DİJİTALLEŞME SÜRECİNDE KİŞİSEL BİLGİLERİN GÜVENLİĞİ VE KORUNMASI

Chapter · September 2021

CITATION
1

READS
36

2 authors:

Mustafa Kocaoğlu
Necmettin Erbakan University
33 PUBLICATIONS **99** CITATIONS
SEE PROFILE

Sinem Şahnagil
Balıkesir University
46 PUBLICATIONS **92** CITATIONS
SEE PROFILE

EĞİTİM yayınevi

EDİTÖRLER
Doç. Dr. Mustafa KOCAOĞLU
Doç. Dr. Sefa USTA

KURUMSAL BİLGİ YÖNETİMİ

Teknolojik Eğilimler

KURUMSAL BİLGİ YÖNETİMİ
Teknolojik Eğilimler

EDİTÖRLER

Doç. Dr. Mustafa KOCAOĞLU

Doç. Dr. Sefa USTA

EĞİTİM
yayınevi

KURUMSAL BİLGİ YÖNETİMİ Teknolojik Eğilimler

Doç. Dr. Mustafa KOCAOĞLU / Doç. Dr. Sefa USTA

Genel Yayın Yönetmeni: Yusuf Ziya Aydoğan (yza@egitimyayinevi.com)
Genel Yayın Koordinatörü: Yusuf Yavuz (yusufyavuz@egitimyayinevi.com)
Sayfa Tasarımı: Eğitim Yayınevi Grafik Birimi
Kapak Tasarımı: Eğitim Yayınevi Grafik Birimi

T.C. Kültür ve Turizm Bakanlığı
Yayıncı Sertifika No: 47830

ISBN: 978-625-7405-82-9
1. Baskı, Eylül 2021

Baskı Cilt
Bulut Dijital Matbaa Sanayi Ticaret Limited Şirketi
Musalla Bağları Mah. İnciköy Sok. 1/A Selçuklu / KONYA
Matbaa Sertifika No: 48120

Kütüphane Kimlik Kartı
KURUMSAL BİLGİ YÖNETİMİ Teknolojik Eğilimler
Doç. Dr. Mustafa KOCAOĞLU / Doç. Dr. Sefa USTA
165x240 mm
Kaynakça var, dizin yok.
ISBN: 978-625-7405-82-9

EĞİTİM
yayınevi
Yayınevi Türkiye Ofis: İstanbul: Eğitim Yayınevi Tic. Ltd. Şti., Atakent mah. Yasemen sok. No: 4/B, Ümraniye, İstanbul, Türkiye

Konya: Eğitim Yayınevi Tic. Ltd. Şti., Şükran mah. Rampalı No: 107, Meram, Konya, Türkiye
+90 332 351 92 85, +90 533 151 50 42
bilgi@egitimyayinevi.com

Yayınevi Amerika Ofis: New York: Egitim Publishing Group, Inc.
P.O. Box 768/Armonk, New York, 10504-0768, United States of America
americaoffice@egitimyayinevi.com

Lojistik ve Sevkiyat Merkezi: Kitapmatik Lojistik ve Sevkiyat Merkezi, Fevzi Çakmak Mah. 10721 Sok. B Blok, No: 16/B, Safakent, Karatay, Konya, Türkiye
sevkiyat@egitimyayinevi.com

Kitabevi Şubesi: Eğitim Kitabevi, Şükran mah. Rampalı 121, Meram, Konya, Türkiye
+90 332 499 90 00
bilgi@egitimkitabevi.com

İnternet Satış: www.kitapmatik.com.tr
+90 537 512 43 00
bilgi@kitapmatik.com.tr

kitapmatik
internetteki kitapçınız
kitapmatik.com.tr

ÖN SÖZ

İnsanoğlu tarih boyunca bir takım toplumsal aşamalardan geçerek bugüne gelmiştir. Tüm bu aşamalar, esasen onun ihtiyaçları ve hep daha ileriye gitmeye yönelik güdüsü sayesinde şekillenmiştir. İlkel (avcı-toplayıcı) toplumdan, tarım toplumuna; tarım toplumundan sanayi toplumuna ve sanayi toplumundan bilgi toplumuna geçişte hem söz konusu güdünün izleri hem de bu güdüye bağlı olarak ortaya çıkan ve dönüm noktası olarak ifade edilebilecek bir takım somut gelişmeler belirleyici olmuştur.

Halen içerisinde bulunduğumuz ve çok yönlü etkilerini yoğun biçimde hissettiğimiz bilgi toplumu aşaması ise küreselleşme olgusu ve teknolojinin baş döndürücü bir hızda gelişmesi ile birlikte günümüzdeki halini almıştır. Özellikle teknolojik gelişmelerin insan hayatının her aşamasını doğrudan etkisi altına almaya başladığı yadsınamaz bir gerçek olarak kabul edilmektedir. Bununla birlikte söz konusu gelişmeler, kurumların yapılarını ve işleyiş biçimlerini de aynı yönde ve yoğunlukta etkilemektedir. Artık gerek özel sektörde gerekse kamu sektöründe, içerisinde teknolojik gelişmelerin yer almadığı bir sürecin anlam ve öneminin olmadığı genel kabul gören bir düşünce haline gelmiştir.

Akademik bir çerçevede konuya bakıldığında ise söz konusu gelişmelerin, sosyal bilimlerde ve özellikle de yönetim alanında önemi her geçen gün artmaktadır. Çok farklı alt disiplinlerin teknolojik gelişmeler ve daha özelde dijitalleşmeyi odak noktasına aldığı ve araştırmaların bu eksende gerçekleşmeye başladığı görülmektedir. Bu noktada, bilgi toplumunun kurumlardaki temel referans noktası olan bilgi ve teknoloji üzerine yönetsel çalışmaların, disiplinler üstü ve/veya disiplinler arası bir bakış açısıyla gerçekleştirilmesi büyük bir önem taşımaktadır.

Tüm bu gerekçeler ile gerçekleştirilen bu çalışma ile kurumsal bilgi yönetimi ve teknolojik eğilimler üzerine kuramsal ve kavramsal çerçeveyi net bir biçimde ortaya koyabilmek; konu ile ilgili ulusal ve uluslararası düzeydeki gelişmeleri, ilgili aktörler üzerinden somut bir biçimde ele almak; bilgiye dayalı olarak ortaya çıkan yeni teknolojilerin yönetsel boyut ve etkilerini irdelemek ve uygulama alanlarına yönelik güncel tartışmaları değerlendirmeye tabi tutmak amaçlanmıştır.

Kurumsal Bilgi Yönetimi ve Teknolojik Eğilimler başlığını taşıyan bu çalışmadaki bazı bölümler salt kuramsal/kavramsal bir çerçeve sunarken bazıları ise doğrudan uygulamaya yönelik olarak kurgulanmıştır. Kitapta bu iki ana grupta toplam 25 bölüm bulunmaktadır. Bu bölümler en son teknolojik gelişmelerin yönetim literatürüne ve pratiğine olan yansımalarını ele almaktadır. Bu bağlamda kitapta öncelikli olarak "Kurumsal Bilgi Yönetimi"; "Toplumsal Dönüşüm Sürecinde Yeni Toplum Yapısı: Toplum 5.0"; "Endüstri 4.0 ve Yeni İş Gücü"; "İnovasyon ve Sosyal İnovasyon" bölümlerine yer verilmiştir. Daha sonra, "Yapay Zeka"; "Dijital İkiz"; "Kamuda Büyük Veri"; "Yapay Sinir Ağları ve Derin Öğrenme"; "Veriden Bilgiye Maline Öğrenmesi"; "Kurumsal Zeka Geliştirmenin Bir Yöntemi Olarak Veri Madenciliği"; "Teknoloji Odaklı Üretimde Paradigma Kayması: Karanlık Fabrikalar" bölümleri kavramsal ve kuramsal çerçevede ele alınmıştır. "Sanal Örgütlerin Güvenlik Ekseninde İncelenmesi"; "Siber Zorbalık ve Siber Güvenlik"; "Dijitalleşme Sürecinde Kişisel Bilgilerin Güvenliği ve Korunması" başlıklı bölümlerde dijitalleşme, teknolojik gelişmeler ve güvenlik sorunsalı tartışılmıştır.

"Blokzinciri Teknolojisi"; "Bulut Bilişim Teknolojisinin Stratejik Yönetim Sürecine Etkisi"; "Dijital Liderlik"; Yükseköğetimde Dijital Dönüşüm: Dijital Olgunlu ve Değişim Yönetimi"; "Bir Bilgi Yönetimi Uygulaması Olarak Sosyal Medya ve Dijital Diploması"; "Elektronik Demokrasi"; "Akıllı Yönetişim ve Kamu Politikaları"; "Akıllı Şehirlerde Bilgi İletişim Teknolojiler ve Akıllı Yönetişim"; "Akıllı Yaşam ve Kent Aracı Olarak Yerel Yönetimlerin Güvenli Kent Uygulamaları"; "Belediyelerde Teknoloji Kullanımı ve Mobil Belediyecilik (M-Belediyecilik) Uygulamaları: Büyükşehir Belediyeleri Üzerinden Bir Analiz"; "Turizmde Teknoloji Kullanımı ve Akıllı Turizm Yaklaşımı" başlıklı bölümlerde ise teknolojik gelişmeler uygulama düzeyinde ele alınmıştır.

Yönetim Bilişim Sistemleri, Kamu Yönetimi, Siyaset Bilimi ve Kamu Yönetimi ve İşletme başta olmak üzere sosyal bilimlerin farklı pek çok alanına hitap eden bu çalışmanın, yalnızca konu ile ilgili olarak çalışan akademisyenler veya bu alanlarda öğrenim gören lisans ve lisansüstü öğrencilere değil, aynı zamanda uygulayıcılara da faydalı olmasını diliyor; yaklaşık bir yıldır gösterilen çabanın ve verilen emeğin neticesinde ortaya çıkan bu çalışmaya katkı sağlayan tüm değerli yazarlarımıza ve basım sürecindeki ilgi ve desteklerinden dolayı Yusuf Yavuz Beyefendi nezdinde tüm Eğitim Kitabevi çalışanlarına ayrı ayrı teşekkür ediyoruz.

Editörler

Doç. Dr. Mustafa KOCAOĞLU & Doç. Dr. Sefa USTA

Konya- Karaman, Eylül - 2021

İÇİNDEKİLER

DİJİTALLEŞME SÜRECİNDE KİŞİSEL BİLGİLERİN GÜVENLİĞİ VE KORUNMASI

Mustafa KOCAOĞLU*

Sinem ŞAHNAGİL**

Giriş

Bilgi toplumunu ifade eden günümüz dünyasında, küreselleşme ile paralellik gösteren ve yaygınlaşan bilginin kullanımı siyasi, ekonomik, toplumsal ve kültürel birçok alanı etkisi altına almıştır. Bilgi iletişim teknolojileri kullanımının tüm dünyada artması ve bu teknolojinin gündelik yaşama nüfuz etmesiyle, tarihsel süreçte daima büyük bir güç olarak ortaya çıkan bilgi, bireylerin düşüncesinden yaşayışına, davranışından gelişimine kadar birçok alanda belirleyici unsur haline gelmiştir. Bilgi iletişim teknolojilerindeki hızlı gelişme ile girilen dijital çağ, elektronik ortamlarda bilginin işlenmesini, taşınmasını ve saklanmasını kolaylaştırmış; bilgiye mekândan ve zamandan bağımsız olarak erişilmesini sağlamıştır.

Bilişime dayalı araçların çeşitli ortamlarda yaygın şekilde kullanılmaya başlanması, değerli bir kaynak özelliği taşıyan bilgiye yönelik güvenlik tehditlerinin ve risklerinin aynı oranda artırmasını beraberinde getirmiştir. Bu durum bilginin korunması gerekliliğini daha güçlü şekilde vurgulayarak bilgi güvenliği kavramını ortaya çıkarmıştır. Bu kapsamda çeşitli güvenlik ilkeleri belirlenerek, bilginin güvenliğine yönelik politikalar geliştirilmeye; olası risk ve tehditler sınıflandırılarak yasal düzenlemeler aracılığıyla bilgi, koruma altına alınmaya çalışılmıştır.

Özel sektörde bu yöndeki çalışmaların geçmişi çok daha eski ve yaygın olmakla birlikte son yıllarda kamu sektöründe de bilgi/veri*** güvenliği konusunda

* Doç. Dr., Necmettin Erbakan Üniversitesi, UBF, Yönetim Bilişim Sistemleri Bölümü, mustafakocaoglu@erbakan.edu.tr, ORCID: 0000-0002-9341-6341

** Arş. Gör. Dr., Balıkesir Üniversitesi, İİBF, Siyaset Bilimi ve Kamu Yönetimi Bölümü, s.sahnagil@gmail.com, ORCID: 0000-0003-0920-6948

*** Bu noktada sıklıkla birbirinin yerine kullanılan veri ve bilgi kavramları arasındaki ince farkı ifade etmekte fayda vardır. Bilginin işlenmemiş hali olarak tanımlanabilen "veri" kavramı, sayısal karakterlerden veya

çok yönlü ve yoğun bir çalışma süreci içerisine girildiği anlaşılmaktadır. Bilhassa BM (Birleşmiş Milletler), OECD (İktisadi İşbirliği ve Gelişme Teşkilatı) ve AB (Avrupa Birliği) gibi uluslararası ve hatta küresel çapta faaliyet gösteren kurumların gerek mevzuat gerekse de uygulama düzeyinde aktif bir konuma yükseldikleri görülmektedir. Türkiye'de de Dünya'da genel olarak gerçekleşen bu yöndeki gelişmelere koşut biçimde pek çok çalışmanın yapıldığı ve halihazırda yapılmakta olduğu görülmektedir.

Çalışmanın birinci bölümünde, kavramsal ve kuramsal olarak bilgi ve bilgi güvenliğinden bahsedilecektir. Bu kapsamda, bilgi güvenliğinin temel düzeyde ne anlama geldiği, bilginin güvenliğinin konusu, amacı, kapsamı, unsurları ve temel ilkeleri ele alınarak tarihsel süreçte nasıl bir gelişime konu olduğu anlatılacaktır. İkinci bölümde uluslararası ve ulusal düzeyde bilgi güvenliğine ile ilgili hukuki ve uygulamaya yönelik çalışmalara göz atılacaktır. Son olarak ise bilgi güvenliğine ve bilginin korunmasına ilişkin olarak ortaya çıkan risk ve tehditler ortaya konularak bunların giderilmesi amacına binaen bir takım çözüm önerileri geliştirilecektir.

1. Dijital Çağın Sorun Alanlarından Birisi Olarak Bilginin Güvenliği Ve Korunması

Sanayi devriminin beraberinde getirdiği köklü değişim ve dönüşüm süreci, tarıma dayalı geleneksel toplum yapısından kopuşa neden olmuş; sosyal, kültürel, teknolojik birçok alanda tümüyle farklı bir toplum yapısının inşasını başlatmıştır. Süreç içerisinde dönüşüm hız kesmemiş, küreselleşmenin eşlik ettiği teknolojik devrim, dijital bilgi toplumuna giden kapıları aralamıştır.

Sanayi toplumu sonrasında ortaya çıkan teknoloji kaynaklı toplumsal değişimlerin önemli nedenlerinin başında, toplumsal değişimlerin bilginin konumu üzerine yaptığı vurgu gelmiştir. Bilgisayar aracılığıyla toplumsal hayata giren ve bilgiyi referans alan yeni teknoloji, bilginin bir değer olarak önemli bir kaynak haline gelmesini sağlamıştır. Dijital çağ ile birlikte bilgiyi üreten ve tüketen arasındaki kanallar çeşitlilik kazanmış, bu kanalların da etkisiyle bilgi, üretilen ve tüketilen bir meta haline gelmiştir (Lyotard, 2000). Hatta zaman içerisinde bir adım daha ileriye gidilerek bilgiyi yalnızca üretmek veya tüketmek değil aynı zamanda "türetmek" de mümkün hale gelmiştir. İlk kez 1980 yılında Alvin Toff-

sembollerden oluşmaktadır. Birbiriyle ilişkisi bulunmayan bağımsız ve anlam ifade etmeyen sayısal veya sayısal olmayan setleri ifade eden veriler, ancak çeşitli işlemlere tabi tutulduktan sonra anlam ve değer kazanarak bilgiye dönüşmektedirler. Dolayısıyla bilgi, verinin belli bir anlama gelecek şekilde düzenlenmiş ve tasarlanmış halini meydana getirmektedir (Canbek ve Sağıroğlu, 2006: 166; Ackoff, 1989: 3). Tüm bu açıklamalara dayanarak bu çalışmada genel olarak "bilgi güvenliği" üzerinde durulması, konu kişisel açıdan ele alındığında ise "veri güvenliği" şeklinde ifade edilmesi uygun görülmektedir.

ler'in "Üçüncü Dalga" (The Third Wave) isimli kitabında geçen bilgi türeticisi (prosumer) kavramı, üretici (producer) ile tüketici (consumer) kavramlarının birleşmesinden meydana gelmektedir. Kavram, "bir şirketin ürün tasarım ve üretimine yardımcı olan tüketici" ve "ürünlerin kendi ihtiyaçları doğrultusunda tasarımına ya da kişiselleştirilmesine dahil olan tüketici" şeklinde tanımlanmaktadır. Bilgi toplumu sürecinde özellikle internet teknolojisinin gelişmesi ile birlikte artık bilginin bireyler tarafından yalnızca pasif biçimde tüketilmesi değil aynı zamanda üretimine dahil olunarak türetilmesi de mümkün hale gelmektedir (Uğraş, 2015: 23-24).

Bilginin yayılması ve paylaşılması ile küreselleşen dünyada ortaya çıkan bilgi toplumu, yeni temel teknolojilerin gelişimi ile bilgi sektörünün, üretiminin, sermayesinin, iletişim teknolojilerinin önem kazandığı yeni gelişmeler ile toplumu ekonomik, sosyal, kültürel ve siyasal açıdan sanayi toplumunun ötesine taşıyan bir gelişme aşaması olarak ifade edilmektedir (Selvi, 2012: 198-199). Gelişmiş teknoloji altyapısı ile insan makine etkileşiminin sağlandığı yeni dijital dünyada yaşanan değişim ve gelişmeler, bilginin belirli bir yer ve fiziki ortama bağlı olmaksızın sistematik olarak saklanabilmesini, düzenlenebilmesini ve gerektiğinde yeniden kullanılabilmesini sağlayarak bilginin tüm insanlar ve toplumlar için temel güç ve kaynak olmasını sağlamıştır (Çalık, 2009).

Dolayısıyla bilginin en önemli kaynak haline geldiği bu süreçte, zamanın, mekânın ve insanın sınırlarının belirsizleşmesi, kaynağa yönelik yeni risk ve tehditleri de beraberinde getirmiş; "güvenlik" olgusu, dijital bilgi çağının sorun alanlarından birisi haline gelmiştir. Kişi veya kurum fark etmeksizin sahip olunan bilginin mahremiyetinin ve bütünlüğünün korunması, elektronik ortamlarda paylaşılan bilginin herhangi bir zarara uğramaması, diğer bir deyişle bilginin güvenliğinin sağlanması, dijital çağın en önemli gerekliliklerinden birini oluşturmuştur. Bu kapsamda bilgi güvenliğinin tesisi, "dijital çağ" olarak adlandırılan günümüz dünyasında bilgi sistemlerinin küreselleşmesine bağlı olarak bu sistemlerle doğrudan veya dolaylı ilişki içinde olan toplumlardan bireylere, devletlerden kurum ve kuruluşlara kadar bütün kesimlerin sorumluluğu kapsamına girmiştir.

1.1. Kavramsal Olarak Bilgi Güvenliği

Araştırma, gözlem ve öğrenme yoluyla elde edilen her türlü kavrayış ve gerçekanlamına gelen bilgi, Platon'un deyimiyle doğruluğu ispatlanmış inançları oluşturmanın yanı sıra herhangi bir konuda belirsizliği en aza indirme yeteneğine sahip kaynakları da ifade etmektedir (Argyris, 1993: 3; Nonaka ve Takeuchi, 1995: 58; Platon'dan aktaran Yalçın, 2016: 8). Bireyin yaşamında hemen her alanda yönlendirici ve belirleyici bir özelliğe sahip olan bilgi, iletişim ve iş

birliğini yaygınlaştıran ve kolaylaştıran bilgi teknolojilerinin gelişmesiyle kendi çağını, diğer bir deyişle bilgi çağını başlatmıştır. Dijital teknolojilerin gelişmesiyle birlikte bilgi, gerek bireylerin gerekse toplumların kolaylıkla ulaştıkları fakat elde tutarak koruması ve güvenliğinin sağlanması aynı oranda zorlaşan bir değer haline gelmiştir.

Bilgi güvenliği, bir varlık olarak bilginin her türlü zarardan korunması, doğru teknoloji ile amacına uygun olarak kullanılarak istenmeyen kişiler tarafından elde edilmesine engel olmak şeklinde ifade edilmektedir (Canberk ve Sağıroğlu, 2006: 169). Pfleeger (1997) bilgi güvenliğini, "bilgiye erişimin kesintisiz sağlanması ve bilginin göndericisinden alıcısına kadar gizlilik içerisinde ulaştırılması" olarak tanımlamış; bilginin bozulmadan ve değişikliğe uğramadan bu süreci tamamlanmasının bilgi güvenliğinin temel noktası olduğunu ifade etmiştir. Puhakainen (2006) ise bilgi güvenliğini, birey veya kurum tarafından, kime ait olduğu fark etmeksizin, bilgiye izinsiz veya yetkisiz şekilde erişilmesini, kullanılmasını, değiştirilmesini ve açığa çıkarılmasını önlemek amacıyla hayata geçirilen önlemler dizisi olarak açıklamıştır. Surwade ve Patil'e göre (2019: 460) isebilgi güvenliği, bilgileri yetkisiz erişime ve tahribe karşı korumak amacıyla hayata geçirilen başta teknolojiler olmak üzere standartlardan politikalara ve yönetim uygulamalarına kadar birçok faktörün toplamı anlamına gelmektedir. Bu kapsamda Cherdentseva ve Hilton (2013: 546) bilgi güvenliğini, "bilgiye yönelik tehdit içermeyen çok disiplinli bir çalışma alanı" olarak tanımlamıştır.

1.2. Bilgi Güvenliğinin Amacı, Konusu ve Kapsamı

Bilgi güvenliğinin temel amacı öncelikle kesintisiz, güvenli ve nitelikli bir hizmet sunumunun sağlanmasıdır (Güngör, 2015: 13). Bilgi güvenliği ile ilgili ortaya konulan bütün çabaların bir diğer temel amacı ise kişi ve kurumların bilgi iletişim teknolojilerini kullanırken tehdit ve tehlikeleri fark etmeleri, ihtiyaç duyulan önlemleri kısa zaman içinde alabilmeleridir (Seferoğlu vd., 2018: 32). Dolayısıyla bilgi kaynaklarının her koşulda gizlilik içerisinde, bütünlüğünün ve erişebilirliğinin korunmasını amaçlayan bilgi güvenliği, herhangi bir risk ve tehdit karşısında zararın en aza indirilmesini öncelikleri arasında saymaktadır.

Kapsam olarak bakıldığında ise bilgi güvenliği, kişisel bilgisayar ve mobil cihazlar başta olmak üzere gerek kurumsal gerekse ulusal düzeydeki tüm iletişim cihazlarını ve kritik bilgi altyapılarını kapsamı içerisine alan, geniş perspektifte bir güvenlik yönetimi anlayışını ifade etmektedir (Güngör, 2015: 9). Söz konusu güvenlik anlayışı, saklanan verinin göndericiden alıcıya kadar bütünlüğü ve doğruluğu bozulmadan taşınmasını, yine saklanan veriye istenilen zamanda güvenli bir şekilde erişim sağlanmasını ve bilginin yetkisi olmayan

kişilerin izinsiz erişimlerinden korunması için ortaya konulan tüm çalışmaları kapsamaktadır (Özdemir, 2019: 10). Bu kapsamda planlanan ve gerçekleştirilen bilgi güvenliği süreçleri, aynı zamanda bu olgunun temel konu başlığını oluşturmaktadır. Zira bilgi güvenliğinin temelinde bilginin gizlilik ve bütünlüğünün her çeşit tehlike, tehdit ve saldırıya karşı korunarak, güvenlik açıklarının önüne geçmek yer almaktadır.

1.3. Bilgi Güvenliği Unsurları/İlkeleri

Bilgi güvenliğinin sağlandığı ortamların temel özellikleri, sadece yetkilendirilmiş kişilerin hassas bilgilere erişim sağlayabildiği ve bilgilerin doğru şekilde işlenerek ancak gerektiğinde kullanıldığı ortamlar olarak açığa çıkmaktadır. Buna bağlı olarak bilgi güvenliğinin "gizlilik", "bütünlük", "erişebilirlik", "kimlik tespiti" ve "güvenirlik" gibi temel özellikler ile ilişkilendirildiği görülmektedir. Diğer bir deyişle bilginin korunan niteliği, birbiri ile bağlantılı çeşitli unsurlardan oluşmaktadır.

Söz konusu unsurlardan ilkini "gizlilik" oluşturmaktadır. Bilginin yetkisiz ve izinsiz şekilde alıcısı dışındaki kişilerin eline geçmesinin önlenmesi anlamına gelen gizlilik ilkesi, bilginin sadece görev sorumluluğu kapsamında ilgili kişilerin erişimine açılmasını kapsamaktadır. Diğer bir unsur olan "bütünlük" ise bilginin alıcıya, göndericiden çıktığı haliyle bozulmadan ve bir bütün olarak ulaştırılmasını ifade etmektedir (Fussell, 2005). Bütünlük ilkesi kapsamında bilgi, alıcısına değiştirilmemiş, yeni veriler eklenmemiş, bir kısmı veya tamamı tekrarlanmamış ve sırasında değişiklik yapılmamış biçimde ulaştırılmalıdır (Tekerek, 2008: 133). Bütünlük ile anlatılmak istenen husus, bilginin doğru, kesin ve kendi içinde tutarlı olmasıdır (Özdemir, 2019: 15). "Erişebilirlik" unsuru ise bilgi veya kaynakların izinsiz şekilde durdurulmasının engellenmesi ve yetkiye sahip olan kullanıcıların uygun zamanda ve kolaylıkla sisteme giriş yapabilmeleri anlamına gelmekte, bilginin yetkili kullanıcılar için mümkün olduğunca serbest olması gerekliliğini açıklamaktadır. Zira bilgi sistemlerinden beklenen öncelikli nokta, işleri belirlenen zamanda yapmalarıdır (Yiğitbaşı, 2015: 60; Tuncer, 2019: 5). Dolayısıyla erişebilirlik, bilginin her an ulaşabilir olmasını ve sürekliliğinin sağlanmasını içermektedir.

Bilgi sistemlerinden hizmet temin eden alıcıların, beyan ettikleri kişiler olup olmadığı konusunda emin olmayı ifade eden unsur ise "kimlik tespiti" olarak ortaya çıkmaktadır (Marcinkowski ve Stanton, 2003). Genellikle ağ kullanımlarında karşılaşılan şifre uygulamaları, kullanıcı kimliğinin tespiti amacıyla diğer bir deyişle bu ilkenin hayata geçirilmesine yönelik kullanılan yöntemlerin başında gelmektedir.

Son olarak "güvenirlik" unsuru, sistemden yapması beklenilen davranış ile ortaya çıkan sonuçlar arasındaki tutarlılık durumunu ifade etmektedir (Genç, 2019: 73; Marcinkowski ve Stanton, 2003). Diğer bir deyişle bilgi iletişim sisteminin kendisinden beklenilen şeyleri belirlenen kurallar çerçevesinde eksiksiz ve tutarlı bir şekilde yerine getirmesi durumu güvenirlik unsurunun içeriğini oluşturmaktadır (Canbek ve Sağıroğlu, 2006; Vural, 2007: 42).

Birbirinden ayrı düşünülemeyen bu unsurlar, aynı zamanda birbirlerini ihlal etmemelidir. Örneğin bilginin gizliliği sağlanırken erişebilirliğine zarar verilmemeli, erişebilir hale getirilen bir bilginin bütünlüğü dikkate alınmalıdır. Zira aksi durumda bilginin doğruluğu tehlikeye düşecek ve olumsuz sonuçlar doğuracaktır.

1.4. Bilgi Güvenliğinin Gelişim Süreci

Bilgi güvenliğinin ortaya çıkışı günümüzde daha çok bilgisayar ve iletişim teknolojilerinde yaşanan hızlı gelişme ile eş zamanlı olarak kabul görse de, aslında bireyler bilgilerini ve deneyimlerini saklama, ihtiyaç halinde tekrar kullanma veya başkalarına aktarma isteğine var oldukları andan itibaren sahip olmuşlar ve bilgi güvenliğine ihtiyaç duymuşlardır.

Yazının icadıyla niteliksel olarak yazılı bir form halini alan bilgi çalınmaya, zarar verilmeye, değiştirilmeye karşı güvenli bir şekilde korunması gereken bir meta haline gelmiştir. (Baykara, Daş ve Karadoğan, 2013). İlk çağlarda özellikle politikacılar ve yöneticiler arasındaki yazışma ve haberleşmelerde görülen bilginin gizlenme ihtiyacı, mühürler veya özel kilitli kutular aracılığıyla sağlanmıştır (Özdemir, 2019: 18). Sanayi devrimi ile birlikte teknoloji gelişmeye ve yaygınlaşmaya başlamış, iletişim araçlarının icadı hızlanmış, sinyallerle taşınmaya başlanan bilgi için güvenlik olgusu farklı bir boyutta kendisini göstermeye başlamıştır. İnternetin hayata geçmesi ile başlayan küresel bilgi akışındaki olağanüstü artış ise, bilgi güvenliğini üzerinde ciddiyetle durulması ve politikalar üretilmesi gereken bir konu başlığı haline getirmiştir.

Solms (2000: 615) bilgi güvenliğinin gelişimini başlangıçta temel olarak üç döneme ayırmıştır. Bu dönemlerden ilki, 1980'lerin başına kadar olan, "İlk Dalga" olarak nitelendirilen ve bilgi güvenliğinin daha çok teknik bir yaklaşımla karakterize edildiği dönemdir. Bilgi güvenliği politikalarının pek yaygın olmadığı ve kullanıcıların yüksek düzeyde bir bilgi güvenliği bilinci geliştirememiş olduğu bu dönemde, bilgi güvenliğine daha çok erişim, kontrol listeleri, kullanıcı kimlik ve şifreleri gibi ana bilgisayar işletim sistemlerinin yerleşik olanakları kullanılarak ele alınabilecek bir şey olarak yaklaşılmıştır. Whitman ve Mattord (2011) bu süreci bilgisayar güvenliği olarak nitelendirerek, daha çok fiziksel güvenlik ve dosya sınıflandırması düzeyinde ele almaktadır.

1980'lerin başından 1990'ların ortalarına kadar olan dönem ise "İkinci Dalga" olarak adlandırılmıştır. Aynı zamanda "Yönetim Dalgası" olarak da nitelendirilen bu dönem, bilgi güvenliğinin önemini artırdığı ve güçlü bir yönetim boyutu kazandığı bir zaman dilimini oluşturmuştur. İnternetin gelişmesi ile birlikte bilgi güvenliği, kurum ve kuruluşların, özellikle de üst yönetim kademelerinin öncelikli konu başlığı haline gelmiştir. Dolayısıyla bu dönem itibariyle üst yönetimin bilgi güvenliği konusunda farkındalığı artmış, bilgi güvenliği konusunda uzman personel temini gerekleştirilerek bilgi güvenliği hakkında politikalar ve raporlar hazırlanmıştır (Solms, 2000: 616).

Dönemin devamında şirketler, bilgi güvenliğinde diğer şirketlerle kıyaslandığında nasıl daha iyi olabilecekleri, bilgi güvenliği konusunda nasıl daha fazla çevirim içi bilgi edinebilecekleri ve bilgi güvenliğinin insan boyutunun belki de en büyük sorun olduğu hususlarında araştırmalarını artırmışlardır. Bu nedenle bilgi güvenliği, birinci ve ikinci döneme paralel olarak kurumsal bir çaba olarak üçüncü dalgada gelişim göstermiştir.

1990'ların son birkaç yılından itibaren "Kurumsal Dalga" da denilen "Üçüncü Dalga" başlamıştır. Bu dalga bilgi güvenliği yönetimi için en iyi uygulama kuralları, uluslararası bilgi güvenliği sertifikasyonu, bilgi güvenliğinin bir kurum kültürü olarak geliştirilmesi, dinamik ve kesintisiz bilgi güvenliği ölçümü gibi yönleriyle karakterize edilmektedir. Bu üçüncü kurumsallaşma dalgası, yöntemsel ve teknik bir bilgi güvenliği altyapısının yanı sıra, şirketlerin bilgi güvenliği politikalarını, yöntemlerini ve sorumluluklarını destekleyen kurumsal bilgi güvenliği kültürünün oluşturulmasını sağlamıştır (Solms, 2000: 615-616).

Bilgi güvenliğinin gelişimi izlendiğinde, her bir dönemin birbirini etkileyerek ve bir ihtiyaçtan kaynaklanarak şekil aldığı görülmektedir. Bu kapsamda bir başka çalışmasında Solms (2006: 165-168), bilgi güvenliğinin "Dördüncü Dalga" ayağını ele almış ve bu dalgayı "Bilgi Güvenliği Yönetişimi" ile yakından ilişkilendirmiştir. 2000'li yıllarla birlikte başlayan bu dönemde bilgi güvenliği sadece teknik bir konu olmaktan tamamen uzaklaşmış, iyi bir kurumsal yönetişimin ayrılmaz bir parçası olarak kabul edilmeye başlanmıştır. Bu dönem itibariyle bilgi güvenliği, teknik, yönetimsel, kurumsal ve yönetişim boyutlarının bir arada ele alındığı bir gelişim sürecine girmiştir.

2. Bilgi Güvenliği Kapsamında Kişisel Verinin Korunması: Yasal ve Kurumsal Düzenlemeler

Bilginin korunması ve güvenliğinin sağlanması, her türlü risk, tehdit, hasar ve saldırılara karşı önlem alınması, günümüzde önemli politika alanlarından birisini oluşturmaktadır. Bununla birlikte bilgi güvenliğinin temelinde insanın yer

alması, insan kaynaklı risk ve tehdit faktörlerinin yanı sıra insana yönelik kişisel verilerin korunması konusunun ciddiyetini de oldukça artırmıştır.

Mahremiyetin, diğer bir deyişle gizliliğin bir insan hakkı olduğuna dair var olan genel kabul, insanların kendilerine ait bilgilerin adil bir şekilde işleneceği ve korunacağı konusunda güven arayışını beraberinde getirmektedir (Tataroğlu, 2013: 263). Kişi mahremiyetinin bir hak olarak toplumsal yaşam ve demokrasi açısından kritik öneme sahip olması, bilgi ve iletişim teknolojilerinde hızlı gelişmelerin yaşandığı günümüzde veri güvenliğine yönelik yasal ve kurumsal düzenlemeleri zorunlu kılmaktadır. Zira kişi mahremiyetinin üçüncü kişiler tarafından ihlalinin önlenmesi kadar, devlet ve birey arasındaki verinin güvenliği de aynı derecede önem taşımaktadır.

Bireyler çoğu zaman modern bilgi ve iletişim sistemlerinde kendileri ile ilgili ne tür verilerin toplandığı, bu verilerin ne kadar süre tutulacağı veya ne için kullanılacağı gibi soruların cevapları hakkında fikir sahibi olamamaktadırlar. Ayrıca internette veya sosyal ağ sistemlerinde bireylerin paylaştıkları kişisel bilgilere kimlerin erişebildiği sorusu, mahremiyet ve gizliliğe yönelik risklerin başka bir boyutunu oluşturmaktadır (Eroğlu, 2018: 134). Bu kapsamda kişisel veri denildiğinde ne anlaşılması gerektiği, gizliliğe yönelik risk ve tehditlerin farkına varmak açısından önemlidir. Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmekle birlikte (Henkoğlu, 2017: 50-21), bu özelliği kazanması ancak verinin işlenme sürecinde mümkün olabilmektedir. Kişisel verilerin işlenmesi, verilen elde edilmesi ve kaydedilmesi süreçlerinin yanı sıra bu verilerin düzenlenmesi, dönüştürülmesi, birleştirilmesi, uyarlanması, silinmesi gibi süreçleri de bünyesinde barındırmaktadır (Kaya, 2011).

Kişisel verilerin korunması amacıyla yasal ve kurumsal düzenlemeler üzerindeki temel çalışmalara bakıldığında, kişisel verilerin ilk defa 1948 tarihli Birleşmiş Milletler İnsan Hakları Evrensel Bildirgesi* ve 4 Kasım 1950'de imzalanan Avrupa İnsan Hakları Sözleşmesi (AİHS)** tarafından güvence altına alındığı görülmektedir. 1960'lı yıllardan itibaren ise bilgi teknolojilerindeki gelişmelerin etkisiyle, kişisel verilerin korunmasına yönelik daha kapsamlı uluslararası düzenlemelere ihtiyaç duyulmuştur. Bunun üzerine Avrupa Konseyi'nin "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına" ilişkin 108 Sayılı Sözleşmesi hayata geçirilmiştir.

* Bildirgenin 12. maddesi "Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır." diyerek kişinin özel yaşamının korunması ve mahremiyet hakkını dile getirmiştir.

** Sözleşmenin 8. maddesi "Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir." diyerek bilgi teknolojileri alanında yaşanan gelişmeler sonucunda, hukuki normlar çerçevesinde kişisel verilerin korunması ile ilgili çeşitli metinlerin hayata geçirilmesine dayanak oluşturmuştur (Avrupa Konseyi, 2020; Genç, 2019: 49).

Sonrasında ise Ekonomik Kalkınma ve İş birliği Örgütü'nün (OECD) 1980 yılında bilginin serbest dolaşımının engellenmesi, gizlilik ve mahremiyetin muhafaza edilmesi amacıyla yayımladığı ve 2013 yılında revize ettiği "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri", kişisel verilen işlenmesi ve korunması sürecinde dikkate alınması gereken temel noktaların altını çizen temel kaynaklardan birisi olarak ortaya çıkmıştır.

Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri başlıklı bu dokümanda yer alan ilkelerin başında "sınırlandırma ilkesi" gelmektedir. Buna göre veriler sadece yasal yollarla, hukuki amaçlara uygun şekilde ve kişilerin bilgisi dahilinde toplanması gerekmektedir. Diğer bir ilke, işlenen verinin doğru, eksiksiz ve güncel olmasını ifade eden "veri kalitesi" ilkesidir. Bir diğeri ise "amacın belirli olması" ilkesidir. Verilerin toplandıktan sonra kullanım amacında değişiklik yapılmamasını ifade eden bu ilke, verilerin sadece amacına uygun olarak işlenmesini ve kullanılmasını anlatmaktadır. "Kullanımın sınırlandırılması" ilkesi ise toplanan verilerin, sahibinin bilinçli rızası olmadan ve hukuki otoriteye dayanmadan açıklanmamasını vurgulamaktadır. Bir diğer ilke olan "koruyucu tedbirler" ilkesi ise verilere karşı oluşabilecek kayıp, yetkisiz erişim, zarar verme gibi tehlikelere karşı gerekli güvenlik önlemlerinin alınmasını içermektedir. "Açıklık ilkesi", kişisel verilerin korunmasına yönelik gelişme, uygulama ve politikalarda açık olunması gerektiğini ifade ederken, "bireysel katılım" ilkesi, bireyin kendisine ait verilere ulaşma, ihtiyaç halinde kopyasını isteme, silinmesini veya düzeltilmesini talep edebilme hakkını açıklamaktadır. Son olarak "hesap verebilirlik" ilkesi ise kişisel verileri kontrol altında tutanların tüm bu ilkelerle uyumunu sağlayacak yasal mevzuat ve yaptırımlara tabi olmasını ifade etmektedir (OECD, 2013; Ceran, 2015: 14; Eroğlu, 2018: 134-135).

Avrupa Birliği'nin 95/46 sayılı "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımı" isimli Yönergesi uluslararası alanda hayata geçirilen bir diğer düzenlemedir. Bu düzenlemeyle Avrupa Birliği'ne üye bütün ülkelerde kişisel verilerin eşit seviyede korunması garanti altına alınmaya çalışılmıştır. Bu çerçevede Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihinde "Genel Veri Koruma Tüzüğü (General Data Protection Regulation–GDPR)" onaylanmıştır (Akıncı, 2017).

Uluslararası düzenlemelerin yanı sıra konuya ilişkin Türk hukuk düzeninde kişisel verilerin korunmasına ve mahremiyetine ilişkin düzenlemelere bakıldığında temel düzenlemenin 1982 Anayasası olduğu görülmektedir. 1982 Anayasası 20. maddesi ile "özel hayatın gizliliğini" düzenlemiş, kişilerin özel hayatlarına ve aile yaşamlarına saygı gösterilmesini isteme hakkına sahip olduklarını belirtmiştir. Ayrıca Anayasa aynı maddede, *"Herkes, kendisiyle ilgili kişisel verilerin korunması-*

nı 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." diyerek kişisel verilerin korunmasını anayasal bir hak olarak düzenlemiştir (2709, md.20). Yine Anayasa'nın, 22. maddesi ile "haberleşme hürriyeti" başlığı ile haberleşmenin gizliliğini esas olarak kabul etmiştir (2709, md.22).

Kişisel verilen korunması noktasında katkı sağlayan bir diğer yasal düzenleme 2003 yılında hayata geçirilen "4982 sayılı Bilgi Edinme Hakkı Kanunu"dur. Kanun genel itibariyle kamu kurum ve kuruluşların faaliyetlerini kapsamakla birlikte mahremiyete ilişkin düzenlemelere de yer vermiştir. Bu kapsamda Kanun'un 21. maddesi *"Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır". (4982, md.21)* diyerek bilgi ve belge talebinde özel hayatın gizliliğini güvence altına alırken, 22. maddesi ile haberleşmenin gizliliğini ihlal edecek bilgi ve belge talebinin önüne geçmiştir (4982, md.22). Yine "Türk Ceza Kanunu" 134. maddesi ile 140. maddeleri arasında özel hayatın gizliliğini ihlal, hukuka aykırı şekilde kişisel verilen kaydedilmesi, başkasına verilmesi veya ele geçirilmesi gibi hususların gerçekleşmesi halinde uygulanacak olan yaptırımlar düzenlemiştir (5237, md.134-140).

Kişisel verilen korunmasına yönelik temel düzenlemelerin yanı sıra birçok alt hukuksal düzenlemeye de gidilmektedir. Fakat kamu yönetiminde bilgi iletişim teknolojilerinin kullanımı kapsamında bilgi güvenliğini etik yönü de dâhil olmak üzere geniş bir perspektifte ele alan en kapsamlı çalışma "6698 sayılı Kişisel Verilerin Korunması Kanunu" olmuştur. 7 Nisan 2016 tarihinde hayata geçirilen Kanun, *"kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları"* düzenlemektedir (6698, md.1). Başta kişisel verileri işlenen gerçek kişileri kapsamı içine alan Kanun, bu verileri herhangi bir veri kayıt sisteminin bir parçası olmak şartıyla çeşitli yollarla kısmen veya tamamen işleyen gerçek ve tüzel kişileri de kapsamına dâhil etmektedir (6698, md.2). Kişisel verilerin işlenmesinde hukuka uygunluk ve dürüstlük; doğru ve güncel olma; belirli, açık ve meşru amaçlar için işlenme; amaçla ilgili, sınırlı ve ölçülü olma gibi ilkeleri düzenleyen Kanun, kişisel verilerin ilgili kişinin açık rızası bulunmaksızın işlenemeyeceğini ifade etmiştir (6698, md.4-5).

Kanun ile birlikte aynı zamanda resmi bir veri koruma otoritesi olarak, söz konusu kanundaki düzenlemeleri uygulamada yerine getirmek amacıyla, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz "Kişisel Verileri Koruma Kurumu" oluşturulmuştur (6698, md.19). Kişisel verilerle ilgili gerek ulusal gerekse uluslararası düzenlemeleri, gelişmeleri ve mevzuattaki değişiklikleri izlemekle görevli olan Kurum, sorumluluk alanı itibariyle kamu kurum ve kuruluşları, üniversiteler, meslek kuruluşları gibi paydaşlarla koordinasyon halinde bulunma yetkisine sahiptir (6698, md.20).

Sonuç olarak kişisel verilerin korunması ve mahremiyetine ilişkin gerek Dünya'da gerekse Türkiye'de hayata geçirilen düzenlemeler değerlendirildiğinde, kişisel verilerin korunmasının her şeyden önce bir temel hak olarak kabul edildiği, temel hak ve özgürlükler arasında yer aldığı görülmektedir. Küresel boyutlara ulaşan veri paylaşımının güvenliğine yönelik bölgesel ve uluslararası çözüm arayışları ve uygulamalar düzenli olarak güncellenmeye çalışılmaktadır. Bu kapsamda Birleşmiş Milletler, OECD, AB ve Avrupa Konseyi gibi kuruluşlar etkili düzenlemeler ortaya koymaya devam etmektedirler. Türkiye özelinde ise 2010 yılı itibariyle anayasal güvence altına alınan kişisel verilerin korunması hususu, çeşitli yasal düzenlemelerle desteklenmekle birlikte 2016 yılında çıkarılan Kişisel Verilerin Korunması Kanunu ile veri koruma noktasında önemli bir basamağı aşmış bulunmaktadır.

3. Bilgi Güvenliğine Yönelik Riskler Ve Tehditler İle Bu Risk Ve Tehditlerin Giderilmesine Yönelik Öneriler

Bu bölümde öncelikle bilgi güvenliğine yönelik risk ve tehditlerin neler olduğuna değinilecek; ardından, bilgi güvenliğine yönelik risk ve tehditlerin giderilmesine yönelik öneriler geliştirilecektir.

3.1. Bilgi Güvenliğine Yönelik Riskler ve Tehditler

Bilgi güvenliğine yönelik tehdit ve riskler, bilgi varlıklarının gizliliği başta olmak üzere bütünlük ve erişebilirliğini olumsuz şekilde etkileyen unsurlar olarak ifade edilebilmektedir (Blanding, 2004). Gerek bireysel gerekse teknik açıdan ortaya çıkan zafiyetler, söz konusu risk ve tehditlerin bilgi sistemine zarar verecek seviyeye erişmesinde en etkili faktörü oluşturmaktadır.

Bilgi güvenliği ihlalleri, itibar kayıpları, finansal kayıplar, hizmetlerin aksaması veya hiç sunulamaması, veri kayıpları, gizli bilgilerin çalınması gibi birçok istenmeyen durumun meydana gelmesine neden olmaktadır (Tekerek, 2008: 132).

Bilgi güvenliğine yönelik risk ve tehditlerin oluşmasında en önemli faktörlerin başında "insan kaynaklı" olanlar gelmektedir. Kendi içerisinde iki kola ayrıla-

bilen bu tehditlerin ilki, kötü bir niyet taşımayan davranışlardan kaynaklanırken, diğeri bu durumun tam aksi şeklinde gerçekleşmektedir. Herhangi bir kullanıcının bilinçsiz ve bilgisizce sistemi kullanmasından doğan ilk gruptaki tehditler, bireylerin yeterli eğitime sahip olmadan sisteme dahil olmaları sonucu ortaya çıkmaktadır (Tekerek, 2008: 134). Kötü niyet taşıyan davranışlar sonucu oluşan tehditler ise özellikle sisteme zarar verme amacı taşıyan, saldırganlar eliyle sisteme yönelik olarak gerçekleştirilen eylemlerden kaynaklanan tehditlerdir. Bu tür tehditlerde saldırganlar daha çok sistemde bulunan güvenlik boşluklarından yararlanmaktadır (Shephard, 2002). Kasıtlı tehditler olarak da ifade edilen bu tür tehditlerde, bilgisayar ağlarını izlemede kullanılan araçlar vasıtasıyla özel bilgilere saldırılar gerçekleştirilmektedir (Seferoğlu vd., 2018: 34)

Bilgi güvenliğine yönelik bir diğer risk ve tehdit faktörü "fiziksel" koşullardan kaynaklanan tehditlerdir. Bu tür tehditlerin önemli özelliklerinden birisi genellikle önceden tespit edilemiyor oluşlarıdır. Doğa olaylarının ağırlıkta olduğu söz konusu tehditler, çoğunlukla öngörülemez olduklarından, engellenme ihtimalleri de çok düşüktür. Deprem, sel, yangın, ani sıcaklık değişimleri, toprak kayması, çığ düşmesi gibi olaylar bu tarz tehditlere örnek olarak gösterilmektedir. (Shephard, 2002).

Yazılım veya donanım sistemlerinden kaynaklanan zayıflıklar nedeniyle oluşan tehditleri ifade eden "korunmasızlık" ise bilgi güvenliğine yönelen bir diğer tehdit unsurunu oluşturmaktadır. Bu tehditte yazılım veya donanımda ortaya çıkan güvenlik boşluğu, saldırganlar tarafından keşfedilmekte, bu güvenlik boşluğu sayesinde sistemdeki bilgisayarlara ve tüm ağ üzerindeki kaynaklara yetkisiz ve izinsiz erişim sağlanmaktadır (Shephard, 2002).

Bunların yanı sıra verilerin değiştirilmesi veya yok edilmesi, fiziksel donanımların imhası gibi bir sistemin işletimine zarar vererek bilgi toplama anlamına gelen aktif tehditlerden bahsedilebileceği gibi, sistemin kaynaklarını etkilemeden bilgi toplamayı amaçlayan pasif tehditlerden de söz edilebilmektedir (Seferoğlu vd., 2018: 34).

3.2. Bilgi Güvenliğine Yönelik Riskler ve Tehditlerin Giderilmesine Yönelik Öneriler

Bilgi güvenliğine yönelik öncelikli husus, hem bireylerin hem de toplum ve kurumların bakış açılarının değiştirilmesi gerekliliğidir. Bilgi güvenliğinin sürekli yönetilecek bir süreç özelliği taşıdığı, teknolojiden önce insana yatırım yapılmasıyla yakından ilgili olduğu ve kurumların en tepe noktasından başlanarak bu konuda bilinçlendirilmesi gerektiği unutulmaması gereken noktaları oluşturulmaktadır (Eminağaoğlu, 2008). Dolayısıyla bilgi güvenliğinin sağlanmasında ve

karşılaşılan risk ve tehditlerin en aza indirilmesinde gerekli olan temel yöntemlerden ilki, gerek bireylere gerekse kurumlara "eğitim ve bilinç" kazandırılmasıdır. Bilgi sistemlerini kullanan bireylerin, bilgi güvenliğine yönelik eğitimlerle bilinçlendirilmesi, risk ve tehditlerin insani boyutundan kaynaklanan aksaklıkların en aza indirilmesini sağlayacaktır. Bunun yanı sıra bilgi güvenliği hakkında bilinçlendirilen bireyler, kendileri kadar kurumlar açısından da bir tehdit unsuru olmaktan çıkacaklardır.

Bilgi güvenliğinin kurumlarda etkin ve etkili sağlanabilmesi ise öncelikle üst düzey yöneticilerin maddi ve manevi desteğine bağlıdır. Yöneticilerin bilgi güvenliği süreçlerini sahiplenmesi, bilgi güvenliğine yönelik politikaların kurum içinde alt kademeler tarafından benimsenmesini kolaylaştıracaktır. Bunun yanı sıra güvenlik süreçleri, denetlenen, desteklenen ve geliştirilen bir yapıda tasarlanmalı, bilgi güvenliğinin sadece teknoloji temelli bir oluşum olmadığı anlaşılmalıdır (Eminağaoğlu ve Gökşen, 2009: 9).

Bilgi güvenliğinin sağlanması noktasında yine, teknik önlemleri alma sorumluluğuna sahip kişilerin yanı sıra hukuksal altyapıyı oluşturmakla yükümlü idari personelin kişisel verilerin korunmasına yönelik bakış açılarında farklılıklar olması, süreci verimsizleştiren unsurlardan birisini oluşturmaktadır (Henkoğlu, 2015: 31-32). Dolayısıyla söz konusu farklılık giderilerek, veri konusunun sistem yaklaşımı çerçevesinde bir bütün olarak değerlendirilmesi ve buna uygun şekilde stratejiler geliştirilmesi gerekmektedir. Bu kapsamda minimum veri kaydının ve depolamanın yapılması, veri yedekleme planlarının oluşturularak veri değişikliklerinin izlenmesi, verilerin saklanacağı ortamın fiziksel tehditler kadar elektromanyetik tehditler açısından da değerlendirilmesi, veri sorumlusunun belli olması gibi hususlar kişisel verilerin risk ve tehditlere karşı korunması adına verilebilecek öneriler arasında yer almaktadır (Henkoğlu, 2017: 54). Yine veri saklama sürecinde yaşanılan belirsizliklerin en aza indirilmesi, verilerin kimlerle ve hangi şartlarda paylaşılabileceğinin güvenlik politikalarında yer alması öneriler arasında sayılabilir.

Sonuç

Bilgi iletişim teknolojilerinin hayatın her alanına nüfuz etmesiyle, geçmişten günümüze değerli bir kaynak olan bilginin elektronik ortamlarda işlenmesi, taşınması ve saklanması kolaylaşmış, bilgiye mekândan ve zamandan bağımsız olarak erişimi mümkün kılan dijital çağ, bilgiye yönelik güvenlik tehditlerini ve risklerini aynı oranda artırmıştır. Bu durum, bilginin korunması gerekliliğine vurgu yaparak "bilgi güvenliği" kavramını daha fazla önemsenmesi ve geliştirilmesi gereken bir unsur olarak ortaya çıkarmıştır.

Kişilerin, kurum ve hatta devletlerin sahip oldukları önemli bilgiler, fiziksel koşullardan kaynaklanan sel, deprem, yangın gibi doğal tehditlerin yanı sıra bilgi hırsızlığı, korsan atakları, yetkisiz ve izinsiz erişim, kötü niyetli bilgi suiistimalleri gibi insan ve sistem kaynaklı birçok tehditle karşı karşıya kalmaktadır. Bu kapsamda bilginin korunması ve güvenliğinin sağlanması ile her türlü risk, tehdit, hasar ve saldırılara karşı önlem alınması, günümüzde önemli politika alanlarından birisini oluşturmaktadır.

Bilgi güvenliğine yönelik karar alma ve politika belirleme süreçlerine dayanak oluşturmak amacıyla bireysel veri güvenliğine yönelik olarak gerek dünyada gerekse Türkiye'de çeşitli hukuki düzenlemeler yapıldığı görülmektedir. Bu sayede ülkeler bu konudaki hukuki boşlukları doldurulmaya çalışmakta; bilginin gizliliğine, bütünlüğüne veya güvenliğine yönelik saldırılar çeşitli yaptırımlara tabii tutulmaktadır. Nitekim, BM, OECD ve AB gibi yapıların konuya özel önem verdikleri, konu ile ilgili uluslararası düzeyde ve etkin ilke ve mekanizmalar oluşturmak yoluyla sürece aktif bir şekilde dahil oldukları görülmektedir. Özellikle "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri" ve "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımı" başlıklı belgeler, kişisel veri güvenliğini temel alarak genel anlamda bilgi güvenliğini de garanti altına almayı hedefleyen çok önemli ilkeler ve uygulama araçları öngörmektedir. Türkiye'de de bu duruma koşut olarak bir takım düzenlemeler yapılmaktadır. Bu çalışmalar içerisinde özellikle "6698 sayılı Kişisel Verilerin Korunması Kanunu"nun çıkarılması ve bu kanuna dayalı olarak kurulan "Kişisel Verileri Koruma Kurumu"nun çalışmaları ile önemli adımlar atıldığı görülmektedir.

Tüm bu düzenlemeler değerlendirildiğinde, öncelikle kişisel verilerin korunmasının her şeyden önce bir hak olarak kabul edilerek temel hak ve özgürlükler arasında yer aldığı görülmektedir. Bilgi güvenliğinin en önemli unsuru olan kişisel veri güvenliğine yönelik bu hak ve özgürlük temelli yaklaşımın konunun önem ve ciddiyetini vurgulamak açısından önemli olduğu ifade edilebilir. Ancak bu yaklaşımın gerçek anlamda hayata geçirilebilmesi için bilgi/veri güvenliği gibi, büyük çaplı değişikliklerin hızlı biçimde gerçekleştiği, içerisinde dinamik süreçler barındıran bir konuda, uluslararası/ulusal tüm kurum ve kuruluşların hızlı ve etkin karar alıp uygulama yetkinliğine sahip olması büyük önem taşımaktadır.

Bilgi güvenliğinin bir ürün, araç veya hizmet olmaktan ziyade bir süreci oluşturduğu göz önüne alındığında bu alanda hayata geçirilecek önlem ve politikaların geniş bir perspektifte ele alınması gerekliliği de ayrıca ortaya çıkmaktadır. Zira özelikle elektronik ortamların kullanımının yaygınlaşması ve buna bağlı olarak kişisel veri olarak nitelendirilen unsurların hedef alındığı saldırıların boyut

ve şekil değiştirmesi, teknik veya idari güvenlik önlemlerini tek başına yetersiz kılmaktadır. Bu kapsamda bilginin güvenliğini sağlamada bilginin üretilmesinden elde edilmesine, saklanmasından yok edilmesine kadar olan bilgi işleme sürecinde sorumluluk paylaşımının esas alınması gerekmektedir. Dijital çağın kullanıcıları olan bireylerde, bilgi güvenliğine yönelik tehdit ve risklerin önlenmesi noktasında farkındalık oluşturulması önemli bir hususu oluşturmaktadır. Bireylerin yanı sıra kurumların da söz konusu bilince ulaştırılması, hukuki ve teknik altyapı ile desteklenen bilgi güvenliği sürecinin başarıya ulaşmasında önemli bir ilerleme gerçekleştirilmesini sağlayacaktır.

Kaynakça

Ackoff, R. L. (1989), "From Data To Wisdom Presidential Address To ISGSR", *Journal of Applied Systems Analysis*, 16(1), 3-9.

Akıncı, A. N. (2017),*Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi*, Çalışma Raporu, T.C. Kalkınma Bakanlığı, Yayın No: 2968.

Argyris, C. (1993), *Knowledge for Action: A Guide to Overcoming Barriers to Organizational Change*, San Francisco: Jossey-Bass.

Avrupa Konseyi (2020), *Avrupa İnsan Hakları Sözleşmesi*, European Convention on Human Rights (coe.int) Erişim 15.03.2021.

Balay, R. (2000), *Yönetici ve Öğretmenlerde: Örgütsel Bağlılık,*Ankara: Nobel Yayıncılık.

Baykara, M., Daş, R. ve Karadoğan, İ. (2013),*Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi*, 1st International Symposiumon Digital Forensics and Security, Elâzığ.

Blanding, S. F. (2004),*An*I*ntroduction To LAN/WAN Security. Information Security Management Handbook,* New York: Auerbach Publications.

Canberk G. ve Sağıroğlu Ş. (2006), "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Politeknik Dergisi*, 9(3), 165-174.

Ceran, A. (2015),*Türkiye'de ve AB'de Kişisel Verilerin Korunması*, İstanbul: İktisadi Kalkınma Vakfı Yayınları. İktisadi Kalkınma Vakfı / Türkiye›de ve AB›de Kişisel Verilerin Korunması (ikv.org.tr) Erişim 15.03.2021

Cherdantseva, Y. ve Hilton, J. (2013),*A Reference Model of Information Assurance Security*, International Conference on Availability, Reliability and Security, IEEE.

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

Eminağaoğlu M. (2008),*Dikkat Casus Var! Bilgi Güvenliği Yazı Dizisi*, İstanbul:Tekborsa.

Eminağaoğlu, M. ve Gökşen, Y. (2009),"Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri",*Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 11(4),1-15.

Fussell, R.S. (2005),*Protecting Information Security Availability Via Self-Adapting İntelligent Agents.* Military Communications Conference, IEEE.

Genç, C. (2019), *Kişisel Verilerin Korunması Kapsamında Bilgi Güvenliği Farkındalığı Analizi ve E-Devlet Yapısının İncelenmesi*, Yüksek Lisans Tezi, İstanbul Okan Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Güngör, M. (2015),*Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma*, Uzmanlık Tezi, Bilgi Toplumu Dairesi Başkanlığı, Kalkınma Bakanlığı.

Henkoğlu, T. (2015),*Bilgi Güvenliği ve Kişisel Verilerin Korunması*, Ankara: Yetkin Hukuk Yayınları.

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

Kaya, C. (2011), "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas Veriler ve İşlenmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 69(1), 317-334.

KVKK (2016), "Kişisel Verilerin Korunması Kanunu", 15.03.2021 tarihinde Mevzuat Bilgi Sistemi adresinden erişilmiştir.

Lyotard, J. F. (2000), *Postmodern Durum,* (Çev: A. Çiğdem). Ankara: Vadi Yayınları.

Marcinkowski, S.J. ve Stanton, J.M. (2003),*Motivational Aspects Of İnformation Security Policies.*, IEEE International Conference On Systems, Man and Cybernetics.

Nonaka, I. ve Takeuchi, H. (1995), *The Knowledge-Creating Company*, New York: Oxford University Press.

OECD (2013), "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri", OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECDErişim 15.03.2021.

Özdemir, A. (2019),*Kamu Kurum ve Kuruluşlarında Bilgi Güvenliği Farkındalığı*, Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

Pfleeger, S. L. (1997),*The Fundamentals Of Information Security*, IEEE.

Puhakainen, P. (2006), A *Design Theory For İnformation Security Awareness. Academic Dissertation.* University of Oulu, Faculty of Science, Department of Information Processing Science, Finland.

Seferoğlu, S. S., YıldızDurak, H., KaraoğlanYılmaz, G. ve Yılmaz, R. (2018),"Bilgi Güvenliği Farkındalığı ve Bilgi Güvenliği Politikalarıyla İlgili Bir İnceleme", (Ed.) Akkoyunlu, B., İşman, A. ve Odabaşı, H. F.,*Eğitim Teknolojileri Okumaları,*Adapazarı: TOJET ve Sakarya Üniversitesi.

Selvi, Ö. (2012),"Bilgi Toplumu, Bilgi Yönetimi ve Halkla İlişkiler", *Gümüşhane Üniversitesi İletişim Fakültesi Dergisi*, (3), 191-214.

Shephard, B. (2002),*Information Security-Who Cares?. Power System Management and Control*, Fifth International Conference on (Conf. Publ. No. 488).

Solms, B. V. (2000),"Information Security-The Third Wave?",*Computers And Security,* 19(7), 615–620.

Solms, B. V. (2006),"Information Security-The Fourth Wave",*Computers And Security*, 25(3), 165-168.

Surwade, Y.ve Patil, H. (2019), "Information Security",*Knowledge Librarian An International Peer Reviewed Bilingual E-Journal Of Library And Information,* (Özel Sayı), 458-466.

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

TBMM. (1949), "İnsan Hakları Evrensel Beyannamesi", BM-30.qxd (ombudsman.gov.tr) Erişim 03.15.2021.

Tekerek, M. (2008),"Bilgi Güvenliği Yönetimi",*KSÜ Fen ve Mühendislik Dergisi,* 11(1), 132-137.

Tuncer, İ. (2019),*Bilgi Güvenliği Açısından Bir Değerlendirme: E-Devlet Uygulamaları,* Yüksek Lisans Tezi, Fırat Üniversitesi Sosyal Bilimleri Enstitüsü, Elâzığ.

Uğraş, T. (2015), "Bilgi Tüketicileri ve Üreticileri", (Ed.) Gülseçen S., *Bilgi Yönetimi*: *Bilgi Türeticileri, Büyük Veri, İnovasyon ve Kurumsal Zeka,* İstanbul: Papatya Yayınları.

Vural, Y. (2007),*Kurumsal Bilgi Güvenliği ve Sızma Testleri,* Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Whitman, M. E. ve Mattord, H. J. (2011), *Principles of Information Security*, Cengage Learning.

Yalçın, Ş. (2016), "Neyi Bilebiliriz?", İnönü Üniversitesi Uluslararası Sosyal Bilimler Dergisi, 5(2), 7-20.

Yiğitbaşı, İ. (2015), "Bilginin Korunması", (Ed.) Gülseçen S., *Bilgi Yönetimi*: *Bilgi Türeticileri, Büyük Veri, İnovasyon ve Kurumsal Zeka,* İstanbul: Papatya Yayınları.