, hem kurumsal mahremiyete hem de toplumsal mahremiyete hiç olmadığı kadar büyük önem atfedilmektedir. Bütün bu gelişmeler dikkate alındığında kişisel verilerin korunarak, bilgi güvenliğinin tesis edildiği ve mahremiyetin garanti altına alındığı güven toplumunun inşası için ortaya konan gayret ve çalışmalar yüksek bir değer taşımaktadır.

Modern yönetim anlayışı çerçevesinde yukarıda bahsedilen kişisel verilerin korunması ve bilgi güvenliğinin sağlanarak mahremiyetin güven altına alınması amacıyla başvurulan MED, Yeni Zelanda, ABD, Hong Kong, İngiltere, İrlanda ve AB ülkeleri başta olmak üzere pek çok devletin çalıştırdığı bir süreç uygulaması olarak karşımıza çıkmaktadır. Proje, program ya da yeni bir uygulamanın kişisel verilerin korunması, mahremiyet ve bilgi güvenliği açısından etki değerlendirmesine

tabi tutulup risk alanlarının önceden belirlendiği MED uygulamasının sosyal, ekonomik ve politik pek çok faydası bulunmaktadır. Hesap verilebilirlik, şeffaflık ve vatandaş odaklılık gibi temel değerler etrafında gerçekleştirilen MED uygulaması ile birlikte sağlık, ticaret, ekonomi ve finans alanında meydana gelen maddi ve manevi kayıpların önlenebileceği ortaya konmuştur. Özellikle son zamanlarda meydana gelen siber saldırılar ile bu saldırılar sonucu oluşan milyar dolarlık kayıpların önlenmesinde de etkili olan MED'in bir taraftan birçok ülkede zorunlu olması tartışılırken diğer taraftan uluslararası MED standartlarının oluşturulması hususunda görüş ve öneriler ortaya konulmaktadır.

Uluslararası arenada bu gelişmeler yaşanırken 108 sayılı Avrupa Konseyi Sözleşmesi imzalamış fakat henüz onaylamamış olan Türkiye'de hali hazırda bir "Kişisel Verilerin Korunması Kanunu'nun" olmayışı büyük eksiklik olarak görülmektedir. En kısa sürede çıkması arzulanan mezkûr kanunu müteakiben MED uygulamalarının her yönüyle ele alınması aciliyet arz etmektedir. Mevcut durum dikkate alındığında yasalaşacak kanundan sonra pek çok proje, program ve uygulama sonucunda ortaya çıkmış olan mahremiyet ihlali, kişisel verilerin korunamaması gibi hususlardan açılacak tazminat davaları ve yaptırımlarının önüne geçmek için MED uygulamaları kurumlar tarafından gündeme alınıp uygulanmalıdır.

Kişisel Verilerin Korunması Kanunu Tasarısı'nda bu kanunla verilen görevleri yapmak üzere, kamu tüzel kişiliğini haiz, idari ve mali özerkliğe sahip Kişisel Verileri Koruma Kurumu kurulması öngörülmektedir. Bu noktada mezkûr Kurumun teşkilatlanmasında dikkate alınması gerekli olan bazı öneriler şu şekilde ifade edilebilir:

1. Kurumda, Mahremiyet Üst Kurulu oluşturulmalıdır. Bu Kurul genel müdür ve üzeri seviyedeki beş veya yedi kişiden oluşturulmalı ve oy çokluğu ile karar vermelidir.
2. İkinci olarak bu üst kurulun altında görev yapacak ve doğrudan kurum başkan yardımcılarına bağlı olan komisyonlar oluşturulmalıdır. Bu komisyonlarda bir defaya mahsus olmak üzere farklı bakanlıklarda görev yapan ve mesleki yarışma sınavı ile göreve başlamış olan kariyer uzmanları "mahremiyet uzmanı" unvanı ile görevlendirmelidir. İlerleyen

dönemlerde buradaki mahremiyet uzmanları tarafından yetiştirilmek üzere yabancı dil bilgisi yüksek olan mahremiyet uzman yardımcıları Kuruma alınarak göreve başlatılmalıdır. Mahremiyet uzmanları MED alanındaki uluslararası gelişmeleri takip etmek, ülkedeki MED uygulamalarını incelemek, kurumlara ve yöneticilere gerekli bilgileri vererek arzulanan rehberlik çalışmalarını yürütmek, MED uygulamalarında objektif denetimi gerçekleştirmek gibi görev ve yetkilerle donatılmalıdır.

Bu kurumsal yapılanmanın yanı sıra Başbakanlık tarafından, MED konusunda kamu kurum ve kuruluşlarını bağlayıcı bir genelge yayımlanmalıdır. Ayrıca buna paralel olarak bütün kamu kurum ve kuruluşlarında Strateji Geliştirme Başkanlıklarının altında daire başkanlığı ya da şube müdürlüğü şeklinde örgütlenmiş "Mahremiyet Etki Değerlendirme Birimleri" oluşturulmalıdır. Bu birimler bağlı bulundukları kurum ve kuruluş tarafından gerçekleştirilecek proje, program ve uygulamalara ait MED çalışmalarını yapmalıdır. Yapılan bu MED çalışması Kişisel Verileri Koruma Kurumu'ndaki ilgili komisyona gönderilmelidir. Daha önceden belirlenen kriterler çerçevesinde komisyon gerekli inceleme ve rehberlik faaliyetlerini yapmalıdır. Komisyon kararlarına itiraz Üst Kurula yapılmalıdır.

Oluşturulması önerilerin bu komisyonlar tarafından verilen kararın objektif olması yönünde gerekli çalışmalar yapılmalıdır. Örneğin komisyon üyelerinin tarafsızlığı için komisyon üyesinin naklen atama ile geldiği bakanlık tarafından gerçekleştirilen MED'lerin değerlendirilmesinde bu üyenin değerlendirmeyi yapan komisyonda görev almaması sağlanabilir. Ayrıca tarafsızlık yeminine başvurulması da bir seçenek olarak düşünülebilir. Komisyon değerlendirmelerine yapılacak itiraz belli bir süre aşımına tabi tutulmalıdır. Üst kurulun kararları yargı denetimine tabi olmalıdır.

Bu süreçte üst kurul ve komisyonlar koordinasyon ile işe başlamalı ve ilk etapta gerekli broşür ve görsel ile yazılı materyaller hazırlamalıdır. Ayrıca başta üst düzey yöneticiler olmak üzere kamu kurum ve kuruluşlarında kurulacak mahremiyet etki değerlendirme birimlerinde görevlendirilen personele gerekli mesleki eğitimler verilmelidir. Genel olarak ise tüm kamu personeline yönelik farklı zaman

dilimlerinde e-öğrenme ya da video ortamında gerekli farkındalık eğitim hizmeti sunulmalıdır. Ayrıca kamu kurum ve kuruluşlarına MED uygulamalarının aşamaları, işleyişi, etkinliği gibi hususlarda yol gösterecek bir "MED Kılavuzu" hazırlanarak yayımlanmalıdır.

Yukarıda sayılan yapının oluşturulması ve bu birimlerin yürütmekle sorumlu tutulacağı faaliyetler zaman ve maliyet açısından kamu kurum ve kuruluşlarına yüklenen bir külfet olarak algılansa da genel süreç ele alındığında ve gerekli fayda-maliyet analizleri yapıldığında bu düzenlemelerin önemi ortaya çıkacaktır. Diğer bir ifade ile, proje uygulamasından önce MED yapılması zaman kaybına ve bürokrasiye neden olacağı öne sürülse de proje uygulamasından önce risk alanlarının tespit edilmesi, paydaşlarla fikir alışverişinde bulunulması, kişisel/kurumsal mahremiyetin sağlanması gibi hususlar vatandaş memnuniyetini artıracak, projelerin sorunsuz şekilde tamamlanmasına yardımcı olacak, siber saldırılar ve veri hırsızlığına karşı koruma sağlanacaktır. Ayrıca mahremiyet ihlalleri önlenerek özellikle yargıya taşınan maddi ve manevi tazminat davaları sonucunda oluşan finansal ve yargı yükü hafifletilmiş olacaktır. Bütün bunlar birlikte düşünüldüğünde MED'in artı yanlarının eksi yanlarına göre çok daha ağır bastığı görülmektedir.

Yukarıda sayılan hususlar dikkate alındığında, sigorta ve sağlık verilerinin yer aldığı SGK, şirketlere ait önemli verilerin tutulduğu Kamu İhale Kurumu, özel ve tüzel kişilere ait mali ve vergi kayıtlarının korunduğu Gelir İdaresi Başkanlığı başta olmak üzere bazı kurumların hâlihazırda kullandıkları önemli programlara ait risk alanlarının tespiti ve gerekli önlemlerin alınması için MED yapılmasına öncelik verilmelidir. Zamanla bu uygulama diğer kurum ve kuruluşların kullandıkları programlara da uygulanarak genişletilmelidir.

Sonuç olarak, önümüzdeki süreç dikkate alındığında Türkiye'de kişisel verilerin korunması ve bilgi güvenliğinin sağlanması alanında MED uygulamalarının sosyal, ekonomik ve finansal açıdan birçok faydası görülecektir. Bu noktada üzerinde durulması gerekli olan en önemli husus; bu çalışmada da belirtildiği üzere standart bir MED uygulamasının olmadığı, ülkeden ülkeye farklılık arz eden MED'lerin bulunduğudur. Dolayısıyla Türkiye'de de oluşturulacak MED ülkeye özgü, ülke değerlerini, toplumsal dinamikleri ve kültürel hassasiyetleri dikkate alan

bir süreç olarak tasarlanmalıdır. Bu kapsamda, kurum ve kuruluşlar arası bilgi ve veri paylaşımı için gerekli alt yapı güçlendirmelerinin yapılması Türkiye'de MED uygulamalarının yapılabilmesi için gereklidir. Bunlardan daha önemlisi toplumda bilgi güvenliği, kişisel verilerin korunması ve mahremiyet konularında gerekli farkındalığın oluşturulması gerekmektedir. Bunun yanı sıra kurum ve kuruluşlarda özellikle üst düzey yöneticilerin MED hakkında bilgilendirilmesi, bu çerçevede gerekli broşür ve yazılı ve görsel materyallerin hazırlanması gerekmektedir. Böylelikle siber saldırılar karşısında gerekli önlemler alınış, uygulamalardaki risk alanları net bir şekilde ortaya konmuş, yargı yükü azaltılmış ve en önemlisi güven toplumu oluşturulmasına katkı sağlanmış olunacaktır.

KAYNAKÇA

Acar, Gökhan, (2008), "Enformasyon Sistemlerinin Stratejik Önemi ve Planlanması", *Yönetim Bilimleri Dergisi,* 6(1), ss.53-76.

Acquisti, Allesandro and College, Heinz, (2010), "The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines", *OECD Conferences*, 1 December, 2010, Paris: OECD Conference center, pp.3-18.

African Union, (2012), *African Union Convention on CyberSecurity and Personal Data Protection,* Addis Ababa, http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20Cyber Security%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pd f (E.T: 25 Ekim 2014).

Akay, Hale, (2009), *Türkiye'de Güvenlik Sektörü: Sorular, Sorunlar, Çözümler*, İstanbul: Türkiye Ekonomik ve Sosyal Etüdler Vakfı (TESEV) Yayınları.

Altman, Irwin, (1975), *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding,* First Printing Edition, Monterey-California: Brooks/Cole Pub. Co.

Anderson, Alicia, (2006), "Effective Management of Information Security and Privacy", *Educause Quarterly*, 1(1), pp.15-20.

Atak, Songül, (2010), "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", *TBB Dergisi*, 1(87), ss.90-120.

Awad, Ali Ismail; Hassanien, Aboul Ella and Baba, Kensuke, (2013), *Advances in Security of Information and Communication Networks First International Conference, SecNet 2013,* Cairo.

Baker, Wade and Wallace Linda, (2007), "Is Information Security Under Control?", *IEEE Security and Privacy*,5(1), pp.36-44.

Barutçugil, İsmet, (2002), *Bilgi Yönetimi,* 1. Baskı, İstanbul: Kariyer Yayıncılık.

Beales, Howard, (2011), "The Value of Behavioral Targeting", *Network Advertising Initiative,* http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (E.T: 14 Mart 2015).

Belgian Presidency of the Council of the European Union, (2010), *Strengthening Social Mainstreaming in the EU, Round up of discussions on social impact assessment during the Belgian Presidency of the Council of the European Union*, Brussels.

Belsis, Petros; Kokolakis, Spyros and Kiountouzis, Evagoles, (2005). "Information Systems Security From A Knowledge Management Perspective", Information Management and Computer Security, 13(3), pp.189-202.

Bennett, Colin; Bayley, Robin; Charlesworth, Andrew and Clarke, Roger, (2007), "Privacy Impact Assessments: International Study of Their Application and Effects", Information Commissioner's Office United Kingdom, London.

Beranek, Bolt and Inc, Newman, (1981), "A Hıstory of The Arpanet" DARPA Report, Virginia.

Cate, Fred; Cullen, Peter and Mayer, Viktor, (2014), *Data Protection Principles for the 21st Century*, Oxford: Oxford Internet Institute,

Cavoukian, Ann, (2005), "Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*", Information and Privacy Commissioner*, pp.1-37. https://www.ipc.on.ca/images/Resources/phipa_pia-e.pdf (E.T: 26 Ocak 2015).

Civelek, Dilek Yüksel, (2011), *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*, Yayınlanmış Uzmanlık Tezi, Ankara: Başbakanlık Devlet Planlama Müsteşarlığı Bilgi Toplumu Dairesi Başkanlığı, Yayın No:2821.

Clark, Ray, and Canter, Larry, (1997). *Environmental Policy and NEPA: Past, Present and Future*, Florida: St. Lucie Press.

Clarke, Roger, (1998), *Privacy Impact Assessments*, First Edition, pp.14, Canberra: Xamax Consultancy Pty Ltd.

Clarke, Roger, (2004), *A History of Privacy Impact Assessments*, First Edition, pp.21, Canberra: Xamax Consultancy Pty Ltd.

Clarke, Roger, (2006), "What's 'Privacy'?", 7 August 2006, pp.2, http://www.rogerclarke.com/DV/Privacy.html (E.T: 18 Mart 2015).

Clarke, Roger, (2009), "Privacy Impact Assessment: Its Origins and Development, C*omputer Law and Security Review,* 25(2), pp.123–135.

Cohen, Jennifer. (2013), "A Critical Overview of the Privacy Debates Regarding Facebook and an Assessment of the "Anti-Facebook" Social Network, Diaspora", *A Research report*, Johannesburg.

Considerati, (2013), *Privacy Impact Assessment: Preventing Privacy Risks by Responsible Design*, Amsterdam, http://www.considerati.com/wp-content/uploads/2013/09/Considerati-Factsheet-Privacy-Impact-Assessment-English.pdf (E.T: 18 Nisan 2015).

Coopersmith, Jonathan, (2009), "The History of Information Security: A Comprehensive Handbook", *Journal of Technology and Culture*, 50(1), pp.262-268.

Council of Europe, (2010), *Data Protection*, Strasbourg. http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf (E.T: 10 Ekim 2014).

Council of Europe, (2014), *European Union Agency for Fundamental Rights*, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf (E.T: 5 Aralık 2014).

Council of The European Union, (2004), *A Comparative Analysis Of Regulatory Impact Assessment In Ten EU Countries*, Dublin.

Cranor, Lorrie, (2005), *Security and Usability: Designing Secure Systems that People Can Use*, Second Edition, Sebastopol: O'Reilly.

Çamsarı, Ulaş Mehmet, (2012), "Dijital Nesil (Z Kuşağı) nedir? – Buruk Kalplerin Z Hikayeleri", *Genç Haber Dergisi,* 1(1), ss.26-28.

Davenport, Thomas ve Laurence Prusak, (2001), *İş Dünyasında Bilgi Yönetimi: Kuruluşlar Ellerindeki Bilgiyi Nasıl Yönetirler*, Günhan Günay (çev.), İstanbul: Rota Yayınları.

David, Flaherty, (2000), "Privacy Impact Assessment: An Essential Tool For Data Protection", Privacy Law and Policy Report, Venice.

DeCew, Judith Wagner, (2012), "Privacy", *The Stanford Encyclopedia of Philosophy* Spring 2015 Edition.

Demirkıran, Özlem; Eser, Hamza B. ve Keklik, Belma, (2011), "Demokrasinin Tabana Yayılması, Yönetimde Şeffaflık ve Hesap Verebilirlik Bağlamında Bilgi Edinme Hakkı Kanunu", *Akdeniz Üniversitesi Uluslararası Alanya İşletme Fakültesi Dergisi,* 3(2), ss.169-192.

Denning, Dorothy, (1998), *Information Warfare and Security*, First Edition, Boston: Addison-Wesley.

Devlet Planlama Teşkilatı, (2001), *Avrupa Birliği Temel Haklar Şartı,* Ankara: Avrupa Birliği ile İlişkiler Genel Müdürlüğü, http://www.eskisehirab.gov.tr/userfiles/files/AVRUPA%20B%C4%B0RL%C4%B0%C4%9E%C4%B0%20TEMEL%20HAKLAR%20%C5%9EARTI.pdf (E.T: 25 Ekim 2014).

Devost, Matthew, (2000), "Current and Emerging Threats to Information Technology Systems and Critical Infrastructures", *The Global Business Briefing journal,* pp.20-23.

Doğantimur, Fulya, (2009), *ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği*, Yayınlanmamış Mesleki Yeterlik Tezi, Ankara: T.C. Maliye Bakanlığı-Strateji Geliştirme Başkanlığı.

Dourish, Paul and Anderson, Ken, (2006), "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena", *Human Computer Interactions*, 21(3), pp.319-342.

Duji, Slobodan, (1996), "The Directive of the European Union on the Protection of Individual Regarding the Processing of Personal Data", *Public service*, 32(1), pp.51-74.

Enyew, Alebachew, (2009), *Regulatory Legal Regime on the Protection of Privacy and Personal Information in Ethiopia*, Master's Thesis, Oslo: University Of Oslo, Faculty of Law.

European Commission, (1998), *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, Brussels.

European Commission, (2010), *Opinion 3/2010 on the Principle of Accountability*, Brussels.

European Parliamentary Technology Assessment (EPTA), (2009), *What is a Technology Assessment ?* Washington.

Evans, David; Peck, Simon; Swanepoel, Lynette and Doyle, Ted, (2014), "The Financial Cost of Healthcare Fraud 2014", BDO Reports, Northern Islands.

Falconer, Maureen, (2012), "Recognising Privacy Risk", *ScotStat Data Linkage Conference*, 26 March 2012, Edinburgh, pp.1-12.

Fenster, Mark, (2012), "Disclosure's Effects: WikiLeaks and Transparency", *Iowa Law Review*, 97(3), pp.753-807.

Fey, Michael; Kenyon, Brian; Reardon, Kevin; Rogers, Bradon and Ross, Charles, (2012), *Security Battleground: An Executive Field Manual*, Hillsboro: Intel Press.

Fibikova, Lenka and Mueller, Roland, (2012), "Threats, Risks and the Derived Information Security Strategy", *Securing Electronic Business Processes*, pp.11-20.

Garfinkel, Simson; Juels, Ari and Pappu, Ravi, (2005), "RFID Privacy: An Overview of Problems and Proposed Solutions", *IEEE Security and Privacy*, 3(3), pp. 34-43.

Gelbstein, Eduardo and Kamal, Ahmad, (2002), *Information Insecurity*, Second Edition, New York: the UN ICT Task Force and UNITAR.

Glancy, Dorothy, (1979), "The Invention of the Right To Privacy, *"Arizona Law Review"*, 21(1), pp.1-39.

Gözler, Kemal, (2007), *Devletin Genel Teorisi*, 1. Baskı, Bursa: Ekin Yayınevi.

Greenleaf, Graham, (2008), "Accession to Council of Europe privacy Convention 108 by non-European states", *Privacy Laws and Business International*, 94(1), pp. 1-3.

Güler, Seval ve Ergül, Coşkun, (2014), "Kişisel verilerin korunması tasarısı TBMM'ye sunuldu", *Anadolu Ajansı*, 26 Aralık 2014.

Güven, Sibel, (2011), "Türkiye'de Düzenleyici Etki Analizi (DEA) Uygulamaları Neden İstenen Düzeyde Değil?", *Akıllı Yönetim: Düzenleyici Etki Analizi Konferansı*, Ankara: Türkiye Ekonomi Politikaları Araştırma Vakfı, ss.1-34.

Güzel, Ahmet, (2011), "Bilişim Güvenliği ve Sayıştay Denetimi Açısından Önemi", *Dış Denetim Dergisi,*1(5), ss.157- 168.

Hennessy, Christopher, (2009), "Security Design, Liquidity, and the Informational Role of Prices", London, http://faculty.london.edu/chennessy/assets/documents/DRAFT18.pdf (E.T: 15 Aralık 2014).

Hermalin, Benjamin and Katz, Michael, (2006), *The Economics of Product-Line Restrictions With an Application to the Network Neutrality Debate*, First Edition, Californnia: UC Berkeley Publishing.

Herold, Rebecca, (2002), "What Is The Difference Between Security and Privacy?", *CSI*, pp.1-3.

Hert, Paul and Gutwirth, Serge, (2003), "Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence", *European Parliament Committee Report,* Seville.

Hert, Paul; Kloza, Dariusz and Wright, David, (2012), "Recommendations for a privacy impact assessment framework for the European Union", *European Commission Report,* Brussels.

Hong, Kwo-Shing; Chi, Yen-Ping; Chao, Louis and Tang, Jungsun, (2006), "An Empirical Study Of İnformation Security Policy On Information Security Elevation in Taiwan", *Journal of Information Management and Computer Security*, 14(2), pp.104-115.

Hong, Kwo-Shing; Chi, Yen-Ping; Chao, Louis and Tang, Jih-Hsing, (2003), "An Integrated System Theory of Information Security Management", *Information Management and Computer Security*, 11(5), pp.243-248.

Hustinx, Peter, (2013), " EU Data Protection Law - Current State and Future Perspectives", *High Level Conference: Ethical Dimensions of Data Protection and Privacy*, 9 January 2013, Tallinn, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-01-09_Speech_Tallinn_EN.pdf (E.T: 18 Ekim 2014).

International Business Machines (IBM), (2008), *Cost, Complexity and Risk: Security for the Enterprise of the Future*, http://www.935.ibm.com/services/us/cio/pdf/5877_security_and_compliance_us_white_paper_final_nov_4-08.pdf (E.T: 9 Kasım 2014).

Information Commissioner's Office (ICO), (2014), *Conducting Privacy Impact Assessments Code of Practice,* Cheshire, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (E.T: 18 Mart 2015).

Information Commissioner's Office (ICO), (2014), *Privacy impact assessment handbook*, Cheshire, https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf (E.T: 16 Nisan 2015).

Information Commissioners Office (ICO), (2009), *Privacy Impact Assessment Handbook*, Cheshire, http://www.ico.gov.uk/handbook (E.T: 21 Mart 2015).

Information Security Policy Council, (2012), *Information Security 2012*, http://www.nisc.go.jp/eng/pdf/is2012_eng.pdf (E.T: 4 Eylül 2014).

International Association for Impact Assessment (IAIA), (1999), *Principles of Environmental Impact Assessment Best Practice*, Fargo.

International Labour Office, (1997), *Protection of Workers' Personal Data,* Geneva, http://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_107797.pdf (E.T: 25 Ekim 2014).

ISO 27001, (2005), *Information Security Management System* Geneva, https://www.tuv-nord.com/cps/rde/xbcr/SID-52E1B301-7AEA007E/tng_in/Product_Information_27001.pdf (E.T: 10 Şubat 2015)

ISO/IEC 17799, (2005), *Information Technology — Security Techniques — Code of Practice for Information Security Management, International Standard,* Geneva.

ISO/IEC TR 18044, (2004), *Information Technology – Security Techniques – Information Security Incident Management,* Geneva. https://webstore.iec.ch/p-preview/info_isoiec18044%7Bed1.0%7Den.pdf (E.T: 10 Eylül 2014).

Israel, David and Perryy, John, (1990), "What is Information?", *In Information, Language and Cognition,* University of British Columbia Press, pp. 1-19.

Kaberia, Ken, Business Continuity and Risk Management, pp.1-26. http://www.garp.org/media/883552/kenya_022212.pdf (E.T: 10 Şubat 2015)

Kalseth, Karl and Sarah Cummings, (2001), *"*Knowledge Management: Development Strategy or Business Strategy?*", Information Development*, 17(3), pp.163-172.

Karol, Thomas, (2001), "Cross-Border Privacy Impact Assessments: An Introduction*", Information Systems Control Journal*, 3(1), pp.1-9.

Kavza, Uğur, (2010), *Veri Madenciliğinde Mahremiyetin Sağlanması*, Yayınlanmamış Yüksek Lisans Tezi, Gebze: Gebze Yüksek Teknoloji Enstitüsü / Mühendislik ve Fen Bilimleri Enstitüsü.

Kayem, Anne and Meinel, Christoph, (2013), *Theories and Intricacies of Information Security Problems*, Potsdam: Publikationsserver der Universität Potsdam.

Kelter, Harald; Bartels, Cord and Hansen, Wolf-Ruediger, (2010), "Technical Guidelines RFID as Templates for the PIAFramework", Report of Federal Office for Information Security (BSI), Bonn. https://www.bsi.bund.de/cae/servlet/contentblob/1130780/publicationFile/90287/TG_RFID_Templates_for_PIA_Framework_pdf.pdf (E.T: 14 Nisan 2015).

Kılınç, Doğan, (2012), "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 61(3), ss.1089-1169.

Kim, Jungsun, (2009), *A comprehensive structural model of factors influencing customers' intention to use biometrics in the hospitality industry*, phd dissertation, Las Vegas: University of Nevada.

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

Laurie, Graeme, (2002), *Law and Ethics of Genetic Privacy*, First Edition, New York: Cambridge University Press.

Lavanya, Nayeneni; Rani, Sandhya and Rao, Raja Prakash, (2012), "A Comparative Study on Privacy by Search Engines while Publishing Search Logs", *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(8), pp.268-270.

Loewenstein, Antony, (2015), " WikiLeaks: not perfect, but more important than ever for free speech", *The Guardian*, 12 January 2015, http://www.tup.tsinghua.edu.cn/Resource/tsyz/006870-01.DOC (E.T:9 Nisan 2015).

Lomas, Elizabeth, (2010), "Information Governance: Information Security And Access Within a UK Context", *Records Management Journal*, 20(2), pp. 182-198.

Luthans, Fred and Stewart, Todd, (1977), "A General Contingency Theory of Management", *Academy of Management Review*,2(2), pp.181-195.

Mantelero, Alessandro, (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), pp.1-6.

Mark, Stamp, (2005*), Information Security: Principles and Practice*, Second Edition, New Jersey: John Wiley and Sons, Inc. Publication.

Marttin, Vedat ve Pehlivan, İhsan, (2010), "ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kurulusu Uygulamaları Üzerine Bir İnceleme", *Mühendislik Bilimleri ve Tasarım Dergisi,* 1(1), ss.49-56.

Max, Theodore, (2011), "Charting A Safe Course In The Perfect Storm Of Consumer Privacy Laws", *The Metropolitan Corporate Counsel,* 19(6), pp.1-2.

Meinrath, Sascha, (2011), "The Future of the Internet: Balkanization and Borders", *Time*, 11 October 2013, http://ideas.time.com/2013/10/11/the-future-of-the-internet-balkanization-and-borders/ (E.T: 25 Şubat 2015).

Mekuriaw, Asnake and Teffera, Belay, (2013), "The role of Environmental Impact Assessment for sustainable development", http://www.iaia.org/conferences/iaia13/proceedings/Final%20papers%20review%20process%2013/The%20role%20of%20Environmental%20Impact%20Assessment%20for%20sustainable%20development%20%20.pdf?AspxAutoDetectCookieSupport=1 (E.T: 15 Ocak 2015).

Metin, Yüksel, (2002), "Avrupa Birliği Temel Haklar Şartı", *Ankara Üniversitesi Siyasal Bilgiler Dergisi*, 57(4), ss.35-63.

Miniwatts Marketing Group, (2014), *Internet Usage and World Population Statistics are preliminary for Dec 31, 2014*, Bogota, http://www.internetworldstats.com/stats.htm (E.T: 11 Eylül 2014).

Murray, Patrick, (1997), "The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet the Standard?", *Fordham International Law Journal*, 21(3), pp.932-1018.

Mutlu, Levent, (2011), *Anayasal Bir Hak Olarak Çevre Hakkı ve Çevresel Etki Değerlendirmesi*, Yayınlanmamış Yüksek Lisans Tezi, Kars: Kafkas Üniversitesi, Sosyal Bilimler Enstitüsü.

Narayanan, Arvind; Barocas, Solon; Toubiana, Vincent; Boneh, Dan and Nissenbaum, Helen, (2012), "A Critical Look at Decentralized Personal Data Architectures", http://randomwalker.info/publications/critical-look-at-decentralization-v1.pdf (E.T: 11 Mart 2015).

Nissenbaum, Helen, (2009), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, First Edition, California: Stanford University Press.

Nugent, Carlsson, (2009), "Review of Environmental Impact Assessment and Monitoring in Aquaculture in Africa", *Reviews And Synthesis*, 527, pp.59-151.

Oetzel, Marie Caroline; Spiekermann, Sarah; Grüning, Ingrid; Kelter, Harald and Mull, Sabine, (2011), *Privacy Impact Assessment Guideline*, Bonn: Bundesamt für Sicherheit in der Informationstechnik,

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile (E.T: 11 Nisan 2015).

Office of the Australian Information Commissioner (OAIC), (2014), *Guide To Undertaking Privacy Impact Assessments*, http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/guide-to-undertaking-pias.pdf (E.T: 18 Nisan 2015).

Office of The Information Commissioner (OIC), (2015), *Overview of the Privacy Impact Assessment (PIA) process*, Quennsland, https://www.oic.qld.gov.au/__data/assets/pdf_file/0009/26568/overview-of-the-pia-process.pdf (E.T: 18 Nisan 2015).

Official Journal of the European Communities, *(2000),* Charter of Fundamental Rights of The European Union (2000/C 364/01), pp.1-21.

Organisation for Economic Co-Operation and Development (OECD), (2013), *The OECD Privacy Framework,* Paris, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (E.T: 5 Aralık 2014).

Organisation for Economic Co-Operation and Development (OECD), (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Paris, http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (E.T: 11 Nisan 2015).

Önel, Dinçer ve Dinçkan, Ali, (2007), *Bilgi Güvenliği Yönetim Sistemi Kurulumu*, Kocaeli: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Yayını.

Palen, Leysia and Dourish, Paul, (2003), "Unpacking "Privacy" for a Networked World", 5–10 April, 2003, Florida, https://www.cs.colorado.edu/~palen/Papers/palen-dourish.pdf (E.T: 06 Mart 2015).

Peltier, Thomas, (2005), "Implementing an Information Security Awareness Program", *Securıty Management Practıces,* 14(2), pp.37-49.

Perrin, Chad, (2008), "10 common security mistakes that should never be made", *Techrepublic*, August 20, 2008, http://www.techrepublic.com/blog/10-

things/10-common-security-mistakes-that-should-never-be-made/ (E.T: 23 Şubat 2015).

Ponemon Institute, (2012), *2012 Cost of Cyber Crime Study: United States*, Traverse City.

Puhakainen, Petri, (2006), *A Design Theory For Information Security Awareness*, First Edition, Oulu: Oulu University Press.

Radaelli, Claudio and De Francesco, Fabrizio, (2007), "Regulatory Impact Assessment, Political Control and the Regulatory State", *The 4th General Conference Of The European Consortium For Political Research,* 6-8 September, 2007, Pisa.

Reid, Randall and Floyd, Stephen, (2001), "Extending The Risk Analysis Model to Include Market Insurance*", Journal Of The Computer And Security*, 20(4), pp.331-339.

Roagna, Ivana, (2012), *Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması*, Ayşe Gül Alkış Schäling (çev.), Strazburg: Avrupa Konseyi Yayınları.

Rotmans, Jan, (2006), "Tools for Integrated Sustainability Assessment: A two-track approach", *The Integrated Assessment Journal Bridging Sciencesand Policy,* 6(4), pp.35-57.

Sadowsky, George; Dempsey, James; Greenberg, Alan; Mack, Barbara and Schwartz, Alan, (2003), *Information Technology Security Handbook,* Washington: World Bank Press.

Sağıroğlu, Şeref; Ersoy, Eren ve Alkan, Mustafa, (2007), "Bilgi güvenliğinin kurumsal bazda uygulanması", *Bildiriler Kitabı Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı*, 2007.

Salihpaşaoğlu, Yaşar, (2013), "Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme", *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, XVII(3), ss.227-266.

SAS, (2013), *Five Big Data Challenges and How to Overcome Them with Visual Analytics*, Cary, North Carolina, http://www.sas.com/resources/asset/five-big-data-challenges-article.pdf (E.T: 25 Şubat 2015).

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

Sezgin, Aslı Şat, (2013), "Dünya'da ve Türkiye'de e-Ticaret Sektörü", *İktisadi Araştırmalar Raporu,* Ankara, http://ekonomi.isbank.com.tr (E.T: 11 Eylül 2014)

SGK, (2015), *Sağlık Hizmeti Sunucularına Duyuru (Biyometrik Kimlik Doğrulama Sistemi)*, 30 Nisan 2015, Ankara, http://www.sgk.gov.tr/wps/portal/tr/e_sgk/diger_uygulamalar/duyurular (E.T: 18 Mayıs 2015).

Shaffer, Paul, (2013), "Q-Squared in Impact Assessment: A Review", Peterborough Ontario, http://trentu.ca/ids/documents/Q2_WP61_Shaffer.pdf (E.T: 9 Mart 2015).

Shroff, Marie, (2007), "Privacy Impact Assessment Handbook", *Report of the Privacy Commissioner Office*, pp.17-23, Auckland.

Siponen, Mikko and Iivari, Juhani, (2006), "Six Design Theories for IS Security Policies and Guidelines", *Journal of the Association for Information Systems*, 7(7), pp. 445-472.

Solms, Basie von, and Solms, Rossouw von, (2004), "The 10 Deadly Sins of Information Security Management", *Computers and Security*, 23(5), pp.371-376.

Solove, Daniel, (2005), "A Taxonomy of Privacy" , *University of Pennsylvania Law Review*, 154(3), pp.477-560.

Solove, Daniel, (2002), "Conceptualizing Privacy", *California Law Review*, 90(4), pp.88-102.

Spiekermann, Sarah and Oetzel, Marie Caroline, (2012), "Privacy-By-Design Through Systematic Privacy Impact Assessment – A Design Science Approach", *European Conference of Information Systems*, June 2012, Barcelona.

Spiekermann, Sarah and Cranor, Lorrie Faith, (2009), "Engineering Privacy", *IEEE Transactions On Software Engineering*, 35(1), pp.67-82.

Stallings, William, (2011), *Cryptography and Network Security Principles and Practice,* Fifth Edition, New York: Prentice Hall Publishing

Stewart, Blair, (1996), "PIAs; an Early Warning System", *Privacy Law and Policy Report,* Christchurch, http://www.austlii.edu.au/au/journals/PLPR/1996/65.html (E.T: 4 Mart 2015).

Stewart, Blair, (1999), "Privacy Impact Assessment: Towards a Better Informed Process for Evaluating Privacy Issues Arising From New Technologies", *Privacy Law and Policy Report,* Christchurch, http://www5.austlii.edu.au/au/journals/PrivLawPRpr/1999/8.html (E.T: 11 Mart 2015).

Stoneburner, Gary; Goguen, Alice and Feringa, Alexis, (2002), "Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology*", National Institute of Standards and Technology Report,* Falls Church, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (E.T: 5 Mayıs 2015).

Streatfield, David and Markless, Sharon, (2009), "What is impact assessment and why is it important?", *Journal of Performance Measurement and Metrics,* 10(2), pp.134-141.

Susanto, Heru and ibni Muhaya, Fahad, (2010), "Multimedia Information Security Architecture Framework", *2010 5th International Conference on Future Information Technology (FutureTech),* 21-23 May 2010, Busan, pp.1-6.

Susanto, Heru; Almunawar, Mohammad Nabil; Tuan, Yong Chee and Aksoy, Mehmet Sabih, (2012), "I-SolFramework: An Integrated Solution Framework Six Layers Assessment on Multimedia Information Security Architecture Policy Compliance", *International Journal of Electrical and Computer Sciences,* 12(1), pp.20-28.

Tahaoğlu, Osman Okyar and Cebi, Yalçın, (2007), "Personal Data Protection in Turkey: Technical and Managerial Controls", Atilla Elçi, S. Berna Ors, Bart Preneel (Ed), *Security of Information and Networks,* İzmir: Trafford Publishing, pp.220-226.

Tancock, David; Pearson, Siani and Charlesworth, Andrew, (2010), "The Emergence of Privacy Impact Assessments", *Report of European Commission,* Brussel.

Tataroğlu, Muhiddin, (2013), "Mahremiyet Sorunlarının Önlenmesinde Mahremiyet Etki Değerlendirmesi (MED)", *Yönetim ve Ekonomi*, 20(1), ss.263-289.

Tekerek, Mehmet, (2008), "Bilgi Güvenliği Yönetimi", *KSÜ Fen ve Mühendislik Dergisi*, 11(1), ss.130-133.

The European Parliament and The Council of The European Union, (1995), *Directive 95/46/Ec of the European Parliament and of the Council of 24 October 1995 on The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Luxembourg: No L 281 /31.

The Information Commissioner's Office (ICO), (2013), *PIA Handbook*, https://ico.org.uk/media/for-organisations/documents/1042837/trilateral-report-executive-summary.pdf (E.T: 18 Mart 2015).

The Office of the Australian Information Commissioner (OAIC), (2012*), Guide to Information Security: 'Reasonable Steps' to Protect Personal Information*, Sydney.

The Privacy Office of United States Department of Homeland Security, (2007), *Privacy Impact Assessments, The Privacy Office Official Guidance* Washington.

Thomson, Kerry Lynn; Von Solms, Rossouw and Lynette, Louw, (2006), "Cultivating an organizational information security culture", *Journal of Computer Fraud and Security*, 10(1), pp.7-11.

Tudor, Junior Kindergarte, (2001), "Information Security Architecture: An Integrated Approach to Security in Orgaznization", *Security Policies, Standarts and Procedures*, New York, pp.79-100.

Türk Borçlar Kanunu, (2011), T.C. Resmi Gazete, 27836, 4 Şubat 2011.

Türk Ceza Kanunu, (2004), T.C. Resmi Gazete, 25611, 12 Ekim 2004.

Türk Medeni Kanunu, (2001), T.C. Resmi Gazete, 24607, 8 Aralık 2001.

Türk Ticaret Kanunu, (2011), T.C. Resmi Gazete, 27846, 14 Şubat 2011.

Türkiye Cumhuriyeti Anayasası, (1982), 17863 Mükerrer, 9 Kasım 1982.

Türkiye Ekonomi Politikaları Araştırma Vakfı (TEPAV), (2007), *Düzenleyici Etki Analizi Rehberi,* Ankara.

U.S. Department of Homeland Security, (2014), *Privacy Impact Assessment for the Border Surveillance Systems (BSS)*, Boston.

UNINETT, (2010), *Information Security Policy Best Practice Document*, http://sigarra.up.pt/up/pt/web_gessi_docs.download_file?p_name=F96095589/no-uninett-terena-information-security-policy-best-practice-document-gn3-na3-t4-ufs126.pdf (E.T. 9 Eylül 2014).

United Nations Environment Programme (UNEP), (2002), *Environmental Impact Assessment Training Resource Manual*, Second Edition, Geneva http://www.unep.ch/etb/publication/EIAman/IntroManual.pdf (E.T: 11 Mart 2015).

Ünsal, Çağrı Zeybek, (2013), "Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu ve Avrupa Birliği'nin 95/46/Ec Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi", *Hacettepe Hukuk Fakültesi Dergisi*, 3(1), ss.99-124.

Van, Lieshout; Marc, Michael Friedewald; Gutwirth Serge and David Wright, (2012), "Reconciling privacy and security", *Innovation: the European Journal of Social Science Research*, 26(1-2), pp.119-132.

Warren, Samuel and Brandeis, Louis, 1890, "The Right to Privacy", *Harvard Law Review*, 4(5), pp.193–220.

Weber, Ron, (1999), *Information System Control and Audit*, Upper Saddle River, NJ:Prencite Hall.

Whitman, Michael, (2003), "Enemy At The Gate: Threats To Information Securıty", *Communıcations Of The Acm,* 46(8), pp.91-95.

Wright, David and De Hert, Paul, (2012), "Findings and Recommendations in Privacy Impact Assessment*", Law, Governance and Technology,* pp.445 – 481.

Wright, David and Wadhwa, Kush, (2012), "A step-by-step guide to privacy impact assessment", *Trilateral Research and Consulting*, pp.1-9, http://www.piafproject.eu/ref/A_step-by-step_guide.pdf (E.T: 11 Eylül 2014).

Wright, David, (2012), "The State Of The Art In Privacy Impact Assessment", *Computer Law and Security Review*, 28(1), pp.54-61.

Wright, David; Gellert, Raphaël; Gutwirth, Serge and Friedewald, Michael, (2011), "Minimizing Technology Risks With PIAs, Precaution And Participation", *IEEE Technology and Society*, 30(4), pp.47-54.

Wright, David; Wadhwa, Kush; De Hert, Paul and Kloza, Dariusz, (2011), "Privacy Impact Assessment Framework for Data Protection and Privacy Rights", *European Commission Report*, Brussels, http://www.piafproject.eu/ref/PIAF_D1_21_Sept_2011.pdf (E.T: 11 Aralık 2014).

Xu, Heng; Dinev, Tamara; Smith, Jeff and Hart Paul, (2011), "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurance", *Journal of the Association for Information Systems*, 12(12), pp.798-824.

Yılmaz, Malik, (2009), "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi", *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi,* 49(1), ss.95-118.

Yılmaz, Sefer, (2011), *Türkiye'deki İç Güvenlik Yapılanmasında Değişim İhtiyacı ve Güvenlik Yöneticilerinin Değişime Yönelik Tutum ve Davranışları Üzerine Bir Araştırma*, Yayınlanmamış Doktora Tezi, Adana: Çukurova Üniversitesi Sosyal Bilimler Enstitüsü.

Young, William and Leveson, Nancy, (2014), "An Integrated Approach to Safety and Security Based on Systems Theory", *Communications Of The Acm*", 57(2), pp.31-35.

Yurtsever, Hatice ve Buran, Burçin, (2012), "Bilgi Edinme Hakkı Kanunu Çerçevesinde Vergi Mahremiyetinin Değerlendirilmesi", *Electronic Journal of Vocational Colleges*, 2(2), ss.46-56.

Yüksel, Mehmet, (2003), "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi" , *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi,* 58(1), s. 181-215.

Yüksel, Mehmet, (2009), "Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar" , *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, 64 (1), ss. 275-298.

Zabunoğlu, Yahya Kazım, (1973), *Kamu Hukukuna Giriş- Devlet (Tanım- Kaynak- Unsurlar)*, Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayınları (No:328).

Zhou, Zhi-Hua; Chawla, Nitesh; Jin, Yaochu and Williams, Graham, (2014), "Big Data Opportunities and Challenges: Discussions from Data Analytics Perspectives", *IEEE Computational Intelligence Magazine*,9(4), pp.62-74.

Zins, Chaim, (2007), "Conceptual Approaches for Defining Data, Information, and Knowledge", *Journal Of The American Society For Information Science And Technology*, 58(4), pp. 526–535.

Žižek, Slavoj, (2014), "How Wikileaks Opened Our Eyes To The Illusion of Freedom", *The Guardian*, 19 Haziran 2014, http://www.theguardian.com/commentisfree/2014/jun/19/hypocrisy-freedom-julian-assange-wikileaks (E.T: 11 Kasım 2014).

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı	: ErkanAĞIRALAN
Doğum Yeri	: Kangal
Mesleği	: Sosyal Güvenlik Uzmanı

Eğitim Durumu

Lisans Öğrenimi	: Siyaset Bilimi ve Uluslararası İlişkiler
Yüksek Lisans Öğrenimi	: -
Bildiği Yabancı Diller	: İngilizce
Yabancı Dil Puan ve Türü	: 80, YDS
Bilimsel Faaliyetler	: -

İş Deneyimi

Stajlar	: -
Projeler	: -
Çalıştığı Kurumlar	: Maliye Bakanlığı (Vergi Müfettişi)
	Sosyal Güvenlik Kurumu (Uzman)

İletişim

E-Posta	: erkan.agiralan@gmail.com
Tel.	: 0312 207 83 72
Tarih	: 27.08.2015