T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI

KİŞİSEL BİLGİLERİN GÜVENLİĞİ ve KORUNMASI: TÜRKİYE VE İRLANDA ARASINDA KARŞILAŞTIRMALI BİR ANALİZ

MUHAMMED ALİ AYDEMİR

YÜKSEK LİSANS TEZİ

DANIŞMAN:
DOÇ. DR. MUSTAFA KOCAOĞLU

KONYA-2021

Bilimsel Etik Sayfası

Öğrencinin	Adı Soyadı	Muhammed Ali Aydemir		
	Numarası	18810401007		
	Ana Bilim / Bilim Dalı	Siyaset Bilimi ve Kamu Yönetimi		
	Programı	Tezli Yüksek Lisans	✓	
		Doktora		
	Tezin Adı	Kişisel Bilginin Güvenliği ve Korunması: Türkiye ve İrlanda Arasında Karşılaştırmalı Bir Analiz		

Bu tezin hazırlanmasında bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını bildiririm.

Muhammed Ali AYDEMİR

ÖZET

Öğrencinin	Adı Soyadı	Muhammed Ali AYDEMİR		
	Numarası	18810401007		
	Ana Bilim / Bilim Dalı	Siyaset Bilimi ve Kamu Yönetimi/Siyaset Bilimi ve Kamu Yönetimi		
	Programı	Tezli Yüksek Lisans	✓	
		Doktora		
	Tez Danışmanı	Doç. Dr. Mustafa KOCAOĞLU		
	Tezin Adı	Kişisel Bilgilerin Güvenliği ve Korunması: Türkiye ve İrlanda Arasında Karşılaştırmalı Bir Analiz		

İnsanlar tarih boyunca bilgiye birçok değer atfetmiştir. Bunlardan en bilineni ise "bilgi güçtür" ifadesidir. Bununla birlikte, bilgiyi her toplum tanımlamaya çalışmıştır fakat ortak bir tanıma ulaşamamışlardır. Ancak bilgisayarın ve bilgi depolama yöntemlerinin icat edilmesi, bilginin tanımlanmasını kolaylaştırmış ve kendi içerisinde aşamalara ayrılmasına imkân sağlamıştır. Bundan dolayı kişisel bilgi ve bilgi arasında bir ayrım yapıldıktan sonra kişisel bilgi; kişisel veri, kişisel enformasyon ve kişisel bilgi olarak birbirinden ayrılmıştır. Böylece bilgi ve kişisel bilgi hakkında yapılan çalışmalarda sıkça görülen veri-enformasyon-bilgi ve kişisel veri-kişisel enformasyon-kişisel bilgi kavramlarının hem kendi içlerinde hem de birbirleri arasındaki kavramsal sınırlar daha belirgin hale gelmiştir.

Güvenlik ve korunma isteği ise insanın fizyolojik ihtiyaçlarından sonra gelen en önemli ihtiyacıdır. İnsanın kendi güvenliği ile birlikte kişisel bilgisinin de güvenliğini sağlaması gerekmektedir. Bu sebeple devletler kişisel bilgileri korumaya yönelik çeşitli önlemler almaktadır. Bu önlemler her ne kadar devlet eliyle yapılmış olsa da insanların başkalarının mahremiyetlerine saygı duyması için bu düzenlemeleri etik kurallardan biri kabul ederek erdemli bir davranış haline getirilmesi gerekmektedir. Bu sebeple bilgi ve kişisel bilgi ile beraber etik, erdem, mahremiyet ve güvenlik gibi kavramlar da önem kazanmıştır.

Dünya'da kişisel bilginin korunmasına yönelik düzenlemeler her geçen gün daha da önem kazanmaktadır. Bu çalışmada ilk olarak bilgi ve kişisel bilgi ele alınmış, ardından kavramsal çerçeve netleştirilmiştir. Diğer bir ifade ile kişisel bilgi, bilgi kavramından ayrılarak sınırları belirginleştirilmiştir. İkinci bölümde ise öncelikle güvenlik ve korunma kavramlarının gelişimi incelenmiştir. Ardından bu kavramlar bilgi ve kişisel bilgi ekseninde ayrıntılı biçimde ele alınmıştır. Son bölümde ise Türkiye ve İrlanda'nın son yıllarda yapılmış olan kişisel veri düzenlenmeleri incelenerek karşılaştırmalı bir analiz yapılmıştır. Bu analiz sonucunda her iki ülkede de son dönemde kişisel bilgi hiyerarşisinde önemli görülen kişisel verinin güvenliği ve korunmasına ilişkin yeniliklerin bu konudaki yetkinlikleri artırdığı görülmüştür.

Anahtar Kelimeler: Bilgi, Kişisel Bilgi, Güvenlik, Korunma, Mahremiyet, Erdem, Etik, İrlanda, Türkiye.

ABSTRACT

Author's	Name and Surname	Muhammed Ali AYDEMİR		
	Student Number	18810401007		
	Department	Political Science and Public Administration		
	Study Programme	Master's Degree (M.A.)	✓	
		Doctoral Degree (Ph.D.)		
	Supervisor	Assoc. Prof. Mustafa KOCAOĞLU		
	Title of the Thesis/Dissertation	Security and Protection of Personal Knowledge: A Comparison Analysis Between Turkey and Ireland		

Throughout history, people have attributed many values to knowledge. The most well-known of these is the phrase "Knowledge is power". However, every society tried to define knowledge, but they could not reach a common definition. Nevertheless, the invention of the computer and knowledge storage methods facilitated the identification of knowledge and allowed it to be divided into stages within itself. Therefore, after making a distinction between personal knowledge and knowledge, personal knowledge; it is separated as personal data, personal information and personal knowledge. Thus, the conceptual boundaries between the concepts of data-information-knowledge and personal data-personal information-personal information, which are frequently seen in studies on knowledge and personal knowledge, both within themselves and between each other have become more evident.

The desire for security and protection is the most important need after the physiological needs of the human being. People need to ensure the security of their personal knowledge along with their own security. For this reason, states take various measures to protect personal knowledge. Although these measures are made by the state, people should accept these regulations as ethical rules and make them a virtuous behaviour in order to respect the privacy of others. For this reason, concepts such as ethics, virtue, privacy and security were studied along with knowledge and personal knowledge.

Regulations for the protection of personal knowledge in the world get more and more importance every day. In this study, firstly, knowledge and personal knowledge were discussed and then the conceptual framework was clarified. In other words, personal knowledge has been separated from the concept of knowledge and its boundaries have been clarified. In the second part, firstly, the development of the concepts of security and protection is examined. Then, these concepts are discussed in detail on the axis of knowledge and personal knowledge. In the last part, a comparative analysis has been made by examining the personal data regulations of Turkey and Ireland made in recent years. As a result of this analysis, it has been seen that the innovations regarding the security and protection of personal data, which are

considered important in the hierarchy of personal knowledge in both countries, have increased the competencies in this regard.

Keywords: Knowledge, Personal Knowledge, Security, Protection, Privacy, Virtue, Ethics, Ireland, Turkey.

İÇİNDEKİLER

TABLOLAR LİSTESİ

KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
APEC	AsiaPasicific Economic Cooperation
BİT	Bilgi ve İletişim Teknolojileri
BM	Birleşmiş Milletler
BS	Bilgi Sistemleri
DPC	Veri Koruma Komisyonu
DYY	Doğrudan Yabancı Yatırımcı
EDPS	Avrupa Veri Koruma Denetçisi
GDPR	Genel Veri Koruma Yönetmeliği
IBM	International Business Machine
KVK	Kişisel Verileri Koruma
KVKK	Kişisel Verileri Koruma Kanunu
LED	Yasa Uygulama Direktifi
ODPC	Veri Koruma Komiseri Ofisi
OECD	İktisadi İşbirliği ve Gelişme Teşkilatı
TBMM	Türkiye Büyük Millet Meclisi
UNDP	Birleşmiş Milletler Kalkınma Programı

TEŞEKKÜR

Tez çalışmam süresince akademik tecrübesi ve bilgisi ile bana destek olan danışmanım Doç. Dr. Mustafa Kocaoğlu'na şükranlarımı sunarım.

Tezimin savunma aşamasında birikimleri ve değerli eleştirileri ile katkı sağlayan Doç. Dr. Resul ÖZTÜRK ve Dr. Öğrt. Üyesi Hikmet Salahaddin Gezici'ye teşekkür ederim.

Beni her daim maddi ve manevi destekleyip hiçbir zaman bana olan güvenlerinden şüphe duymayan ve beni yetiştiren annem Leyla Aydemir ve babam Mahmut Ercan Aydemir'e, ağabeylerim Niyazi Aydemir ve Yalçın Aydemir'e, kardeşlerim Abdullah Enes Aydemir ve Rabiya Aydemir'e sonsuz teşekkürü bir borç bilirim.

GİRİŞ

Sokrates "iyi olan tek şey bilgi, kötü olan tek şey bilgisizliktir" demiştir. Farabi ise "Erdemlerin en büyüğü bilimdir, bilgeliktir. Bilgi uçsuz bucaksız ve kıyısız bir denizdir. Doğru bilgi insanca yaşamanın temelidir" diyerek bilginin öneminin anlaşılmasına ışık tutmuştur. Filozof F. Bacon ve A. Comte ise "Egemen olmak için bilmek" gerekir diyerek bilgiye sahip ve hâkim olmanın önemini vurgulamışlardır (Atılgan, 2009: 201; Engin, 2005). Aristoteles ise "İnsan düşünen bir hayvandır" diyerek düşünmenin insana ait olduğunu ve bu yol ile bilginin sadece insana ait olduğuna ışık tutmuştur.

Bilgi, insan yaşamının var olduğu ilk andan bugüne kadar değerini artırarak süregelmiştir. Bilginin önemli olduğu ve aynı derecede geliştiği toplumlar her çağda refah seviyelerini artırmakta başarılı oldukları bilinmektedir. Bununla birlikte bilgiyi kendi çıkarları doğrultusunda kullanan devletler ise bilgi sayesinde kendi dönemlerine hükmetmekte oldukça başarılı olmuşlardır. Devletlerin bilgiye sahip olduklarında elde ettikleri başarılarla birlikte bilginin gelişmesi için sağlanması gereken destekler de önemli hale gelmiştir. Nitekim modern çağ öncesi devletler kuruluşları ile birlikte bilginin merkezi olan kütüphaneleri ve eğitimin merkezi olan medreseler/okullar imar edilmesine öncelik vermişlerdir.

Toplumda bilgi her zaman önemli olmuştur. Bu nedenle toplumlar geliştikçe bilgiye sahip olmanın öneminin de çok hızlı artmakta olduğu yadsınamaz bir gerçektir. İnsanlığın yerleşik hayata geçmeye başlamasıyla birlikte insanlar arasındaki ilişki ve iletişim seviyesi de artmaya başlamıştır. Fakat bu dönemde iletişimi piktografik[1] işaretler aracılığıyla yapıldığı bilinmektedir. Örneğin; Göbeklitepe'nin ibadet bölümünde bulunan taşlar üzerindeki kabartma tasvirlerin yazının ilk şekilleri olduğu düşünülmektedir. Ayrıca bu durum ispatlandığı zaman yazının ilk olarak Sümerler tarafından bulunduğu tezi de çürütülmüş olacaktır. Bu durumla birlikte bilginin de oluşmasının ve diğer nesillere yazı yoluyla aktarılması olayının daha eskilere dayandığı da anlaşılacaktır. Yazının gelişmesiyle birlikte bilgilerin gelecek nesillere

[1] Mağara duvarlarına çizilen veya resmedilen şekillere denilmektedir. Bir sonraki aşaması çivi yazısıdır.

aktarılması kolaylaşmış ve bilginin de gelişimi aynı seviyede artarak devam etmiştir (Özkaral, 2015: 372).

Bilginin gelişimi ise özellikle bilginin tanımlanması çalışmaları sürecinde gerçekleşmiştir. Bilgiyi ilk olarak antik çağ filozofları tanımlamaya ve yorumlamaya çalışmışlardır. Fakat bu tanımlama çalışmalarına rağmen nesnel bir tanıma ulaşılmamıştır. Çünkü bilgi içinde bulunduğu dönemin, coğrafyanın, kültürün, ırksal ve dinsel faaliyetlerin durumuna göre değişiklikler ve farklılıklar gösterdiği için sürekli bir tanımsal değişim içerisinde bulunmuştur. Bununla birlikte sanayinin geliştiği 18.yüzyıla kadar bilginin tanımlanması çalışmaları felsefeciler/filozoflar tarafından epistemoloji(bilgi felsefesi) dalı altında yapılmıştır. Fakat sanayi devrimi ile birlikte bilginin tanımlanmasında her bilim dalı kendi bilgi tanımını yapmaya çalışmıştır. Böylece bilgi çok yönlü durumlarda değerlendirilmeye alınmıştır. Özellikle İkinci dünya savaşı sonrasında bilgisayarın icadı ve bilgiyi depolamanın dijital yöntemleri keşfedilip ilerlemeye başlamasıyla birlikte bilgi kendi içerisinde aşamalara ayrılmıştır. Bu durum bilginin anlaşılmasında nesnel tanım eksikliği karmaşanın azaltılabileceği de düşünülmüştür. Bu sebeple bilginin işlenmesi, analiz edilmesi ve kavranması halleri birbirinden ayrılarak bilgiye "veri" (data), "enformasyon" (information) ve "bilgi" (knowledge) aşamaları eklenerek bilgi kendi içinde ayrıştırılmıştır.

Bunlarla birlikte bilginin kendisi "Açık ve Örtük bilgi, Sığ ve Derin Bilgi, Teknik ve Uygulanabilir Bilgi, Ortak Anlayış Olarak Bilgi" bölümlerine ayrılarak bilginin türlerinde sınıflandırılma yapılmıştır. Yapılan bu sınıflandırmayla hangi bilginin nasıl, nerede, ne zaman ve kim tarafından kullanılması gerektiğinin anlaşılmasında önemli bir adım atılmıştır.

Bu çalışmada özellikle kişisel bilginin aşamalandırılması ile sosyal, kültürel, ekonomik ve bilimsel vb. olarak kullanılan bilgi türü ile bireylerin özel hayatındaki bireyler arası ilişkilerden ve kendi üretimlerine bağlı olarak oluşan eserlerden vb. durumlardan meydana gelen kişisel bilgileri birbirinden ayırmak amaçlanmıştır. Bu

yolla bu konu hakkındaki karmaşa azaltılmak istenmiştir. Bilgi ve kişisel bilgi arasındaki ayrımı belirleyen tanımsal ve kavramsal çerçeve oluşturulmadığı için bilginin anlaşılması ve tanımlanması zorlaşmaktadır. Bu sebeple bu çalışmada bilgi; veri, enformasyon ve bilgi olarak ele alınmıştır. Kişisel bilgi ise; kişisel veri, kişisel enformasyon ve kişisel bilgi olarak kendi içinde aşamalara ayrılarak tanımsal çerçeve daha anlaşılır hale getirilmiştir.

Nitekim ilk olarak bilgi ve kişisel bilgi arasında bir ayrım yapıldıktan sonra, bilgi güvenliği çerçevesinde kişisel bilginin korunmasının önemi ve nedenleri incelenmiştir. Devamında kişisel bilgilerinin korunması hususunda erdem, etik, mahremiyet ve güvenlik kavramlarının kişisel bilgilerin korunması üzerindeki rolleri ve önemleri çalışılmıştır. Bu kavramların kişisel bilgilerin korunmasını sağlama hususunda hayati bir öneme sahip olduklarının da yadsınamaz bir gerçek olduğu anlaşılmaktadır. Çünkü kişisel bilgilerin korunması genel geçer etik kurallarına dâhil edilmesi ve bu hususun bir erdem davranışı olduğu anlayışı oluşturulduğu zaman kişisel bilgilerin mahremiyeti ve güvenliği sağlanmış olacaktır. İlk bölümün son başlığında ise bilgi ve kişisel bilginin tarihsel süreç içerisindeki konumu ele alınarak bilginin ve kişisel bilginin gelişimine genel olarak ışık tutulmuştur.

Hem ulusal hem de uluslararası düzeyde risklerin çoğaldığı ve arttığı bir çağda, yaygın kullanılan bir ifadeyle insan güvenliği olarak bilinen bireyin güvenliği, yaygın tehdit ve korkulara karşı bir entelektüel söylem ve politika tartışması alanı haline gelmiştir. Bu durum özellikle soğuk savaşın sona ermesi ile birlikte ortaya çıkan çok kutupluluğun ve küresel terörizmin yayılması gibi durumlardan sonra daha da önem kazanmıştır. Bununla beraber kişisel bilginin korunması eylemi de modern çağın getirdiği teknolojik gelişmelerle daha sorunlu ve zor hale gelmiştir. Bu teknolojik gelişmeler arasından özellikle telekomünikasyon alanında gerçekleşen gelişmeler bilginin ve kişisel bilginin işlenmesini, depolanmasını ve aktarılmasını kolaylaştırmıştır. Bundan dolayı kişisel bilgilerin korunmasında ve güvenliğinin sağlanmasında karşılaşılan sorunlar da aynı düzeyde artmaya başlamıştır. Bu sebeple

ikinci bölümde kişisel bilgilerin güvenlik ve korunma sorunsalı genel düzeyde çalışılmıştır.

Son bölümde ise Türkiye'de ve İrlanda'da kişisel bilgilerin korunmasına yönelik karşılaştırmalı bir analiz yapılmıştır. Her ne kadar bu bölüm başlığında kişisel bilgi kavramı ön planda görünüyor olsa da tüm dünyada olduğu gibi söz konusu bu iki ülkede de kişisel bilgilerin korunmasında temel olarak kişisel verilerin korunması kavramı ön planda tutulmaktadır. Bundan dolayı bu bölümde kişisel verilerin korunmasına yönelik yapılmış olan mevzuat ve bu mevzuatın gerekçeleri, verileri korumaya yönelik kurulmuş olan kurumlar ve işleyişleri incelenmiş ve analizleri yapılmıştır. Bu analiz kapsamında Türkiye'nin seçilmesindeki sebep, Türkiye'de teknoloji kullanımının yüksek seviyede olması ve bunun kişisel bilgi güvenliği ve korunması konusunda hassasiyet oluşturmasıdır. Türkiye ile birlikte İrlanda'nın seçilmesindeki sebep ise İrlanda'nın büyük teknoloji şirketlerinin Avrupa'daki merkezi olmasıdır. Son olarak da bu iki ülkede kişisel verilerin korunmasında göz önünde bulundurulması gereken yönler ele alınmıştır.

BİRİNCİ BÖLÜM

BİLGİ VE KİŞİSEL BİLGİ: TANIM, AŞAMALAR VE ÖZELLİKLER

Bilginin yaşadığımız çağa ve öncesindeki çağlara damga vuran bir etken olduğu yadsınamaz bir gerçektir. Fakat özellikle içinde bulunduğumuz çağda bilginin değerinin hiç olmadığı kadar artmasının yanı sıra bilgiye kolayca erişilmesi ve yaygın kullanımıyla birlikte bilgi gün geçtikçe değerini de kaybetmeye başlamıştır. Bu sebepten dolayı bu döneme "*bilgi çağı*" veya "*bilginin devrimi*" gibi isimlendirmeler verilmiştir ki bu durum bilginin son yüzyıla etkisinin daha iyi vurgulanması açısından oldukça önemlidir. Böylece insanlığın varoluşundan beri kendi önemini korumaya devam eden bilgiyi, kavramak ve bilgi ile ilgili hususları incelemek, insanlık tarihinin başlangıcından itibaren geçen süreçte ileriye yönelik gelişimini şekillendirmenin en önemli anahtarı olduğu düşüncesi hâkim olmaktadır. Bunlarla birlikte bilgi özellikle 19. yüzyılda ön plana çıkmış gibi gözükse de, aslında bilgi; dünün ve bugünün anahtarları iken, geleceğin şekillenmesinde de her zaman önemli roller üstlenmektedir (Canbek ve Sağıroğlu, 2006:165).

Bilgi, bireyin zihninden, inancından veya değerlerinden gelen ve rekabet avantajlarını geliştirmek için değer yaratan önemli bir organizasyonel varlıktır (Sokhanvar, Matthews, ve Yarlagadda, 2014). Bundan dolayı bilgiye verilen önemin mevcut durumda[2] olduğu gibi tarihin her döneminde de farklı olarak algılanmaktaydı. Nitekim bilginin tarihsel kronolojisinde bilginin tanımlanması Antik Yunan filozofları ile başladığı kabul edilmektedir. Bu sebeple bilgiye verilen değeri felsefenin alt dallarından birisi olan epistemoloji yani bilgi felsefesi tarafından yoğun bir şekilde tanımlanmaya çalışılmaktadır. Fakat bu düşünce teknolojik imkanların artması ve bilgi aktarımının kolaylaşması ile beraber bilginin ilişkili olduğu disiplinlerin sayısı her geçen gün çoğalmaktadır. Bu disiplinler bilgiyi kendileri ile ilişkisi çerçevesinde farklı şekillerde tanımlama girişimlerinde bulunmaktadır (İnce ve Oktay , 2006: 15-16).

[2] Mevcut durum ile bilginin merkezi olan her bilimsel alanda veya bilginin günlük hayattaki kullanımları vurgulanmaktadır.

Bunun yanı sıra bilginin, teknolojik gelişmeler ile birlikte özellikle bilgisayarın icadı ve veri depolamayı kolaylaştıran cihazların geliştirilmesinden sonra iç yapısında bir sınıflandırılmaya ihtiyaç duyulmuştur. Bu sınıflandırma bilginin ham maddesi olarak varsayılan veri (data) ile başlayarak enformasyon (information), bilgi (knowledge) ve bilginin insana veya bireye verdiği bilgelik(wisdom) özellikleri ile çeşitlenmekte ve sınıflara ayrılmaktadır (Yılmaz , 2009: 97-101).

Ayrıca bilginin özelliklerinin tanımlanması ve bilginin ayrı bir sınıflandırmaya tabi tutulmasıyla birlikte bilginin tanımlandırılmasında ve sınıflandırılmasındaki eksikliklerin de giderilmesine yönelik adımlar atılmaktadır. Bu bölümde bilginin tanımlanması sınıflandırılması özellikleri gibi konuları incelenmeye ve bu konu üzerindeki eksiklikler giderilmeye çalışılmaktadır.

1.1. Bilgi Kavramı

Yaşamın her alanında bilgiye olan ilgi ve ihtiyaç ilk çağlardan beri süregelen canlılığını her zaman canlılığını korumaktadır. İnsanı, doğduğu andan itibaren verilerle beslenen ve verileri elekten geçirerek bilgi üreten bir makine olarak tanımlanması ise bilgiye olan ilgi ve ihtiyacı daha da vurgulamaktadır. Bu sebepten ötürü insana "bilginin güç olduğu" ve refahın giriş kapısı olduğu bilinci ilk insandan beri varlığını sürdürmektedir. Böylece, sorgulayıcı zihinlere sahip olan insanlar bu yanıltıcı bilgi kavramını tanımlamaya, sınıflandırmaya ve ölçmeye çalışmışlardır (Geisler, 2008: 1). Bunun yanı sıra bilgi farklı şekillerde tanımlanmasına rağmen her dönemde önemi artarak devam etmiştir. Bu bağlamda bilgi kavramı filozoflar ve çeşitli disiplinlerden bilim insanları yüzyıllardır tanımlamaya, sınıflandırmaya veya anlamaya açık hale getirmek için çeşitli çalışmalar yapmıştır. Fakat bilgiye ait ortak bir tanıma ulaşmak mümkün olamamıştır. Çünkü bilgi, her zaman yenilenerek tanımını güncelleme ihtiyacı duymaktadır (Hoegl ve Schulze, 2005).

Bilginin tarihsel kökeni incelendiği zaman bilgi hakkında en temel tanımlamaların yapıldığı dönemin Antik Yunan dönemi olduğu görülmektedir. Bu dönemde filozoflar bilgiyi "Epistemoloji" çatısı altında felsefenin bir alt dalı olarak

incelenmiştir. Bilginin kavramsal olarak incelenmesiyle ilgilenen Epistemolojinin kelime anlamı ise, bilgi ile ilgili felsefe dalı olarak ifade edilmektedir. Temelleri iki Yunanca kelimedir: Episteme ve logos… Episteme, bilgi ve logos ise kuram/teori anlamına gelmektedir. Bu terimler tanımladıkları kavramlardan yanı sıra nitelikli bir tanıma da eşlik etmektedirler (Tennis , 2008: 103-104).

Nitekim epistemoloji, bilginin insana ait olduğunu yani bilginin insanın bir özelliği olduğunu ve bilginin çözümlenmesinin nasıl yapılacağının ancak insanlar tarafından bilinebilecek bir olgu olduğu da ifade etmektedir. Bu sebeple bilgi sahibi olan varlık "bilen" olarak adlandırılmaktadır. Bir bilen olduğuna göre, diyalektik düşünüşe göre bir de bilenin antitezi olan "bilinen" varlığın olması gerektiği de ifade edilmektedir. Böylece bilen, bilinen şeye yönelerek bilgiyi ortaya çıkarmaktadır. Bu sebeple bilgi felsefesinin en temel kavramları bu şekilde ifade edilmiştir (Çüçen, 2003: 3-4):

- Bilen
- Bilinen
- Bilgi

Epistemolojide bilen "özne" veya "süje" olarak adlandırılmaktayken bilinen ise "obje" veya "nesne" olarak adlandırılmaktadır. Özne olan bilen, bir şeye yönelerek o şeyi kendi bilgi nesnesi yaparak onun ya bir kısmı ya da tamamı hakkında bilgi sahibi olmaktadır (Uçak, 2000a: 144). Bu sebeple bilgi, bir sürecin sonunda oluşan ürüne verilen adı ifade etmektedir. Özne ve bilgi nesnesi veya bilen ve bilinen arasındaki ilişki sürecinde ortaya çıkan olguya bilgi denilmektedir. Bu yüzden bilme etkinliği özne (bilen) ve nesne (bilinen) arasında oluşan süreç olmaktadır. Böyle bir etkinliğin sonucunda çıkan ürüne de bilgi adı verilmektedir. Bu sebeple insan, bilgi üreten bir varlık olarak da tanımlanabilmektedir. Bunları temel alarak ulaşılan sonuca göre insan olmadan bilginin olması veya üretilmesi mümkün olmamaktadır (Orman, 2020).

İlk olarak Antik Yunan döneminde tanımlama girişimlerinin başladığı düşünülen bilginin tanımlanma süreci günümüze kadar aktif bir şekilde etkinliğini

sürdürmüştür. Bilgi 18. yüzyıla kadar etkin bir şekilde gücün kaynağı olarak görülmüş olsa da 18.yy.'da buharlı makinelerin icat edilmesiyle birlikte hızlı bir şekilde yeni bir sürece geçilmiştir. Bu dönemden itibaren bilginin insan yaşamına olan hızlı etkisi ve teknolojiye adapte oluşu ve devamında makinaların gelişmesiyle birlikte, bilgiye verilen önem her geçen gün güçlenerek artmaktadır (Maclellan ve Soden, 2007).

İkinci Dünya savaşı sırasında modern bilgisayarın icadı ve özellikle de 1951 yılında bilgisayarlarda manyetik teypler kullanılarak verileri kayıt altına alma özelliği kazandırılması ile birlikte ise bilgiyle beraber enformasyon ve veri kavramlarının da tanımlama tartışmaları ortaya çıkmaya başlamıştır. Bu dönemin başlaması ayrıca bilginin aktarımını ve kayıt altına alınması da teknolojinin seyrine göre kolaylaşmaya başlamaktadır. Ama bu kolaylaşmanın sonucunda bilginin aktarımında ve kayıt altına alınmasında bir ölçü olmaması, insan hayatını doğrudan etkileyerek kişilerin bilgisinin de güvensiz ve sınırsız olarak aktarılmaya başlamasına yol açan bir durum haline gelmiştir. Zamanla bilgi aktarımı hızlanmasıyla birlikte bilgilerin güvensiz bir şekilde depolanması sorunları da ortaya çıkmıştır. Hatta kişisel bilginin aktarımındaki güvenlik sorunları günümüzde dahi etkin bir şekilde devam etmektedir. Bunların yanı sıra bilginin ve kişisel bilginin tanımlaması, aşamaları ve özellikleri tanımsal olarak açıklanmaya ve sınıflandırılmaya çalışılmaktadır (Jahns, 2006).

Bilgi günlük yaşamda çok kullanılmasına rağmen tanımlaması zor bir kavramdır. Bilgi farklı disiplinler tarafından alanlarının özelliklerine göre farklı tanımlar ile ortaya konulmaktadır. Nitekim bilgi daha önce felsefenin ilgi ve tartışma alanında yer almaktayken, zamanla farklı bilimsel alanların ortaya çıkması ile birlikte tüm bilim dallarının konusu haline gelmiştir (Cansever, 2016).

Bununla birlikte bilgi kavramına tarih boyunca çeşitli tanımlar yapılmasına rağmen ortak bir tanımın oluşması her yeni dönem ile birlikte daha da zorlaşmaktadır. Bundan dolayı "Bilgi Nedir?" sorusuna kolay bir şekilde basit cevap vermek mümkün olmamaktadır. Bu soru son derece basit görünse de buna verilecek cevap kişilerin tanımlama sınırlılıklarına göre değiştiği için ortak bir tanım elde etmek zorlaşmaktadır.

Özellikle geçtiğimiz yüzyılda farklı disiplinlerin bilgiyi tanımlamaya çalışması, bilginin farklı tanımlarının daha da artmasına ve çeşitlenmesine yol açmıştır (Uçak, 2010b:707).

Ancak "Bilgi nedir?" sorusuna yanıt olarak birbirlerinden farklı olmalarına rağmen aynı zamanda da birbirlerini tamamlayan tanımla başlamak mümkündür. Bunlardan birincisi; bilginin yapılandırılma şeklini araştırır. Başka bir deyişle, bilgiyi üreten unsurları, bilgiyi oluşturan aşamalar ile veri ve bilgi arasında başka bir bileşen olup olmadığını araştırır. İkinci yol; bilginin dinamikleri ve ilerlemesinin doğasını incelemektir. Ayrıca "Bilgi nasıl ilerler?", "Bilgi nasıl birikir ve büyür?", "İlerlemeyi ve gelişmeyi sağlayacak ilkeler nelerdir?" gibi soruları da cevaplandırmaya çalışır. Üçüncü akış ise; bilginin bireylerin yaşamlarındaki kullanımını, bilginin toplumdaki yerini, ulus ekonomilerine ve sosyal ilişkilere katılımlarına nasıl uyguladıklarını incelemektedir. Bu durum, bilgiyi kullanma etiği ve bilginin insan faaliyetlerini test etme yollarına odaklanmaktadır. Nitekim bu insan faaliyetlerinin test etme yolları da aslında bilginin tanımlanmasının temel etkenlerinden biri haline gelmektedir. Bilgi edinme ve kullanma etiğine ve bu durumun insan eylemine bir araç olarak hizmet ettiği yönleri ve araçları da odak noktasında tutmaktadır (Geisler, 2008).

Bilginin tanımlanması birçok farklı disiplin tarafından yapıldığı için bilgi kavramı tanımlanırken farklı disiplinlerin tanımlamalarının incelenmesi bilginin anlaşılmasında etkili olmaktadır. Bu sebeple Türk Dil Kurumu(2019) tarafından yapılan bir tanımda "insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, malumat ve kavrayıştır" olarak tanımlanmaktadır. Bir başka tanıma göre, "bilgi; mantıklı bir yargı ya da deneysel bir sonuç sunan, başkalarına sistemli şekilde bir iletişim aracıyla ulaştırılan veya aktarılan, olgulara ya da düşüncelere ilişkin düzenli ifadeler dizisidir" denilmektedir (Turhan ve Okçu, 2018:30).

Bilgi kavramını felsefenin bir alt disiplini olan epistemoloji ile incelendiği zaman; bilginin öncelikle insana ait olduğu ifade edilmektedir. Bu sebeple "Bilgi, insan bilgisidir" denilmektedir. Böylece, epistemolojinin konusu olan bilgi insanın

kendi bilgisidir. Bu sebepten ötürü böyle bir bilgi de genellikle akılsal ve zihinsel bir etkinlik olarak anlaşılmaktadır. Bu çerçevede bakıldığı zaman; "Niçin sadece insan bilgisi ele alınmıştır" diye sorgulandığı görülmektedir ki buna yanıt olarak insan önce kendi bilgi yetilerini, imkânlarını ve koşullarını inceleme gereksinimi duymaktadır. Bu sebepten dolayı akıl sahibi insan, zihnin veya aklın gücünü kullanarak bilgi nesnesinin verilerini kavramsal hale getirerek bilgiyi elde etmektedir. İnsan kendine ait olan bilgiyi, bilginin nesnesi olan veriyi analiz ederek bilgiye ulaşabilmektedir. Bilgi insana ait bir özellik olduğu için yalnızca insanın bilmesi mümkün olmaktadır. Bu yüzden bilgi, özü itibari ile kişiye yani insana aitliği ile de kişiselleşmektedir (Çüçen, 2003: 3).

İnsan, kendi dışındaki varlıkları ve kendini tanımaya ve bilmeye çalışan tek varlık türü olarak bilgi nesneleriyle farklı tarzlarda ilişkilenmekte ve farklı bilgiler elde etmektedir. Çocukluğun ilk günlerinden itibaren bilme ve tanıma merakı içinde olan insanoğlu tarih sahnesine çıkmış ilk toplumlardan itibaren çeşitli türlerde bilgi ürettikleri tarih, sosyoloji ve antropoloji bilimlerini ortaya koymuştur. İradeli ve akıllı varlık olma vasıflarına sahip olarak diğer canlılardan üstün olmasını mümkün kılan insanın en büyük özelliği, nesnelerle çok çeşitli türden ilişkilere girerek, yalnızca tek tür bilgiye sahip olmak yerine farklı bilgiler üreten bir varlık olması insanın bilgiyle ilişkisini belirginleştirmektedir. İnsanlık tarihine bakıldığında, insanoğlunun nesneleri dinsel veya gündelik bilgi ile kavramaya çalıştığı görülmekteyken son yüzyıl insanınsa çoğunlukla nesnelere bilimsel açıdan yaklaştığı görülmektedir. Bu sebeple günümüzde insanoğlunun elde ettği bilgi bilimle ispatlanmadığı sürece toplumlar, bilim dışı yollarla elde edilen her bilgiyi ötekileştirme eğiliminde olmaktadır (Arslan, 2012:47-52).

Nitekim, öznenin nesneye yönelmesinde kullandığı yöntem veya ilişki türü, bilginin ne tür bilgi olduğunu da belirlemektedir. Bilgi, taşıdığı özelliğe ve elde ediliş yöntemlerine göre farklı türlere ayrılır: Gündelik bilgi, Dinsel bilgi, Teknik bilgi, Sanat bilgisi, Bilimsel Bilgi, Felsefî bilgi (Uçak, 2010b: 716-717).

Gündelik Bilgi; insanların günlük hayatta kullandıkları bilgilerdir. Kişinin bireysel algı ve çıkarımlarından elde ettiği ve bireylerin günlük hayatını kolaylaştırmaya yarayan genel veya özel bilgilerdir. Öznel(sübjektif) genellemelerin bir sonucudur. Deneme–yanılma, bilinçsiz gözlem ve genellemelerin birer ürünüdür. Örneğin, "gündelik yaşamda bir insanın herhangi bir meteorolojik bir bilgiye dayanmaksızın havanın bulutlu ve sıcak olmasından dolayı bir serzenişte bulunması gündelik bilgide yüzeysel bilgilere, duygusal ifadelere ve bireyin kendi kaygısına doğal olarak yer verildiğine işaret etmektedir(Çüçen, 2003: 4).

Dinsel Bilgi; din, her şeyi yarattığına ve yönettiğine inanılan doğaüstü bir varlığa inanmak demektir (Dawes ve Maclaurin, 2012: 3-4). Dinsel bilgi ise bu doğaüstü varlığın insanlara ilettiği mesajlar olarak tanımlanmaktadır. Kaynağı mutlak inanca dayanmak ile birlikte kayıtsız şartsız kabul edilmektedir. Değişmez, gelişmez ve eleştiriye kapalıdır. Bu sebeple dogmatiktir. Ayrıca ibadet şekilleri ile insanların yaşamını düzenler. Fakat bu dini düzenleme söz konusu dinin üyesi olan kişileri kapsamaktadır (Arslan , 2012: 335-339)

Teknik Bilgi; kendisine dayanılarak bir ürünün veya herhangi bir şeyin üretilebileceği bilgi türüdür. Bu bilgi türünde asıl amaç anlamak değil, üretim ve pratik yapmaktır. Bu durumu bir örnekle açıklamak gerekirse bir elbisenin nasıl dikileceğinin tarifi veya bir binanın nasıl inşa edilebileceğinin direktifleri olarak söylenebilmektedir(Engin, 2005: 438).

Sanat Bilgisi; bu bilgi türü de teknik bilgi gibi üretim faaliyeti olarak meydana gelmektedir. Fakat teknik bilgiden farkı yararlı araçlar üretmeyi değil, estetik ve güzellik üretmeyi ifade etmektedir. Ürünleri somuttur ve tektir. Bir yazarın kitabı, bir şairin şiiri veya bir ressamın tablosu bu bilgi türüne örnek olarak gösterilebilir. Sanatsal bilgi tek olması sebebiyle özneldir. Çünkü sanatçı nesneyi kendi bakış açısıyla şekillendirir. Bu bilgi türünde bilginin varlığı kişinin yeteneğine ve hayal gücünün genişliğine bağlıdır. Eserin son haline sanatçının manevi yönüne ve iç dünyasında neler beslediğinin bir yansıması denilebilmektedir (Young, 2001)

Bilimsel Bilgi; bilginin bu türünün tanımlanmasında birbirinden farklı nesnel özellikleri bulunmaktadır. Bu sebeple bilimsel yöntemlerle elde edilen ve doğruluğu bilimsel ölçütlerle gösterilebilen objektif bilgilerdir. Bilimsel Bilgi'ye nedenlerden oluşan bilgi de denilmektedir. Bu yöntem kullanılarak elde edilen bilgiler aynı koşullar altında aynı sonuçları verdiği için varsayım olarak bilim tarafından kabul edilmektedir. Bu nedenle kesin olarak da kabul edilmektedir. Yine bu bilgi türünde elde edilen bilgiler herkese göre kabul edilen yöntemlerle elde edildiği için nesneldir ve tüm dünyada kabul gördüğü için de evrenseldir. Elde edilen bilgiler olgulara dayanmaktadır. Her bilim dalı ele aldığı konuyla kendini sınırlamakta ve sonuç alabileceği konuları ele almaktadır. Bu sebeple bilimsel bilgi seçicidir. Aklın ve mantığın ilkelerine dayanmaktadır. Yani çelişkiden uzak, tutarlı düşünme kurallarına dayanır. Eleştiriye açıktır. Düzenli ve sistemlidir. Bilgilerin basitten karmaşığa ilişkilendirildiği ve mantıksal düzenliliğin bulunduğu bir yapıdır. Olayların gelecekte gerçekleşme şekilleri için önceden öngörüde bulunmaktadır. Bu bilgi türüne bir örnek vermek gerekirse her hava durumunun bir öngörü olduğu söylenebilir (Güçlü ve Kseanela, 2006: 355).

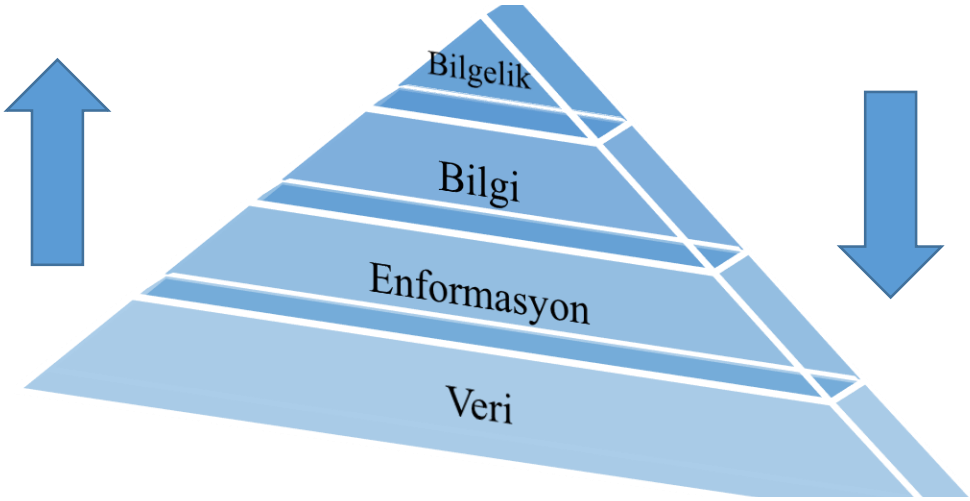
Felsefi Bilgi; sürekli ve kesintisiz bir araştırmaya ve eleştirmeye dayanan bir çabanın bilgisidir. Sürekli sorgular ve en doğruyu bulmaya çalışmaktadır. Genelleyici, birleştirici ve bütünleştirici bilgidir. Tam birleştirilmiş bilgidir. Örneğin; biyoloji canlı varlıkları, psikoloji canlı varlıkların davranışlarını (insan ve hayvan davranışlarını), fizik fiziksel olayları vb. incelerken; felsefe "bir bütün olarak varlığı" konu edinmektedir. Felsefi bilgi evrenseldir fakat kesin değildir. Çünkü her zaman eski bilgiyi de kullanarak yeni çözüm yolları bulmayı amaçlamaktadır. Akla dayanan yani bir araştırma ve soruşturmanın sonucudur. Çelişkisiz, tutarlı ve mantıklı bilgidir (Uçak, 2010b: 709).

1.1.1. Bilginin Aşamaları

Bilginin tanımlanması Klasik Antik Yunan döneminden beri sürekli bir tartışma konusu olmasına rağmen son dönemde teknolojik gelişmelerin etkisi ile özellikle İkinci Dünya savaşı sonrasında bilgisayarın da icat edilmesi ile birlikte ortaya

çıkan veri (data), bilginin tanımlanmasında aşamaların oluşmasını sağlamaktadır. Fakat verinin ortaya çıkması ve tanımlanması ile bilginin tanımlanmasında ve anlaşılmasında yeni teoriler ortaya çıkarmaktadır. Bu teorilerin artmasına rağmen bilginin tanımlanmasında ortak bir tanıma da ulaşılamamaktadır (Cansever, 2016: 44-45).

Şekil 1.1. DIKW Hiyerarşisi



Kaynak: Rowley, 2007.

Nitekim son yüzyıl ile birlikte ortaya çıkmış olan bilginin aşamalandırılması ve bu aşamaların arasındaki sınırları belirleme çalışmaları kazanması bilginin daha iyi anlaşılmasının yolunu açmaktadır. Bunların yanı sıra bu bilgi aşamalarının birbirleri arasındaki ilişkiyi ve geçişleri sağlayan bir terimin daha etkisi ve önemi anlaşılmaya başlamaktadır. Bu terim "Understanding" yani bu terimin kavrama ya da anlama olarak Türkçe' ye çevirisi yapılmaktadır. Bu terim bilginin bir aşaması değil veriden bilgiye oradan da bilgeliğe ulaşmadaki en önemli etkendir. Başka bir açıdan bakılacak olursa; "Understanding", bilginin sadece insana ait olabileceğinin de bir kanıtı niteliğindedir. Bir veriyi bir insan olmadan enformasyona çevirmek veya bir veri elde edilmesi imkânsız hale gelmektedir (Hey, 2004: 2-5)

Bilgiyi tanımlamak için ilk önce bu aşamaları kavramak ve analiz etmek gerekmektedir. Yani, veri, enformasyon, bilgi ve bilgelik aşamaları ayrı ayrı ele

alınmadan bilgiye bir bütün olarak bakıp bilgeliğe ulaşılamamaktadır. Literatürde bu aşamalar bilgiyi daha belirgin tanımlamak için kullanılmaktadır. Bu çalışmada da bilginin daha iyi anlaşılması için bu aşamalar ele alınmaktadır. Bu aşamalar ise,

Veri, bir bağlamda bazı farklılıklar veya tekdüzelik eksikliği ile ilgili varsayılan bir gerçektir. Örneğin; herhangi birisi eline aldığı boş bir beyaz kâğıdın üzerine kalemle bir işaret bırakırsa, beyaz kâğıdın boş olma özelliği kaybolmaktadır. Yani beyaz kâğıdın tek düzeliği kaybolmakta ve üzerinde karşıt bir şey oluşmaktadır. Yukarıdaki veri tanımı bize bu tekdüzelik eksikliğinin aslında veri dediğimiz şey olduğunu söylemektedir. Burada, verilerin yalnızca siyah çizgi olmadığını, verileri oluşturan bir fark veya karşıtlık yaratanın beyaz bir kâğıt üzerindeki siyah çizgi olduğunu anlamak çok önemli olmaktadır. Bu perspektiften bakıldığında, veriler, beyaz ve siyah vuruşların fizikselliğinin üzerinde duran, fiziksel olmayan bir "model" karakterini edinmektedir. Fiziksel olmamanın bu özelliği, bilginin mutlaka maddi bir düzenlemeyi gerektirmediğini savunan yorumlara yol açmaktadır. Bu ilginç bir görüş olsa da, bu bölümde daha fazla ilerlenmek istenmeyen bir nokta haline gelmektedir (Schumaker, 2011: 39).

Buna alternatif olarak, Floridi'nin (2014: 17-18) tekdüzelik eksikliği açısından üç görüşünü birbirinden ayırdığından bahsedilmektedir. İlk olarak, gerçek dünyada tekdüzelik eksikliği mevcuttur. Bu algıladığımız dünyanın boş olmadığı anlamına gelmektedir. Dünyamız tekdüze olarak hiçbir şeyden yapılmamıştır. Çünkü dünyamızda nesneler var olmaktadır. İkincisi, bir sistemin durumları (ör. Tam dolu bir pil) veya sinyaller (ör. nokta ve mors alfabesinde bir satır). Üçüncüsü, veriler iki sembol arasında tekdüzelikten yoksun olabilmektedir (örneğin, alfabedeki "B" ve "P" harfleri arasındaki fark). Bu üç görüş birlikte bilgi üretimine izin verilmektedir. Örneğin; dizüstü bilgisayarlarda(nesne) bir metin yazmak istediğinizi varsayalım. Dizüstü bilgisayarların pilinin(nesnesinin) boş olmaması durumunda (durum), başlangıçta dizüstü bilgisayardaki ekran boş bir sayfa (tekdüzelik) gösterebilmektedir. Yazmaya başladığında, ekranda karakterler(semboller) belirmektedir (tekdüzelik eksikliği, dolayısıyla veriler). Bu süreçte üretilen metnin anlamlı olduğunu varsayarak

bir adım daha ileri gidersek, aşağıdaki tanıma göre bilgi (anlamsal içerik olarak anlaşılmaktadır) üretilmektedir (Dubois ve Gershon, 1996).

Başka bir yönden, daha basit bir dil ile tanımlamak gerekirse; verileri, sayılar olarak tanımlanabilmektedir. Yani sayısal büyüklükler veya oranların gözlem, deney veya hesaplamadan türetilen özellikler de denilebilmektedir (Bergeron, 2003: 9). Diğer bir deyişle amaçlara bağlı olarak işlemlerin işlenmemiş bir şekilde kayıt altına alınması denilebilmektedir. Veri, özümlenmemiş ve yorumlanmamış gözlemler; işlenmemiş gerçekler olarak tanımlanabilmektedir. Modern anlamda veri, teknolojik sistemlerde saklanmakta; çoğu zaman bir anlam veya içerik ifade etmemektedir. Tüm örgütler veriye ihtiyaç duymaktadır. Bununla birlikte her örgütün enformasyon üretmesi için ihtiyacı olan veri miktarını ve türünü belirlemesi gerekmektedir (Güçlü ve Kseanela, 2006: 353)

Kısaca bilginin ham maddesi veridir. Sadece var olur ve varlığının ötesinde (kendi başına) hiçbir önemi yoktur. Kullanılabilir olsun olmasın herhangi bir biçimde olabilmektedir. Kendisinin işlenmediği sürece tek başına bir anlamı bulunmamaktadır.

Enformasyon, belirli bir nesne, olay veya süreçle ilgili verilerin ve ilgili açıklamaların, yorumların ve diğer materyallerin bir koleksiyonudur (Bergeron, 2003: 10). Başka bir deyişle verilerin anlam taşıyacak şekilde işlem gördükten sonraki haline denilmektedir (Çapar, 2006: 2). Ham verinin ilişkilendirilmesi, sınıflandırılması, hesaplanması, düzeltilmesi ve yoğunlaştırılmasıyla anlaşılmaya, iletilmeye ve kullanılmaya hazır hale getirilmesine denilmektedir. Enformasyon işlenmemiş verilere anlam kazandırılarak oluşturulmaktadır (Turhan ve Okçu, 2018: 28).

Enformasyonun yalnızca ve ancak aşağıdaki durumlarda anlamsal içerik olarak anlaşılan bir bilgi örneğidir (Hey, 2004):

- bir veya daha fazla veriden olmaktadır;
- içindeki veriler iyi biçimlendirilmektedir;
- iyi biçimlendirilmiş veriler anlam kazanmaktadır.

Özet olarak, yukarıdaki enformasyon, bilgilerin verilerden oluştuğu anlamına gelmektedir (örneğin, dizüstü bilgisayar ekranındaki karakterler verilerdir). Veriler, bazı kurallara veya prosedürlere göre iyi biçimlendirilmelidir. Örneğin; dizüstü bilgisayar ekranında resmi bir kuruma yazılan dilekçede veya yazıda "Sayın İlgili, Gereğini bilgilerinize arz ederim" gibi cümlelerden resmi bir mektup/dilekçe olduğu anlanabilmektedir. Bu sebeple bu tarz yazıların iyi biçimlendirilmiş veriler olduğu söylenebilmektedir (Floridi, 2011).

Bilgi, anlamayı, farkındalığı veya anlayışı geliştirmek için organize edilen, sentezlenen veya özetlenen enformasyondur. (Headriok, 2006: 13). Bilgi "veri" ile başlayıp, işlenerek "enformasyona" dönüşmesi ile devam eden sürecinin en kapsamlı ve uç noktası yani İngilizce'deki "knowledge" anlamındaki kullanımını ifade etmektedir. "Knowledge" anlamında kullanılan bilgi, enformasyonun tecrübe, duygu, algı, sezgi, toplumsal değerler, kültür, yetenek, karakter, gibi bireysel özellikler ile işlenerek hayatı kolaylaştıran forma dönüştürülmüş hali denilmektedir (Medeni ve Aktaş, 2019: 2). Ayrıca İngilizce' deki "knowledge" kelimesine karşılık gelen bir kavram üretilmediği için bilgi genellikle enformasyon ile karıştırılmaktadır (Uçak, 2000a: 147).

Bilgelik, bilginin disiplinler arası transferine olanak sağlayacak şekilde derinliğine ve hâkimiyetine sahip olma durumudur (Turhan ve Okçu, 2018: 29). Bilgelik 2000'li yıllar ile birlikte tanımlanmaya başlanmıştır. Veriden bilgiye geçen süreçte insanın veri, enformasyon ve bilgiyi yöneterek kavradığı ve özümsediği durum ile birlikte bu aşamaya ulaşması olarak adlandırılmaktadır. Fakat eğer insan bilgiyi özümseyip kavrama yeteneğini kullanmazsa bilgelik oluşması mümkün olmamaktadır (Satija, 2015: 72).

1.1.2. Bilginin Özellikleri

Bilgi sözcüğü iki anlamda kullanılmaktadır: Birinci anlamı, bir konuyla ilgili bilgi ve fikir sahibi olmak, konuyu anlamaktır; ikinci anlamı ise fikirleri ve durumları

gösteren belgeler ve verilerdir (Canlıoğlu, 2008). Genel itibariyle bilginin altı belirgin özelliği bulunmaktadır (Ünal, 2009: 126):

- Niceliği: Bilginin ölçülebilir sayısal özelliğidir.
- İçeriği: Bilginin anlamıdır.
- Yapısal Özelliği: Bilginin hangi formatla ve nasıl bir düzen içinde ifade edildiğidir.
- Dil: Simgeler, alfabeler, kodlar biçiminde ifade edilerek anlatımıdır.
- Niteliği: Bilginin bütünlüğü, doğruluğu, zaman karşısında dayanaklılığıdır.
- Süreci: Bilginin değerini kaybetmeden geçerliliğini koruma sürecidir.

1.1.3. Bilginin Sınıflandırılması

Bu noktaya kadar bilginin ne olduğunu ve bilginin hangi aşamalardan oluştuğu incelenmektedir. Bilgiyi insana atfederek bilginin insan olmadan var olamayacağı vurgulanmaktadır. Nitekim bu başlık altında bilginin literatürde farklı şekillerde sınıflandırılması yapılmaktadır. Ancak bu çalışma açısından bilginin en yaygın olarak kullanılan çeşitleri ele alınmaktadır. Bilginin kullanım amacına göre anlam kazanmasında bilginin ne tür bilgi olduğunu öncelikle belirlenmesi gerekmektedir (Durna ve Demirel , 2008: 141). Bilginin ne olduğunun ve neye yaradığını daha iyi anlamak için aşağıdaki kıstaslara göre sınıflandırılarak tanımlanması ve açıklanması yararlı olmaktadır (Güçlü ve Kseanela, 2006: 254).

1.1.3.1.Açık ve Örtük Bilgi

Örtük bilgi, 20. yüzyılın ikinci yarısından sonra özellikle gündeme getirilmeye başlanmış ve hakkında düzenlemeler yapılmaya halen devam etmektedir. Araştırmacılar tüm bilgimizi bir buz dağı ile simgeleştirerek, buz dağının %90'ının örtük bilgi olarak denizin dibinde ve görünmez halde olduğunu, ancak %10'unun denizin üzerinde ve açıkta, açık bilgi şeklinde bulunduğunu dile getirmektedirler. Bu belirlemeden sonra, başlangıçta ifade edilen, "örtük bilgi açıkça kendi anlamına bürünmüştür" ifadesi daha bir açıklık kazanmaktadır (Günay, 2019).

Açık bilgi, bilenin sözlü bir ifade aracılığıyla açıklayabileceği bilgidir: "Bir kimse, eğer bir ifade ondan uygun sorgulama veya yönlendirmeyle elde edilebiliyorsa, bir şey hakkında açık bilgiye sahiptir" (Atılgan, 2009). Örtük bilgi, açık olmayan bilgi olarak tanımlanabilmektedir. Bu bağlamda, örtük bilgi kabaca Polanyi'nin (1966) "zımni bilme" dediği şeye karşılık gelmektedir: "Söyleyebileceğimizden daha fazlasını bilebiliriz" (Kirsh, 2009: 397-398)

Açık ve örtük bilgi arasındaki ayrım, bir önermenin bilgisi "bunu bilmek" ile bir beceri "nasıl yapılacağını bilmek", günlük “bunu bilme” durumlarında kurşunun atomik sayısının olduğunu bilmek gibi, bilen kişi bildiklerini söyleyebilmektedir. Aksine, performansın nasıl elde edildiğine dair herhangi bir sözlü açıklama yapamamakla birlikte, bir beceriye “birinin ayakkabı bağını bağlama yeteneği” gibi sahip olması açıkça mümkün olmaktadır (Fayganoğlu, 2019: 1070)

Örtük bilgi, çoğunlukla kişisel deneyime, öngörüye dayanmaktadır. Açık olarak ifade edilmeyen veya ima olarak ifade edilen, anlaşılan, belli bir anlam çıkarılan bilgi denilmektedir. Açık bilgiden kesin olarak ayrılan yönü bütün anlamlarının ifade edilmesi ima veya önerilerle olmasıdır (Durna ve Demirel , 2008: 142). Açık bilgi ise, kitap, doküman, rapor, kısa not ve eğitim kurslarında düzenlenen bilgi denilmektedir. Açık bilgi, örtülü bilgiye göre daha hızlı iletilebilmekte ve düzenlenebilmektedir. Çünkü açık bilgi direkt olarak tecrübeden elde edilen bir bilgidir. Bu bilgi, kelime, rakam, sesli veri, bilimsel formül, kayıt veya ürün şeklinde ifade edilebilmektedir; kişilere formal ve sistematik olarak iletilebilmektedir (Güçlü ve Kseanela, 2006: 355).

Michael Polanyi (1966)’e göre örtük bilgi açık bilgiyle zıttır. Fakat bu ikisi kesin olarak birbirinden ayrı değildir. Örtük bilgi kendi kendisine ait olabilirken; açık bilgi, örtük olarak anlaşılan ve uygulanan bilgi üzerine oturmak zorundadır. Dolayısıyla, bütün bilgimiz ya örtük bilgidir ya da kökü örtük bilgidedir. Bütünüyle açık bilgiden söz edilememektedir.

“Örtülü Bilgi” teknolojinin kullanımı ile “Açık Bilgi ”ye dönüşebilmekte ve bunun yapılması sağlanmaktadır. Çünkü deneyimlerin iş süreçlerine yansıması

kalitenin artmasını sağlamaktadır (Dampney, Busch ve Richards, 2019). Örnek vermek gerekirse, "Türkiye'nin başkenti Ankara" şeklinde ifade edilebilen bilgi açık bilgi sınıfına girmekteyken, bir müzik aleti çalmak, bir dili konuşmak gibi bilgi ve beceriler örtük bilgi kapsamına girmektedir.

1.1.3.2.Sığ ve Derin Bilgi

Sığ veya yüzeysel bilgi, problem alanının en asgari anlaşıldığının göstergesi sayılmaktadır. Derin bilgi ise, tecrübe ile kazanılan ve zor kararlarda ve problemlerin çözümünde kullanılan bilgi denilmektedir (Güçlü ve Kseanela, 2006: 354).

Yüzeysel bilgi, bilginin yanı sıra ne, ne zaman, nerede ve kim sorularına cevap vermektedir. Ayrıca, öncelikle açık ve minimum anlayış gerektiren görünür seçimleri temsil etmektedir. Nitekim, tipik olarak çok az eylem gerekli olmaktadır. Daha çok alıcı tarafından ne olduğuna dair bir farkındalıktır (Bennet ve Bennet, 2008: 4).

Bilgi şeklindeki yüzey bilgisi; kitaplarda, bilgisayarlarda ve ya akılda saklanabilmektedir. Hafif sohbetler, açıklamalar ve hatta kendini yansıtma gibi günlük hayatımızın çoğu, yüzey bilgiyi oluşturan yüzeysel düşünme ve öğrenme şekli olarak düşünülebilmektedir. Örneğin; Ulusal Araştırma Konseyi, ABD eğitim sisteminin öğrencilere fen bilimini bir mil genişliğinde ve inç derinliğinde bir yaklaşım kullanarak öğrettiği konusundaki endişesini dile getirdi. Vurgu, yüzeysel öğrenmedir, yani öncelikle kısa süreli ezbere dayanan gerçekleri, verileri, kavramları ve bilgileri, sınavları ve sınavları geçmek için sıkıştıran derin öğrenme gerekliliği bireyin kişisel anlayışını yaratmasını ve bunun tekrarlanmasını istemektedir. İskoçya, Kanada ve Avustralya'da öğrencilerin öğrenmesinin yüzde 90'ının yüzeysel öğrenme olduğunu keşfettiler ve bu rakamın Birleşik Devletler'dekine benzer olduğunu tespit ettiler. Bu gelecekteki birçok yetişkinin derin öğrenme gerektiren sorunları ele almaya hazır olmayabileceğini göstermektedir. Dahası, yüzey bilgisinin hatırlanması genellikle zordur ve unutulması kolaydır. Çünkü hatırlamayı iyileştirici ve kolaylaştırcı çok az anlamı ve etkeni bulunmaktadır. Ayrıca diğer saklanan anılarla çok az bağlantısı bulunmaktadır (Karp ve Wilkins, 1989).

Sığ bilgi, bilginin yanı sıra biraz anlayış, anlam ve anlam üretmeye sahip olunulan zamandır. Anlamak, tipik olarak bir birey veya kuruluşla ilgili olan ve belirli bir eylem düzeyini ima eden bir düzeyde anlam oluşturmaktır. Anlam üretmek için bağlam gerekmektedir. Örneğin; Can'ın arabası bir telefon direğine çarptı" ifadesi açıklayıcıdır. Can'ı bilmiyorsanız, minimum anlamı vardır (yüzey bilgisi). Öte yandan, eğer Can arabanızı kullanıyorsa bunun sizin için daha derin bir anlamı bulunmaktadır. Bu anlam sizin tarafınızdan eklenmektedir. Çünkü bu ifadenin bağlamı sizin için özel bir öneme sahiptir. Anlam, bireyin alınan bilgilerden ve kendi iç bilgilerinden yarattığı bir şeydir. Bu nedenle yüzey bilgisi, bilgi yapıcının mantıklı bir şekilde bilginin bütünlüğünü belirleyebilmesi için bir anlayış ve anlam gerektirmektedir. Bu anlam mantık, analiz, gözlem, yansıtma ve hatta bir dereceye kadar tahmin yoluyla oluşturulabilmektedir. Örneği kullanarak, bunun sizin arabanız olduğunu biliyorsanız, formları doldurmanız, arabayı tamir ettirmeniz vb. işlemler yapmak zorunda kalacağınızı tahmin edebilmektesiniz. Bu durumda ne olduğunu bütünleştirerek, tutarlı veya tutarsız olduğunu kendi kendinize kurgulayarak anlamlandırırsınız. Böylece tutarlı anlam oluşturma sürecinde anlam ve anlayış kazandıran bilgi üretilmektedir (Bennet ve Bennet, 2008: 4).

1.1.3.3.Teknik ve Uygulanabilir Bilgi

Teknik bilgi, daha sistemli ve daha dar alanlara yönelik donanımsal bir bilgi türüdür. İnsanların dünyada hâkimiyet alanları oluşturabilmek için kullandıkları ve teknolojik üretime dönüştürülebilecek olan bir bilgi çeşididir. Marksist düşünürlere göre teknik bilginin sınırları ifade edilenden daha geniştir ve üretici güçlerin varlıklarını ve faaliyetlerini sürdürebilmeleri için gerekli olan çok önemli bir bilgidir. Fakat bu bilgi türünü sadece teknoloji ile ele almak noksan olabilmektedir. Bu sebeple doğayı, insanı ve toplumu anlayarak onlara egemen olup; onları yönetmek için gereken bütün üretici, yıkıcı, koruyucu, yönetici ve planlayıcı çareler ve etkinlikler kapsamına alınmaktadır (Engin, 2005: 438).

Bilginin uygulanabilirliği ise teknik sınırlara uygun ve faaliyete geçirilebilmesi mümkün olan bilgi çeşididir. Kısaca teknik ve uygulanabilir bilgi pratik tecrübeden kazanılmış derslerden oluşmaktadır. Nitekim uzmanlık bilgisine ulaşmak için gerekli bilgi türüdür (Güçlü ve Kseanela, 2006: 354).

1.1.3.4.Ortak Anlayış Olarak Bilgi

Ortak anlayış; birden fazla insanın ortak bir amaç için fikir birliği yapmalarına denilmektedir. Bu sebeple bir topluluk meydana gelmektedir. Yani bu gruptaki insanların ortak bir hedef için sözlü ve/veya yazılı olarak birlik olunmasıyla ortak anlayış kurulmuş olmaktadır. Ortak anlayış beş unsurdan meydana gelmektedir. Bunlar (Jaatinen ve Lavikka, 2008: 151);

- Ortak düşünme yöntemleri;
- Ortak çalışma yöntemleri;
- Ortak bilgi;
- Ortak hedefler;
- Güven;

Ortak anlayış olarak bilgi ise, insanların farklı biçimlerde ve seviyelerde sahip oldukları bilgidir. Bunun yanında kazandıkları tecrübe ve olgulardan oluşan ve insanların kabullenmek için edindikleri bilgi türüdür(Awad ve Ghaziri, 2004: 44).

1.2. Kişisel Bilgi Kavramı

Kişisel bilgi kavramını anlamak için ilk olarak "kişi", "kişisel" ve "kişilik" kavramlarının kökenlerinin incelenmesi gerekmektedir. Bu sebeple "kişi", "kişisel" ve "kişilik" kavramları etimolojik açıdan ele alındığında kelimenin İngilizcedeki karşılığının "personality", Fransızcadaki karşılığının "personalite", Almancadaki karşılığının "personlichkeit", Orta Çağ Latincesindeki karşılığının "personalitas", Klasik Latincedeki karşılığının ise "persona" kelimeleri ile ifade edildiği görülmektedir. Etimolojik kökeni bu şekilde gelişen kişilik kavramının Latince kökeni olan "persona" kelimesi, Klasik Roma Tiyatrosunda sahne ile seyirciler arasındaki

uzaklığın fazla olması nedeniyle oyuncuların temsil ettikleri rolleri daha net ifade edebilmek için yüz mimiklerine uygun biçimde hazırlanmış yüze takılan maske anlamına gelmektedir (Tekin vd., 2012: 4612).

Kişisel bilgi kavramını anlamak için ikinci olarak bilginin ve/veya bilmek eyleminin etimolojik kökeninin de incelenmesi gerekmektedir. Bununla birlikte birçok dilde "bilmek" fiili iki adet birinci şahıs fiiline sahip olmaktadır. Bunlar "biliyorum" ve "biliyoruz "dur. "Biliyorum" demek bir bireyin kendine ait bilgisi yani kişisel bilgisi denilmektedir. "Biliyoruz" demek ise bilgiyi ifade etmektedir (International Baccalaureate Organization, 2020). Nitekim "bilmek" eylemi insana aittir. Bu sebeple bilgi de sadece insana ait bir olgudur (Tan ve Crawford, 2006).

Herhangi bir bireyin sahip olduğu kimlik kartı detayları, beğeniler ve/veya beğenmediği şeyler, özel hayatı hakkındaki detaylar, karakter özellikleri vb. bilgilere kişisel bilgi denilmektedir. Çoğunlukla gözlem veya kişisel deneyimler yoluyla birikmektedir. Pozitivist düşünürlerin iddiasına göre kişi bilgisinin öznel bileşeninin tamamen dış dünyanın doğrudan gözlemine dayanarak ortadan kaldırılabileceği ya da en azından azaltılabileceği anlayışı hâkim olmaktaydı. Fakat bilginin kaçınılmaz olarak kişisel bilgiye ait olduğu savunulmaktadır (Hammond, 2019: 25).

1.2.1. Kişisel Bilginin Aşamaları

İnsan var olduğun günden bu yana durmaksızın bilgi üretmiş ve üretmeye devam etmektedir. Ayrıca bilgiyi kendini ispatlamadaki en güçlü anahtar olarak görmüştür. Bu sebeple her dönemde bilginin güç olduğu söyleyen veya bu düşünceyi sık sık pekiştiren kişiler hep var olmaktadır. Bilginin güç olduğu ve hatta bilginin yok edici bir güç de olduğu 18. yüzyıl sanayi devrimi ile anlaşılmaya başlanmıştır. Nitekim bilginin ikinci en büyük yükselişi olan İkinci Dünya Savaşı sonrasında bilgisayarın icadı ile bilgi ayrıca kendi içinde bölümlere ayrılarak veri kavramını oluşturmuştur. Bilim insanları bilgiyi bu son döneminden sonra üç ayrı bölümde tanımlayarak anlaşılmasının kolaylaştırmaya çalışmışlardır. Bu sebeple bilgiyi, veri, enformasyon ve bilgi olarak ayrı ayrı tanımlamaktadırlar (Scardamalia ve Bereiter, 2010).

Kişisel Veri, tanımlanmış veya tanımlanabilir yaşamakta olan veya ölmüş bir bireye ilişkin herhangi bir bilgidir. Birlikte toplanan farklı bilgi parçaları, belirli bir kişinin tanımlanmasına yol açabilmektedir. Ayrıca kişisel verileri oluşturmaktadır (European, 2001). Başka bir ifade ile kimliği belirli veya belirlenebilir, gerçek kişiye ilişkin her türlü bilgi anlamına gelmektedir. Bu yüzden sadece gerçek kişilere ait kişisel verilerin korunması esas olduğu iddia edilmektedir. Bu bilgilerden kastedilen sadece ad, soyad veya doğum yeri gibi bilgiler değil aynı zamanda pasaport numarasından parmak izine, genetik bilgilerden motorlu taşıt plakasına kadar kişiyi belirlenebilir hale getirebilmesinden dolayı kişisel veri sayılmaktadır (Miilard ve Hon, 2011).

Kişisel veriler tanımlanmamış, şifrelenmiş veya taklit edilmiş ancak bir kişiyi yeniden tanımlamak için kullanılabilen verilerdir. Kişisel verilere; bir isim ve soy isim, ev adresi, kişiye ait e-posta adresi, kimlik kartı numarası, telefonunuzun reklam tanıtıcısı, bir hastane veya doktor tarafından tutulan ve bir kişiyi özel olarak tanımlayan bir sembol olabilecek veriler örnek olabilmektedir. Kişisel veri olarak kabul edilmeyen verilere bir şirket sicil numarası, şirket e-maili veya anonim veriler örnek olabilmektedir (Hammond, 2019).

Kişisel Enformasyon, kişisel verilerin sistematik şekilde işlenerek kişiler hakkında oluşturulan kişisel algoritmadır. Örneğin; bir kişinin sosyal medya hesaplarındaki beğenilerin, paylaşımların veya izlediği herhangi bir videonun içeriklerinin veri tabanlarında kayıt altına alınarak ve bunlardan elde edilen sistematik şemalara göre kişiye elektronik ortamda ilgi alanına göre reklam gösterilmesi kişinin verilerinin işlenerek kişisel enformasyonunun oluşturulmasını ifade etmektedir (Madden, 2000: 346-347).

Kişisel Bilgi ise, kişiye ait ham verinin kayıt edilmesi ile başlayıp, sistematik olarak işlenerek enformasyona dönüştürülmesi ile devam eden sürecinin en üst seviyesidir. Burada kişinin veri veya enformasyon halindeki verilerinin tecrübe, duygu, algı, sezgi, kişinin bulunduğu dinsel ve toplumsal değerler, kültür, yetenek ve

karakter ve hayal dünyası gibi bireysel özellikleri ile harmanlanarak kişinin başka bir kişinin hakkında oluşturduğu veya kişinin kendisi hakkında oluşturduğu bilgiye denir. Yani kişisel verinin evrimleşmesiyle detaylı bir analiz yapılması sonucunda oluşturulan taslağa kişisel bilgi denir. Bu bilgi türü sadece bir bireyin kendisi veya diğer bir bireyin hakkındaki bilgi çeşididir. Bu kişisel bilgiyi, bilgiden ayıran en önemli özellik bir bireyin hakkında veya onun üretiminden çıkmış olmasıdır. Kişileri doğrudan ruhsal, fiziksel, karakteristik vb. özellikleriyle tanımlamada kullanılır (Uğraş, 2015: 23-25).

Nitekim kişisel veri olmadan kişisel bilginin oluşamayacağı iddiasının sanat ve edebiyat alanlarında istisnası bulunmaktadır. Dolayısıyla kişilerin/bireylerin belirli bir zaman diliminde özellikle bir konu üzerinde veya özel bir amaca yönelmeksizin edebi ya da sanatsal bir çalışma veya eser meydana getirmesi de kişisel bilgiye örnek olarak verilebilir. Bu sebeple bir ressama ait resimler, bir heykeltıraşa ait heykeller, bir yazara veya şaire ait hikâyeler/romanlar, bir mucide ait bilimsel buluşlar/icatlar hatta kişilerin çocukken oyun oynadığı oyuncaklar ve çizmiş oldukları resimler kişisel bilgiye örnek olarak gösterilebilir. Bunlar aracılığıyla söz konusu kişilerin psikolojik durum analizi, kişilerin karakteristik tanımlaması ve kim olduklarının çözümlemesinin yapılması mümkündür. Ayrıca bu eserlerin, buluşların meydana gelmesinde belirli bir gözlem, öğrenme ve kavrama etkinliklerinin kişiler tarafından gerçekleşmesi gerekir. Bundan sonra ise bu kazanımları kişilerin hayal dünyası, kültürel kazanımları, inanç biçimi vb. etkenler yoluyla belirli bir öğütme aşamasından geçirerek bu bilgileri somutlaştırmaktadır (Özsağır, 2008).

Fakat özellikle belirtmek gerekirse kişisel bilginin bu örneklere rağmen tamamen sınırlarını belirlemek mümkün olmamaktadır. Her ne kadar bireyler çeşitli yollarla sahip oldukları bilgileri somutlaştırmaya çalışmış olsalar da sahip oldukları bilgelikten gelen bilgiyi tam anlamıyla göstermeleri mümkün olmamaktadır. Buna sahip olduğumuz dil becerisinin düşüncelerimizi yansıtmakta yetersiz olması örnek gösterilebilmektedir.

1.2.2. Kişisel Bilginin Özellikleri

Kişisel bilginin temelinde bilgi de olduğu gibi insan vardır. İnsan olmadan kişisel bilgi oluşmaz. Kişisel bilginin de ana etkeni insandır. Bir kişinin verileri yoksa bilgisi de oluşturulamaz. Bir kişi yoksa bilgi de oluşmaz. Kişisel bilgiyi bilgiden ayıran temel özellik kişisel bilginin sadece kişi/birey hakkında olan ya da doğrudan kişinin hayat tecrübesi ile hayal dünyasının süzgecinden geçirmesi sonucu oluşan bilgidir. Diğer bir deyişle insanın sahip olduğu her bilgi kişisel bilgi değildir. Kişisel bilgi söz konusu bireyleri doğrudan tanımlayan, onların hayat tarzlarını, beğenilerini, karakter özelliklerini vb. ilgili bilgileri kişisel bilgi olarak adlandırabilir (Engin, 2005).

-Kişiye/insana aittir,

-Kişileri tanımlamada kullanılır,

- Kişisel veri yoksa da kişisel bilgi oluşabilir,

-Tamamen ifade edilmesi mümkün değildir.

Bir bilginin kişisel bilgi olarak adlandırılması için kişileri doğrudan tanımlamaya yardımcı olacak kişisel verilere (ad, soyad, doğum tarihi vb.) her zaman ihtiyaç yoktur. Bazı anonim nitelikteki sanatsal eserlerden yola çıkılarak kişiler tanımlanabilir. Bu tür durumlarda kişilerin doğrudan ve tamamen tanımlanması mümkün olmasa da ortaya çıkmış bilginin kişisel bilgi olduğu gerçeğini değiştirmemektedir.

1.2.3. Kişisel Bilginin Korunmasının Önemi ve Nedenleri

Bilgi ve İletişim Teknolojileri'nin gelişmesi ve internete erişimin artmasıyla, kuruluşlar çeşitli tehdit türlerine karşı savunmasız hale gelmektedir. Veriler, siber saldırılara ve sonuç olarak ortaya çıkan zararlara maruz kalmaktadırlar. Bu saldırılar ve tehditler, çalışanların yaptığı etkinlikler veya bilgisayar korsanlarının saldırıları gibi farklı kaynaklardan gelebilmektedir. Güvenlik ihlallerinin neden olduğu finansal kayıplar genellikle tam olarak tespit edilememektedir. Çünkü küçük ölçekli güvenlik olaylarından önemli sayıda kayıp yaşanabilmektedir. Bunun sonucunda ise bilgi

sistemi güvenlik riskinin olduğundan daha az tahmin edilmesine neden olmaktadır. Bu nedenle yöneticilerin, uygun karşı önlemleri belirleyerek ihtimal dahilindeki saldırıları önlemek için ne yapmaları gerektiğine karar vermeleri için varlıklarını etkileyen tehditleri bilmeleri ve etkilerini belirlemeleri gerekmektedir (Jouini ve Aisa, 2014: 492).

Kişiler, özellikle bilgilerinin işleme amaçları hakkında bilgilendirilmedikleri zaman, kişisel bilgilerin tam olarak kullanılmasıyla ilgili olası risklerin genellikle farkında olamamaktadırlar. İletişim sistemlerinin değişmesi nedeniyle, insanlar e-posta gibi birçok farklı mesajlaşma uygulamalarına kadar birçok kaynağı kullanmaktadırlar. Ne yazık ki, insanlar çoğu zaman güvenlik risklerini umursamamaktadırlar. Çünkü herhangi bir şekilde iletişim kurmak nihai hedeflerine yani insanın sosyal bir varlık olmasından dolayı kaynaklanan iletişim ihtiyacını karşılamaya çalışmasından kaynaklanmaktadır. Bununla birlikte internetin insan hayatına etkisi yani kişilerin diğer insanlarla uzaktan bile etkileşime girebilme avantajı başarılı olmaktadır. Fakat kişilerin kendi kişisel bilgisinin korunmasında eksikliklerinin fazlaca olmasına da yol açmaktadır (Bergeron, 2003).

Yani diğer bir yönüyle coğrafi uzaklıktan bağımsız olarak insanlar arasında tartışma ve bilgi paylaşımını desteklemek için farklı sosyal medya araçları oluşturulmaktadır. Bilgi güvenliği açısından bakıldığında, bu tür araçlar, bilgi alışverişi kanalları, yani farklı iletişim türlerinin gerçekleştiği alanlar olmanın yanı sıra bilgi ve veri havuzlarıdır. Bilgiye bağlı riskleri tanımlamanın ve yönetmenin sistematik bir yolu ile birleşik bir bilgi koruma düzeyi oluşturmaya yardımcı olabilmektedir. Ancak bunun en azından kuruluşlarda yaygın olarak bulunmadığını veya iyi yönetiminin sağlamadığı için faydasının yanısıra bazı dönemlerde kişiler üzerinde ciddi zararlara da yol açabilmektedir. (Ilvonen, Jussila, Kärkkäinen ve Päivärinta, 2015: 3943).

Kişisel bilginin korunması insan huzurunu, güvenini, yaşam standartlarını ve genel olarak toplumsal düzenin sağlanmasında önemli bir etken olduğu apaçık bir

gerçektir. Bundan dolayı kişisel bilgilerin korunması eylemini insan hakları arasına dahil edilmesi mümkün hale gelmektedir. Nitekim insan hakları tüm insanların hiçbir ayrım gözetmeksizin sadece insan oldukları için eşit, özgür ve onurlu yaşama hakkına sahip olması olarak tanımlanmaktadır. Bu sebeple her bir insanın kendisine ait kişisel bilgilerinin korunması esas haline gelmektedir. Özellikle insan haklarının temel şartlarından olan mahremiyet hakkının kişisel bilginin korunmasında önemli bir konumu bulunmaktadır (Tan ve Crawford, 2006).

Kişisel bilginin bir şemsiye kavram olarak ele alınması ve diğer aşamaların yani kişisel veri ve kişisel enformasyonun bu kavram altında ele alınması kişisel bilginin anlaşılmasında önem arz etmektedir. Nitekim daha önce kişisel bilgi tanımlanırken belirtildiği gibi kişisel bilgi insanın anlama ve kavrama süzgecinden geçerek hayal dünyasında şekillenmeye başlayan bilgidir. Bu yüzden resimleri, heykelleri, roman ve hikaye vb. kişilere ait eserleri ve icatların da bir çeşit kişisel bilgi kabul edildiği için korunması gerektiği de inkar edilemez bir gerçektir. Bu sebeple sadece kişisel verilerin korunması gerektiğinin ifade edilmesi yanlış olmaktadır. Örneğin; bu çalışmada belirtilen kişisel bilgilerin(sanatsal ve edebi eserler gibi) örnek etmenlerin tüm dünyada telif hakları çerçevesinde korunması esas alınmaktadır (Young, 2001).

Son dönemde hız kazanmış sosyal medya mecralarında paylaşılmış bir sözün, fotoğrafın, video kaydının, yazının dahi telif hakları çerçevesinde koruma altında olmuş olması bu tür kişisel bilginin nasıl korunduğuna örnek olarak gösterilmesini mümkün kılmaktadır (Töre, 2007).

1.2.4. Kişisel Bilginin Korunmasında Erdem, Etik, Mahremiyet ve Güvenlik

Erdem, etik, mahremiyet ve güvenlik gibi kavramlar kişisel verilerin korunması konusunda birbirlerine sıkı bir şekilde bağlıdırlar. Mahremiyetin sağlanması ve güvenlik hükümleri temelde güvene dayanmaktadır. Örneğin; kişiler yalnızca güvendiği kişilerin erişilemezlik özelliği olan alanına girmesine izin verir. Bu

sebeple güvenlik sağlayıcısına güvenmedikçe kendini güvende hissetmemektedirler. Mahremiyetin ihlal edilmesi bir risk oluşturur ve dolayısıyla güvenlik için bir tehdit meydana gelmektedir. Etik, hırsızlığın yanlış olduğunu bilmektedir. Erdem ise hırsızlığın yanlış olduğunu bilmekle beraber bu yanlışa kişinin yaklaşması dahilinde kötü şeyler olacağını psikolojik olarak adapte etmeye çalışmaktadır. Güvenlikle ise bu süreçler emniyet altına alınmaktadır (Lee, Zankl ve Chang, 2016: 1).

Gizlilik olarak da bilinen veri koruma, (gizli veya hassas) verilerin etik kurallarla erdemli bir şekilde korunmasına değil, kişilerin kişisel verilerinin kötüye kullanılmasına karşı korunmasıyla ilgilidir. Örneğin, yeni bir ürünün tasarımı, onu geliştiren şirketin bakış açısından son derece gizli olabilmektedir. Ancak genel olarak veri koruma kapsamında olmamaktadır. Nitekim bilgi korunmasından söz edildiği zaman aynı zamanda erdem, etik, mahremiyet ve güvenlik kavramlarının da kişisel bilginin korunmasındaki etkisinin belirtilmesi gerekmektedir (Kneuper, 2019: 1). Bu sebeple bu dört kavramın kavramsal analizleri ve kişisel bilgiyle olan ilişkisinin incelenmesi de gerekmektedir.

1.2.4.1.Erdem

Beş bin yıl önce, eski Mısırlılar tarafından "Maat" olarak bilinen bir kavram geliştirilmiştir. Adalet, hukuk, düzen, hakikat, ahlak ve dengeyi içeren "Maat", kaosun, adaletsizliğin ve sahtekârlığın tam tersi anlamına gelmekteydi (Küçüktaşdemir, 2016: 102). Birçok yönden bu kavram, bugün erdem olarak adlandırdığımız şeye benzemektedir. Erdem çoğu zaman dini bir kavram gibi değerlendirilmesinin yanı sıra kendine ait bir yapısı bulunmaktadır. Yani yüksek ahlaki standartlarla ilişkili bir dizi karakter özelliğini tanımlamaktadır (Froom, 1994).

Erdemli olmak ise, bir kişinin ahlaki mükemmelliğini yansıtan bir davranış türüdür. Bu kelime, toplumun ahlaki açıdan iyi olduğunu düşündüğü herhangi bir nitelik veya karakter özelliğine atıfta bulunabilmektedir. Dürüstlük, sadakat, cesaret ve nezaket evrensel olarak olumlu özellikler olarak görülmektedir. Bu kavramların her

biri aynı zamanda bir erdem olarak tanımlanabileceği anlamına gelmektedir. Başka bir deyişle erdem, "*kazanılan insan nitelikleri, kişinin iyi yaşama ulaşmasını sağlayan karakterin mükemmellikleridir*". Bu normatif etik dalı, eski Yunan felsefesine, özellikle de insan varoluşunun amacını mükemmellik veya erdem arayışı olarak gören Platon ve Aristoteles'in öğretilerine dayanmaktadır. Bu sürekli karakter mükemmelliği çabası, tüm insanlar tarafından mutlulukla tanımlanan "iyi bir toplumda" yaşayabilmeleri için gerekli bir faaliyet olarak görülmektedir (Arıkan, 2018).

Erdem terimi ilk olarak 13. yüzyılda İngilizceye girdi. İnsanların hayranlık uyandıran niteliklerini tanımlamak için kullanıldığı Antik Roma'da yüzyıllar önce icat edilmişti. Bunlar sadece ahlaki davranışlarını değil, aynı zamanda güçlerini ve fiziksel özelliklerini de içermekteydi. Aslında erdem kelimesinin kökü, Antik Roma'da insan için kullanılan "er" kelimesinden gelmektedir (Bejczy ve Newhauser, 2005).

Musevilik, Hıristiyanlık, İslam ve diğer dinler, erdemli bir kişinin Tanrı'nın sözüne itaat etmesi gerektiğini öğretmektedir. Felsefe, erdeme sahip olmanın hem kendine hem de başkalarına faydalı olacak şekilde hareket etmek anlamına geldiğini öğretmektedir. İster dini ister seküler olsun, tüm erdem tanımları, erdemli bir kişinin iyi bir ahlaki karaktere ve doğru ile yanlış arasındaki farkı söyleme yeteneğine sahip olduğu konusunda hemfikir olduğu düşünülmektedir. Erdemler tekrar yoluyla geliştirilmektedir. Erdemli olmayı günlük yaşamda uygulayarak, erdemler yavaş yavaş alışkanlıklara dönüştürülebilmektedir (McDowell, 1979).

Bunların yanı sıra kişisel verilerin korunmasında yapılan hukuksal düzenlemeler ne kadar ciddi olursa olsun insanın kendisin de olması gereken erdem duygusu veya davranışları yetersiz ise yapılmış olan hukuksal düzenlemeler işlevsiz kalmaktadır. Bu sebeple erdemin gerekliliği olan davranış şekillerini kişisel verilerin güvenliğinin sağlanmasında da uygulamak önceliklerden olması gerekmektedir. Çünkü insanlara sadece kurallarla bir düzeni kabullendirmek her zaman yetersiz olmaktadır. Fakat olması gereken davranış biçiminin erdem çatısı altında toplanması bireyin psikolojik olarak da kişisel verinin mahremiyetinin korunması gerektiğini

aşılamaktadır. Bu işlev ise insanların gelişiminde ve eğitiminde en etkili faktör olan aile tarafından sağlanabilmektedir. Bu sebeple kişisel veri mahremiyetinin önemi ilk olarak ailesel eğitimin içinde yer alması gerekmektedir (Froom, 1994).

Başka bir ifadeyle Farabi'nin El-Medinetü'l Fazıla (2001: 80) adlı eserinde de belirttiği gibi "*bütün şehirler saadete erişmek için toplumsal olarak elele vererek çalışmasıyla fazıl bir millet olabilir; bütün milletlerin saadete ulaşmak maksadıyla elbirliğiyle çalışması ile dünya da fazıl bir dünya olur*". Bu sebeple kişisel verilerin korunması için gerekli olan erdemi toplumların davranış biçimine adapte edilmediği sürece yapılan her düzenleme işlevini zamanla kaybetmektedir.

1.2.4.2.Etik

Etik olarak da adlandırılan ahlaki felsefe, ahlaken iyi ve/veya kötü ve ahlaki olarak doğru ve yanlış olan ile ilgilenmektedir. Bu terimi aynı zamanda bir sisteme ya da bireyin davranışlarına da uygulamak mümkündür (Bejczy ve Newhauser, 2005).

Etik üzerine odaklanan felsefi araştırma dalı, insanların yaşaması gereken tutarlı bir kurallar veya ilkeler kümesi üzerinde çalışmak ve/veya bunları oluşturmakla ilgilenmektedir. Etiğin teorik çalışması, normalde birçok insanın günlük faaliyetlerini yürütmek için gerekli gördüğü bir şey değildir. Sistematik olarak incelenen etik çerçevelerin yerine, çoğu insan davranışlarını etkileyen ve yöneten yararlı bir dizi günlük pratik kurallar taşırlar; genellikle bunlar "çalmak yanlıştır", "muhtaç insanlara yardım etmek doğrudur" gibi kuralları içermektedir (Feldman, 1978: 1-15).

Etik kelimesi Yunanca ahlak anlamına gelen "ethicos"tan gelmektedir. Bir disiplin olarak etik, neyin iyi neyin kötü olduğunun belirlenmesi ile ilgili ahlaki görev ve sorumlulukları belirtmektedir. Etik; ahlaki davranış, eylem ve yargıları ilgilendiren bir konu olarak felsefe ve bilimin önemli bir parçası olmaktadır. Ahlak yanlış-doğru, iyi-kötü, erdem ve kusur ile davranışları ve davranışların sonuçlarını değerlendirmeyle ilgilidir (MacIntyre, 1998: 1). Birçok yerde etik sözcüğü yerine ahlâk sözcüğünün

kullanıldığını ve bazı batı dillerinde aynı şekilde geçtiğini görülebilmektedir (Kesgin, 2009: 145).

Ancak bazen hayatın değişimleri ve karmaşıklıkları, basit etik kuralların bazen teste tabi tutulduğu anlamına gelmektedir. Öldürmenin yanlış olduğu fikri düşünülürse; idam cezasının yanlış olduğu anlamına mı geliyor? Hayvanları öldürmek yanlış mı? Kendini savunma yani meşr-u müdafaa yapmak, öldürmek yanlış mı? Hamileliğin sonlandırılması yanlış mı? Ötenazi yanlış mı? Günlük doğru ve yanlış kavramlarımızı bu sorulara uygulamaya çalışırsak, her zaman açık cevaplar verilememektedir. Bu soruların daha detaylı incelenmesi gerekmekte ve karmaşık sorunları analiz etmemize ve bu sorunlara akılcı, tutarlı çözümler bulmamıza yardımcı olabilecek teorik çerçevelere ihtiyaç duyulmaktadır. Bazı insanlar bu işi bireysel olarak yapmaya çalışırken, filozoflar toplumda herkes tarafından kullanılabilecek genel cevaplar bulmaya çalışmaktadırlar. Fakat mevcut etik kurallara yeni eklenmiş olan kişisel verilerin nasıl korunması gerektiğini tartışmak ve fikir üretmek yetersiz kalmaktadır. Her ne kadar söz konusu temel etik kurallar üzerinde filozoflar tarafından çözümler üretilmeye ve önemleri vurgulanmaya çalışılmış olsa da günümüzün temel sorunlarından olan kişisel verilerin korunması gerekliliği hakkında henüz net bir çözüm yolu üretilememektedir. Böylece doğru koruma alanı sağlanamamaktadır (Tripodi, 2019).

Etik, neyin doğru neyin yanlış olduğunu öğrenmeyi ve sonra doğru olanı yapmayı gerektirmektedir. Bu sebeple etiği "Davranış Bilimi" olarak görebiliriz. Etik, hayatta yaşanılan temel kuralları içermektedir. Sokrates ve Platon gibi filozoflar tarafından etik davranış için kanun, düzenleme veya kural gibi kılavuzlar verildi. Bu nedenle kanunlara, düzenlemelere veya kurallara uymak etiğin temel erdemlerinden olduğu söylenmektedir. Nasıl davranmamız gerektiğini yönlendiren ahlaki değerler denilebilmektedir. Örneğin; saygı, dürüstlük, adalet, sorumluluk vb. değerlerin nasıl uygulandığına dair ifadeler bazen ahlaki veya etik ilkeler olarak adlandırılmaktadır (Rich, https://samples.jbpub.com: 4-5).

Nitekim kişisel verilerin korunması etik bir davranıştır. Bireylerin mahremiyetle ilgili haklarını ve onlar hakkındaki bilgilerin kullanılmasını içermektedir. Bu durumun etik davranışlardan olduğunu topluma kabul ettirerek kişisel verilerin korunmasını erdemli davranışlardan birisi haline getirmek istenmektedir. Yani küresel düzeyde veri korumanın önemini vurgulayan fon sağlayıcıları yani kişisel verilerin korunmasının önemini belirten aktörler özellikle Avrupa Birliği (AB), veri koruma ve etik açısından artan düzeyde güvence aramaktadırlar. Kişisel veriyi etik davranış yoluyla koruyarak olası tehlikelerin engellenebilmesine yardımcı olması beklenmektedir (Fabiano, 2019).

1.2.4.3.Mahremiyet

İlk olarak mahremiyeti tanımlamadan önce mahremiyet kavramı ile birbirine bağlı olan özel hayatın ne olduğunun tanımlanması gerekmektedir. Bu sebeple özel hayatı bireylerin özgür olarak kişiliğini oluşturabildiği ve geliştirebildiği, hem diğer insanlarla hem de dış dünya ile ilişkili bir alanı kapsayan, mahremiyetten daha geniş bir kavram olduğu ifade edilmektedir. Bu hayat kişinin kendisi tarafından dış dünyaya karşı gösterilmemektedir. Bu yüzden kişiye özgüdür. Özel hayatın içeriği, dokunulmazlığı, ulaşılmazlık özellikleri kendisinde mevcut olmalıdır. Diğer bir ifade ile özel hayat kavramında iki temel boyut bulunmaktadır. Bunlardan ilki bireyin kendini ifade ettiği, diğeri ise bireylerle paylaşmak istediği boyuttur. Kişi bu ortak alanında kendi hayatıyla ilgili olayları başkalarının bilmesinde sakınca duymamaktadır. Bu alan mahremiyet kavramının içine giren, bilgilerin gizli kalmasını ve erişimin mümkün olmamasını istediği özel ve gizli alan kavramları burada karşımıza çıkmaktadır. Kişi özel alanında yaşadıklarını, sadece paylaşmak istediği kişilere anlatmaktadır. Gizli alanında ise sadece kendisinin bildiği ve bu olayların sadece kendisinde saklı kalmasını istediği olaylar yer almaktadır (Moor, 1990).

Mahremiyet yapısı gereği iki alt başlık altında ele alınmaktadır. Bunlar bedensel mahremiyet ve kişisel bilgi mahremiyeti olarak adlandırılmaktadırlar. Bedensel mahremiyet, kişinin yaşarken veya öldükten sonra bedeninin mahremiyet

kuralları gereğince korunmasını ifade etmektedir. Kişisel bilgi mahremiyeti ise kişilere ait her türlü bilginin açık rıza olmaksızın kullanılamamasını ifade etmektedir. Bu çalışmayı ilgilendiren mahremiyet ise kişisel bilgi mahremiyetidir. Bu sebeple mahremiyet kavramı kişisel bilgi mahremiyeti altında değerlendirilmektedir (Eroğlu, 2018).

Mahremiyet kelimesinin kökü "mahrem", Arapça "haram" kelimesinden gelmektedir. Haram; "*Yasaklamak, men etmek, mahrum etmek, mümkün olmamak, el sürmemek*" gibi anlamlar içermektedir. Mahremiyet ise "*gizlilik, bir şeyin (mahrem) gizli hali, bir şeyin gizli yönü*" demektir. İngilizcede ise kavram, 'privacy' ve 'confidentiality', 'intimacy' gibi sözcüklerle ifade edilmektedir. Bu İngilizce kelimeler kullanım amacına göre birbirinin yerine kullanılmaktadır (Avaner, 2018: 111).

Mahremiyet, ilk insandan başlayarak bugüne kadar uzun bir gelişim ve değişim içinde bulunmaktadır. Fakat özel olarak nitelendirilmesi gerekirse çağa, topluma ve kişiye göre farklılık göstermektedir. Ayrıca neyin özel olduğu ve neyin özel olarak yasalarla korunduğu veya korunması gerektiği konusu farklı olabilmektedir. Yazılı medyadaki hızlı büyümeyle birlikte tecrit için bireysel haklar tehdit altına girmiştir. 1850'den 1900'e kadar, dolaşımdaki gazete sayısı sadece ABD'de 10 kat artışla 8 milyonun üzerine çıkarak 100'den 950'ye çıkmıştır. "Paparazziler" terimi günlük konuşmaların bir parçası olmayabilmektedir. Ancak bir kutu kamera olan Kodak Brownie, üst sınıf seçkinlerin özel hayatlarına tıklayan çok sayıda foto-muhabir meydana getirmiştir. Bireylerin mahremiyet haklarıyla çelişse bile gerçeğin zenginlerin ve seçkinlerin aşırılıklarını ifşa etme zorunluluğu olduğunu hissettikleri söylenmektedir. Bu hikâyeler, hızla büyüyen okuyucunun zengin ve ünlülere olan ilgisini ve hayal kırıklığını beslemiştir (Sharma, 2020: 24). Bu yüzden çok önemli bir ilk adım olarak 1890'da Louis Brandeis ve Samuel Warren isimli iki avukat tarafından yazılan ünlü çalışmada (Mahremiyet Hakkı) ortaya çıkan modern mahremiyet kavramının oluşturulması olarak ele alınmaktadır. Bu makalede yazarlar mahremiyet hakkını "yalnız olma hakkı"(the right to be alone) olarak adlandırmaktadırlar. O

zamandan beri, mahremiyet hakkı yaygın olarak bilinen ve kabul edilen toplumsal olarak temel insan haklarından birisi olmaktadır (Lukács, 2016: 256).

Mahremiyet yalnızca 19. ve 20. yüzyılda genel bir erişim hakkı haline gelmesine rağmen, mahremiyet bu çağlardan çok önce de var olmuştur. Mahremiyetin çok uzun bir tarihi bulunmaktadır; kökenleri eski toplumlara dayanmaktadır. Hukuki açıdan, Hammurabi Yasası, birinin evine izinsiz girilmesine karşı bir madde içermekteydi veya Roma hukuku da aynı şekilde mahremiyeti güvence altına almaktaydı. Hatta yakın tarihte Osmanlı kent mimarisine[3] bakıldığında hiçbir evin avlusu diğer bir ev tarafından görülmemekteydi. Kısaca bu örneklerle birlikte tarihte de mahremiyetin ne derece önemli olduğu anlaşılabilmektedir. Aslında mahremiyet fikri geleneksel olarak "özel" ve "kamusal" arasındaki farktan gelmektedir. Bu ayrım, bireyin kendisi ile dış dünya arasında bir ayrım yapma ihtiyacının insanlık kadar eski olan bir doğal ihtiyaç olduğu anlamına da gelmektedir. Elbette özel ve kamusal arasındaki sınırlar dönem ve topluma göre değişmektedir. Bu durum da tarih boyunca insanların özel olarak gördüklerinin değişmesine neden olmaktadır (Yüksel, 2003).

İlk çağlarda mahremiyet özel ve kamusalın genel bir ayrımını ifade ederken teknoloji çağı ile birlikte bu durum değişerek özel ve kamusal ayrımını daha detaylı olarak yapmaktadır. Diğer bir ifade ile kişinin mahremiyet sınırları ona ait olan özel veya kamusal bilgilerinin korunması gerektiğini hatta söz konusu kişiyi tanımlayabilecek veya onun kim olduğunu belirlenebilir hale getirebilecek her türlü açık veya örtülü veri ve bilginin de mahremiyet alanında olduğu ifade edilerek güvence altına alınmaya başlanmaktadır (Avaner, 2018).

Mahremiyet çoğunlukla bilginin kontrolü açısından tanımlanır. Mahremiyet, başkalarının kafasında sadece belirli bir kişiyle ilgili bilginin yokluğu değil, kişinin kendisi hakkındaki bilgi üzerinde sahip olduğu kontroldür. Mahremiyetin, bireylerin ve grupların kendileri hakkındaki bilgilerin başkalarına ne zaman, nasıl ve ne ölçüde

[3]Osmanlı mimarisinde evlerin avlusu olan "hayat" kısmı dışa kapalı olup, yarı kapalı ve açık yaşam alanıdır. Diğer evlerin iç avluyu görmeleri mümkün değildir (Özkeçeci, Durukan ve Alacalı, 2018: 216).

iletileceğini kendileri için belirledikleri iddia olduğu söylenmektedir. Başka bir ifade ile kişilerin kendileri hakkında ne zaman ve ne kadar bilginin başkalarına açıklanacağına karar verme hakkına sahip olduğunu öne sürmektedir (Moor, 1990: 74). Kavram üzerindeki bu sürekli değişim birçok tanımı meydana getirmesi net bir tanım oluşumunu etkilemektedir. Bununla birlikte kavramın tanımlanması, sınırlarının belirlenmesi güçleşmektedir. Bu sınırların belirlenmesini kolaylaştırmak için mahremiyet yaklaşımının üç boyutta ele alınarak tanımlanması yapılmaktadır. Bunlar (Kokolakis, 2017):

- Bölgesel mahremiyet; bir insanı çevreleyen fiziksel alanla ilgili gizlilik.

- Kişi mahremiyeti; bir bireyin fiziksel varlığına karşı gereksiz müdahaleyi temsil etmektedir (örneğin; fiziksel arama).

- Bilgi mahremiyeti (gizliliği); kişisel verilerin toplanması, depolanması veya nasıl işlenebileceğinin ve dağıtılabileceğinin kontrol edilmesi ile ilgilidir.

Mahremiyet ile ilgili tanımlar birçok bağlamda farklılık göstermesine rağmen, hukukta ortak ve yaygın mahremiyet tanımları bedensel, bölgesel, bilgi ve iletişim gizlilikleri üzerine yoğunlaşmaktadır. Mahremiyet kavram olarak ele alındığı zaman, kişilerin yalnız kalabildikleri, düşünebildikleri, davranabildikleri, diğer bireylerle hangi sınırlarda ilişki ve iletişim kuracaklarına kendilerinin karar verdiği bir alanı ifade etmektedir (Yüksel, 2003). Bu bağlamda mahremiyet hakkı da bireylerin kendi hayat alanlarını diğerleri ile ne ölçüde paylaşacaklarını belirleme hakkı olarak düşünülebilmektedir (Bennett, 2009).

Güncel teknolojik gelişmelerle ele alınması gereken ise, mevcut düzenlemeler potansiyel gizlilik sorunlarını göstermekte yeterli olmadıkları görülmektedir. Özellikle tüm vücut görüntüleme tarayıcıları, barkod özellikli seyahat belgeleri, insansız hava araçları, ikinci nesil DNA sıralama teknolojileri, insan geliştirme teknolojileri ve ikinci nesil biometri gibi teknolojiler, geliştirilmesi gereken ek gizlilik politikaları ortaya çıkarmaktadır. Bu yeni ve gelişen teknolojilerle beraber kişinin mahremiyeti, davranış

ve eylemlerin mahremiyeti, kişisel iletişim mahremiyeti, veri ve görüntü mahremiyeti, düşünce ve duyguların mahremiyeti, konum, alan ve grup mahremiyeti dâhil olmak üzere birçok farklı mahremiyet türü ele alınarak genişletilebilmektedir. Bu mahremiyet türlerinden bazıları birbirini kapsamasına rağmen mahremiyeti daha belirgin ve net tanımlanması için ayrı ayrı sınıflandırarak ele alınması mahremiyetin tanımlanmasında daha etkili olmaktadır (Akça ve Başer, 2011).

Nitekim hukuk sistemlerinin mahremiyetin korunmasının sağlanması gerçeğine rağmen, tam olarak ne/nelerin korunması gerektiği hakkında fikir birliği bulunmamaktadır: Tam olarak ne korunmalıdır, mahremiyet nedir? Birkaç büyük hukukçu, bir mahremiyet tanımı yaratma girişiminde bulunmuştur. Ancak bu tanımların kavranamaması, bireyin özel alanına ait unsurların süregiden değişmesi nedeniyle, tanımların çoğu mahremiyetin sadece bir yönünü vurgulamaktadır. Hukukçu William Prosser (1960) ise, mahremiyet davalarını dört farklı ancak ilgili haksız fiil olarak derecelendirmektedir. Bunlar:

İzinsiz giriş: Bir başkasının mahremiyetine oldukça saldırgan bir şekilde (fiziksel veya başka türlü) izinsiz girmek. Örneğin, hastanede nadir görülen bir hastalığı olan bir kadın, bir muhabirin fotoğraf ve röportaj talebini reddediyor. Fakat muhabir itiraz olmasına rağmen yine de fotoğrafını çekiyor. Bu sebeple izinsiz şekilde mahrem alan aşılmış olmaktadır (Eroğlu, 2018).

Özel durumlar: Kamuoyunu meşru olarak ilgilendirmeyen biri hakkında oldukça özel bilgilerin duyurulması olarak ifade edilmektedir. Bir otel odasında eşini başka birisi ile aldatan bir şirket yöneticisinin fotoğraflarının bir dergide yayınlanması örnek gösterilebilir (Gruschka, Mavroeidis ve Vishi, 2018).

Yanlış ışık: Bir kişinin oldukça saldırgan ve yanlış izlenimini kamuya duyurmak için yanlış bir bilgilendirme yapmak olarak tanımlanmaktadır. Örneğin; halkı, kötü niyetli taksi şoförlerine karşı bilgilendirmek için yapılan bir gazete haberinde olayla ilgisi olmayan bir taksi şoförünün resmini kullanarak yanlış

bilgilendirmeye ve kişi hakkında yanlış algıya yol açmaktadır (Solove ve Richards, 2010: 1890).

Sahiplenme: Başkasının rızası olmadan başkasının adını veya benzerliğini bir avantaj için kullanmak olarak tanımlanmaktadır. Örneğin; ünlü bir yazarın fotoğrafının, rızası olmadan bir ürünün reklamını yapmak için kullanılmasına denilebilir (Al-Khouri, 2012).

İnternet çevrimiçi bankacılık veya çevrimiçi alışveriş gibi hizmetleri anonim olarak taramak veya kullanmak isteyen oldukça fazla kişiyi çevrimiçi kullanıcı haline getirmektedir. Bununla birlikte, bir birey olarak mahremiyetleri de tehlikededir. Çünkü birçok bilgi onların bilgisi veya rızası olmadan toplanabilmektedir. Toplanan bilgilerin çoğu, çerezler, ziyaret edilen Web sitelerindeki günlükler veya genellikle e-postalar, yasal olarak indirilmiş virüslü dosyalar aracılığıyla elde edilen virüslerin, casus yazılımların ve Truva atı denilen elektronik ortam virüslerinin sessizce yüklenmesi yoluyla gizlice yapılmaktadır. Kişisel bilgiler karşılığında tüketicilere tasarruf veya kolaylık sunarak, toptan veya perakende mağazalar, bankalar, devlet daireleri veya çevrimiçi hizmetleri olan herhangi bir işletme gibi kuruluşlar, bireyler hakkında çok fazla bilgi toplayabilmektedirler. Bu süreçler; müşterilerin yalnız bırakılma ve tanımlanmama haklarını ortadan kaldırdığı, gözetimden uzak olduğu ve paylaştıkları bilgilerin kontrolüne sahip oldukları için mahremiyeti ihlal etmektedir. Ayrıca, müşteriler kendileri hakkında neyin toplandığını, ne kadar süreyle saklanacağını, toplama amaçlarını ve üçüncü şahıslarla paylaşılıp paylaşılmayacağını bilmediğinde mahremiyet ihlal edilmektedir (Ménard, 2006: 116).

Kişisel verilerin doğal insan haklarından olan mahremiyet çerçevesinde korunması hukuk sistemlerinin temel odak noktalarından biri haline gelmektedir. Bu durum her ne kadar son yıllarda küresel sisteme sert bir etkisi olan Covid-19 hastalığı sebebiyle birçok defa göz ardı edilmektedir. Hatta bu süreçle birlikte internet üzerinden canlı derslerin yapılması veya ofis ortamında yapılan işlerin ev ortamında da yapılmaya başlanmasıyla kişiler teknolojinin getirdiği yeniliklere daha aktif dâhil

olmak zorunda kalmaktadırlar. Bu süreçte yaşanan aksaklıklar, bilinçsiz veri paylaşımları ve kişisel veri paylaşımının getireceği zararlara karşı bireylerin bilgisiz olması mahremiyet sınırlarının zarara uğrama oranını artırmaktadır (Akça ve Başer, 2011).

Söz konusu sağlık krizi yayıldıkça, birçok ülkede ulus içi ve uluslararası seyahatlerin yasaklanması gibi önlemlere başvurulmuştur. Özel kuruluşlar, devlet önlemlerine uymak ve işgücünü korumak için daha fazla kontrol uygulayarak kendi planlarını oluşturmaktadır. Bunun genel uygulaması, bireyleri profesyonel ve özel seyahat planları hakkında sorgulamak, sıcaklık kontrolleri yapmak ve işyeri dışındaki enfekte kişilerle olası temas bilgileriyle birlikte sağlık kayıtlarını tutmak gibi istilacı gizlilik önlemlerini gerektirmektedir (Avaner, 2018).

Bu önlemler, sağlık verileri de dâhil olmak üzere farklı kişisel verilerin işlenmesini içerdiğinden, mahremiyet ve veri koruma durumları için kritik önem ve tehlike arz etmektedir. Yani, kuruluşlar belirli önlemlerin bireylerin mahremiyeti üzerinde bir etkisi olduğunun ve halk sağlığına yarar sağlayan güvenlik önlemleri ile bireylerin mahremiyetini etkileyen istilacı kontroller arasındaki çizgiyi nereye çekecekleri konusunda bir seçime sahip olduklarının farkında olmalıdır. Buna göre, kuruluşlar için bir yandan mahremiyet ve veri koruma arasındaki kaçınılmaz değiş tokuş fikrini, diğer yandan da halk sağlığını koruyan etkili önlemler fikrini çürütmek için bir katalizör görevi görmesi gerekmektedir. Veri koruma ilkeleri ve doğru dengeyi sağlamayı sağlayan teknik araçlar, gizlilik/mahremiyet uzmanları tarafından kullanılabilmektedir (Deloitte, 2020: 1-2).

1.2.4.4.Güvenlik

Güvenlik, gizlilik/mahremiyet ile aynı şey değildir ve sağlam güvenlik uygulamalarının uygulanması, gizliliğin sağlanacağını garanti etmemektedir. Bunun nedeni, gizliliğin en çok tanımlanabilir kullanıcı verileri ve onlar hakkında nelerin toplanabileceğini kontrol etme haklarıyla ilgilenmesi, ne için kullanılabilir ve kime ifşa edilebileceği olarak bilinmektedir. Kuruluşların kullanıcı verilerini kötüye

kullanımdan korumalarının tek yolu politikaları, standartları ve adil bilgi uygulamalarını göz önünde tutmaları gerekmektedir. Öte yandan, güvenlik, bilgileri gizli tutmak için gereken fiziksel, mantıksal ve prosedürle ilgili önlemleri sağladığından, gizlilik güvenlik olmadan elde edilememektedir (Ménard, 2006: 117).

Hem ulusal hem de uluslararası düzeyde risklerin çoğaldığı ve arttığı çağda, yaygın olarak güvenlik, yaygın tehdit ve korkulara karşı bir entelektüel söylem ve politika tartışması alanı haline gelmektedir. Kişilerin zararlı dış etkenlere karşı korunması sorunu hep değişmektedir. Bu özellikle soğuk savaşın sona ermesinden, çok kutupluluğun ortaya çıkmasından ve küresel terörizmin yayılmasından sonra önemi artmaktadır. Bununla birlikte, dünyadaki ana akım sosyal bilim tartışmalarında yerleşik bir bireyin/kişinin güvenliğini sağlayan sınırları net bir insan güvenliğini tanımlayabilecek bir kavram bulunmamaktadır. İnsan güvenliği teorisinin yokluğunda çok az nicel gösterge bulunmaktadır. Bu nedenle insan güvenliğine ilişkin çok az veri tabanı varolmaktadır. Daha yakın zamanlarda siyaset teorisyenleri, insani gelişme ve insan hakları kavramına dayalı bir insan güvenliği kavramı geliştirmeye çalışmaktadır. Fakat sosyal bilim teorisi, insan güvenliğini tam olarak neyin oluşturduğuna dair kapsamlı bir bakış açısı veya kavram oluşturamamaktadır. Bunun yanı sıra bireyin güvenliğininin sağlanması gereken alanlarda her dönemde artış göstermektedir. Özellikle bilgisayarın icadı ve veri aktarımının gelişmesi, kişisel verilerin kişilerin rızası olmaksızın aktarılmaya başlanması yeni bir güvenlik sorunu meydana getirmektedir (Powell, 2012).

Nitekim, özel ve kamu sektörlerindeki veri denetleyici aktörler, bireyler hakkında artan miktarda kişisel veri tutmaktadır. Azalan elektronik depolama ve işleme maliyeti buna büyük katkı sağlamaktadır. Kuruluşlar ayrıca veri işlemeyi üçüncü taraflara (veri işlemcileri) giderek daha fazla dış kaynak olarak sağlamaktadır. Birçok kuruluş, büyük miktarlarda kişisel veriyi manüel olarak iş yerlerinde tutmaya devam etmektedir. Bu işlenen ve elde tutulan verilerin miktarları her geçen gün artmaktadır. Bu sebeple bu kuruluşların güvenlik sorunları ortaya çıkmaktadır. Bu

durumda kişisel verilerin korunmasının sağlanmasını denetleyen aktörlerin, mevcut süreçleri düzenli olarak denetleyip kontrol altında tutması gerekmektedir (Shi, 2018).

Bilgi sistemlerine yönelik tehditler ise oldukça çeşitli sebeplerden ortaya çıkmaktaıdr. Yabancı ülkeler arasındaki birçok hedefli saldırıda olduğu gibi tehditler kasıtlı casusluk, bilgi gaspı veya sabotaj eylemleri olabilmektedir. Ancak çoğu zaman en büyük tehditleri doğa güçleri (kasırga, sel), insan hatası veya başarısız insan eylemleri sebep olabilmektedir. Her tehdidi tahmin etmeye ve azaltmaya çalışmak kolay gibi görünmesine rağmen bu mümkün olamamaktadır. Ancak tehdite sebep olan unsurlar, yalnızca kendilerine bir güvenlik açığından yararlanma fırsatı sağladığında tehdittir ve nihayetinde güvenlik açığından yararlanılacağına dair hiçbir garanti bulunmamaktadır. Bu nedenle hangi tehditlerin önemli olduğunun belirlenmesi yalnızca kuruluşlar bağlamında yapılabilmektedir. Bunların manevi zararını bireyler üzerinden ölçmek mümkün olamamaktadır. Bu sebeplerle birlikte kişisel verilerin güvenlik zaafiyetlerinin titizlikle incelenmesinin önemi artmakta ve kişisel verilerin kullanımında güvenliğin sağlanması ana faaliyetlerden birisi haline gelmektedir (Caballero, 2020: 6).

1.3. Bilgi ve Kişisel Bilginin Tarihsel Süreç İçerisindeki Konumu

Kabile topluluklarından oluşan ilkel toplumlarda, konuşarak ve işaretlerle aktarılan bilgi, daha sonraki aşamalarda değişik biçimlerde yazıya dökülerek eski uygarlıkları doğurmuştur. Nitekim insanlığın doğuşundan beri insanlar kendileri ve içinde yaşadıkları doğal dünya hakkında kavramlar geliştirmektedirler. Hatta Antik ve Orta Çağ kültürlerinde geliştirilen veya kullanılan kavramlar, metinsel, ikonografik ve maddi kalıntılarda halen izlenebilmekte ve incelenebilmektedir. Dolayısıyla bilgi üretimi insanlığın var olduğu ilk andan itibaren başladığı iddia edilebilmektedir (Ünal, 2009: 127).

Bilgi ilk ortaya çıktığı günden beri nesillerden nesillere aktarılarak gelişimi ve değişimi sağlanmaktadır. Bu bilgi aktarımı kimi zaman gelenekler ve kültürlerle kimi zaman ise bilimsel (yazının icadı ve devamındaki süreç ile) yollar aracılığıyla meydana

gelmektedir (https://mytok.blog). Nitekim bilgiyi belirli bir biçimde saklamak burada insan açısından bilinçli ve kasıtlı bir eylem olarak kabul edilmektedir. İki ana niyet uygun görünmektedir: Birincisi, bilgiyi bireysel amaçlar için depolamak[4] ve ikincisi, bir kişiden diğerine, gelecek nesiller için veya diğer gruplar ve kültürler için bilgi paylaşılmaktadır (Althoff, Berrens ve Pommerening, 2019: 13-14).

Bu sebeple karanlık çağlardan kalan mağara resimlerine bakıldığı zaman insanın bilgiyi hem kayıt altına almak hem de sonraki nesillere dolaylı olarak avcılık ve toplayıcılığın nasıl olduğuna dair bilgilerin bırakılmış olması bilginin oluşumu ve paylaşımı konusunda çağlar öncesine ışık tutmaktadır. Özellikle 13.000 yıl önce tarımın ilk gelişim dönemi ile birlikte, insanoğlu yerleşik hayata geçmeye başladığı tarihsel kaynaklara ve tezlere göre iddia edilmektedir[5]. Bu durum günlük tüketim malzemelerinin, ticari malların ve el sanatlarının depolanmasını ve idaresini zorunlu hale getirmektedir. Bunun devamında zaman ve mekan boyutunda insanlar, bilgi depolamak ve iletişim kurmaya zorunlu kaldıkları bir pozisyona geldikleri görülmektedir. Bu yüzden sayılar ve yazının gelişimi bu tarihi geçmişe göre değerlendirilmelidir. Bilginin tartışılması ise M.Ö. beşinci yüzyılda, felsefeci Sokrates'in bilginin sınırları sorusu ile başladığı esas alınmakta ve başlangıçtaki yüzyıl boyunca bilgi; aletlere, süreçlere ve ürünlere uygulanmıştır. Bu da sanayi devriminin temelini oluşturmuştur. İkinci aşama ise 1880'den başlayıp İkinci Dünya Savaşı ile biten dönemde, bilgi artık yeni anlamıyla işlere uygulanmaya başlamaktadır. Son aşama İkinci Dünya Savaşı'ndan sonra başlamış olup bilginin kendisine uygulanmaktadır. Yani bilgisayarın keşfedilmesi bilgininin son devrimlerinden olmuştur. Burada artık bilgi, son hızla üretimin en önemli faktörü hâline gelmekte, sermaye ve emek faktörlerini bir yana itmektedir (Güçlü ve Kseanela, 2006: 353).

---

[4] Antik Mısır'da papirüslerin üzerine yazılarak kayıt altına alınan bilgilerin yüzyıllar sonrasına ışık tutması gibi.

[5] Göbeklitepe, Şanlıurfa şehir merkezinin 15 km kuzeydoğusunda yer alan ve Karaharabe (Örencik) Köyü'nün 2,5 km doğusunda bulunmaktadır. Neolitik döneme (MÖ. 10.500 - MÖ. 7.500) ait bir inanç merkezidir. Yaklaşık 200-300 metre yüksekliğinde ve kireçtaşı kayalıklardan oluşan bir höyüğün üzerine inşa edilen bu megalitik yapı, Harran Ovası'na hâkim bir konumda bulunmaktadır. Düz kireç taşı platodan yukarıya doğru yükselen bu höyük, bir göbeğe benzediği için Göbeklitepe olarak adlandırılmıştır (Kurt ve Güler, 2017: 1111).

İkinci Dünya Savaşı'ndan sonra bilgisayarların icadı ve yaygınlaşması, sanayi ve hükümetin faaliyetlerini yürütme biçiminde değişiklikler meydana getirdiği yadsınamaz bir gerçektir. 1950'lerde ve 1960'larda bilgisayarlar veya bilgi ve telekomünikasyon teknolojisi "veri çatışması" amacıyla büyük bilimsel, ticari ve devlet uygulamalarıyla sınırlandırılmaktaydı. Bilim adamları hesaplamak için ihtiyaç duydukları çok miktarlarda veriyle uğraşmıştır. İş ve hükümet kuruluşları borç hesapları, alacaklar, bordrolar ve envanter kontrolü ile mücadele etmiştir. Bütün bunlar, halk gözünden gizlenen, ancak büyük kuruluşların rutin faaliyetleri için çok önemli olan "arka oda operasyonları" denilen şeyle sınırlandırılmaktaydı. Yazılımın o dönemde şimdiye oranla daha karmaşık olduğu düşünülmüştür. Bundan dolayı bilim odaklı ve iş odaklı gibi amaçlar ortaya çıkmıştır. Daha sonra diğer dillerde görünmeye başlamıştır. Böylece bilgisayar sistemlerinin gelişimi ivme kazanarak bilginin altın çağının yaşanmasında en etkili sebep haline gelmiştir (Geisler, 2008).

Bilgi devriminin ortaya çıkmasına yol açan asıl itici güç, 1970'lerde başlayan üç yakınsak fenomen şeklinde gelişmiştir. İlk olarak, entegre devrelerin tanıtımı nedeniyle bilgi işlem gücünün (donanım) performansı artmıştır. Bu da hesaplama maliyetinde sürekli göreli bir düşüşe yol açmıştır (Moore Yasası[6]). İkinci fenomen, masaüstü bilgisayarların (kişisel bilgisayarlar veya PC'ler) icadı ve hızlı çoğalması ve 1970'lerde icat edilen bu makineler, kısa süre içinde şirket ve devlet dairelerinde kullanılmaya başlanmıştır. Böylece bu sistemler sadece arka oda sistemi olmanın ötesinde, kuruluşların tüm fonksiyonel departmanlarındaki yöneticilerin ön bürolarında da yerini bulmuştur. Bilgisayarların yayılması ve kullanım kolaylığına büyük bir destek Microsoft ve yüksek performanslı işletim sistemi tarafından sağlanmıştır. Üçüncü fenomen, ilk ikisinin ve elektronik iletişimin İnternet ve World Wide Web ağları şeklinde çoğalmasını kolaylaştıran hipermetin yazılımının ortaya çıkmasıyla meydana gelmiştir (Jensen, 2000).

[6] Her 18 ayda bir tümleşik devre üzerine yerleştirilebilecek bileşen sayısının iki katına çıkaracağını, bunun bilgisayarların işlem kapasitelerinde büyük artışlar yaratacağını, üretim maliyetlerinin ise aynı kalacağını, hatta düşme eğilimi göstereceğini öngören deneysel (ampirik) gözlem(https://tr.wikipedia.org/)

Yirminci yüzyılın son on beş yılında şirketler, bilgi ve telekomünikasyon teknolojilerine büyük yatırımlar yapmış ve bu teknolojileri kuruluşlarının her yerinde yaygın hale getirmiştir. Sistemlerin bakımı için daha fazla donanım, daha iyi yazılım ve büyüyen bütçeler, üretim, pazarlama ve hatta müşteri ilişkileri gibi alanlara genişletilmiştir. Bunlarla birlikte ise 1990'ların internet tabanlı şirketlerinin ani yükselişine ve hızlı düşüşüne inanılmaz bir şekilde bakılma eğilimindeydi. Bu on yılda nasıl olabilir? gibi bir soru sürekli düşünülmüştür. Ancak bu patlama ve başarı öyküsü, bilgi teknolojisini ve interneti temel ögelerin bilgi çağını hızlandıran tek faktör olmadığı gerçeğini gizlemektedir. Elektronik ağlar işletmelerde, devlet kurumlarında ve özel konutlarda bir gerçeklik haline geldikçe, bu sistemlere yapılan yatırımlar artmaya devam etmektedir. Her geçen gün teknoloji arttıkça yapılan yatırımlar artmaktadır. Böylece teknoloji hayatımızın vazgeçilmezi haline gelmektedir (Montolio ve Trujillo, 2012).

Bilginin ve bilginin müşterek olarak araştırılması hâlâ erken emekleme aşamasında olma özelliğini sürdürmektedir. Bununla birlikte, çeşitli biçimlerindeki "bilgi" ile çeşitli biçimlerindeki "müşterekler" arasındaki bağlantı çok çeşitli akademisyenler, sanatçılar ve aktivistlerin dikkatini çekmiştir. "Bilgi müşterekleri" hareketi çarpıcı bir hızla ortaya çıktı. 1995'ten önce, birkaç düşünür bu bağlantıyı görmekteydi. O sıralarda, "müşterekler" kavramının yeni kullanımları görülmeye başlanmıştı (Kranich, 2003).

Artan sayıda bilim insanı, "müşterekler" kavramının, yaygınlaşmış dijital bilginin yükselişiyle birlikte gözlemledikleri yeni ikilemleri kavramsallaştırmalarına yardımcı olduğunu bulmuştur. 1990'ların ortalarında, çeşitli disiplinler de bu yeni ortak bilgilerin bazı yönlerini ele alan makaleler ani bir şekilde ortaya çıkmaya başlamıştır. Bazı bilgi bilimciler, sanal toplulukların ve müştereklerin yeni alanlarında ilerleme kaydetmiştir. Diğerleri, internette tıkanıklık ve serbest sürüş gibi ortak ikilemleri araştırmıştır. En büyük "yeni ortak" keşif dalgası yasal incelemelerde ortaya çıkmıştır. Yaygınlaşan, çevrelenen, metalaştırılan ve aşırı patentli dijital bilgi için moda bir sözcük haline gelmiştir. "Dijital", "elektronik", "bilgi", "sanal", "iletişim",

"entelektüel", "İnternet" veya "teknolojik" müşterekler olarak etiketlenmiş olsun, tüm bu kavramlar küresel olarak dağıtılmış bilginin yeni paylaşılan alanına hitap etmektedir. (Hess ve Ostrom, 2007)

1990'ların sonunda “bilgi çağı” ve “bilgi toplumu” hakkında pek çok şey yayınlanmıştı. Bu sebeple yirmi birinci yüzyıl, bilgi çağının dünyanın hemen her köşesine yayılması, ekonomik ve sosyal yaşamın neredeyse her yönünde yaygınlaşmasını hızlandırmaktadır. 2000’li yıllara gelindiği zaman bilginin aktarımında devrim olmuştur. Özellikle akıllı telefonların yaygınlaşması ve sosyal medya mecralarının çoğalmasıyla bilgi değişiminde ve gelişiminde ivme kazanmıştır. Bu nedenle bilgi önceki yüzyıllara göre daha hızlı, daha yaygın olarak paylaşılabilen bir hal almıştır. Nitekim bu sayede ortaçağda ancak bir bilim adamının bileceği ve ulaşabileceği çeşitli bilgiye son yüzyılla birlikte herkes erişebilmektedir (Östling, vd., 2018).

İKİNCİ BÖLÜM
KİŞİSEL BİLGİLERİN GÜVENLİĞİ ve KORUNMASI SORUNU

Hem ulusal hem de uluslararası düzeyde risklerin çoğaldığı ve arttığı çağda, yaygın olarak insan güvenliği olarak bilinen bireyin güvenliği, yaygın tehdit ve korkulara karşı bir entelektüel söylem ve politika tartışması alanı haline gelmektedir. Bu özellikle soğuk savaşın sona ermesi, çok kutupluluğun ortaya çıkması ve küresel terörizmin yayılması durumlarından sonra daha da önem kazanmıştır. Bununla birlikte dünyadaki ana akımın sosyal bilim tartışmalarında yerleşik bir insan güvenliği kavramı bulunmamaktadır. İnsan güvenliği teorisinin yokluğunda, çok az nicel gösterge bulunmaktadır. Bu nedenle insan güvenliğine ilişkin çok az veri tabanı bulunmaktadır. Daha yakın zamanlarda siyaset teorisyenleri, insani gelişme ve insan haklarına dayalı bir insan güvenliği kavramı geliştirmeye çalışmaktaydılar. Yine de, sosyal bilim teorisi, insan güvenliğini tam olarak neyin oluşturduğuna dair kapsamlı bir görüş sunamamaktadır. Yani bu durum, küreselleşme süreci ve bununla bağlantılı yüksek sosyal maliyetler nedeniyle daha da karmaşık hale gelmektedir (Menon, 2007).

Bir kişinin ne zaman gerçekten özgür olduğunu, özgürlüğün neden önemli olduğunu ve özgürlüğün neye bağlı olduğunu anlamak için üç bağlamsal faktör tanımlanarak eksiklikler giderilmeye çalışılmaktadır. Bu üç faktör ise; "*kimin özgürlüğü söz konusu*", "*failin neyden muaf olduğu* (engelleme koşulu)" ve "*aracı kişinin yapmakta, yapmamakta, ne hale gelip gelmemekte özgür olduğu*" faktörleri olarak belirlenmiştir. Diğer bir deyişle, anlamlı özgürlük tartışmaları bağlama yerleştirilmeli ve uygun bilgilere dayandırılmalıdır. Burada aynı şeyin güvenlik için söylenebileceği tartışılmaktadır. Güvenlikle ilgili anlamlı tartışmalar, kimin güvenliğinin söz konusu olduğu, hangi değer veya menfaatin güvence altına alınacağı, hangi risk veya tehdidin ortaya çıktığı ve kimin korumak ve sağlamak için en iyi konumda olduğuna ilişkin uygun bağlamsal bilgilere dayanmaktadır. Güvenlik kavramının kendisi bu bilgiyi içermemektedir. Güvenlik ilişkisel bir kavramdır. Çünkü bu üç tartışma faktörü arasındaki ilişkiyi tanımlamakta ve herhangi bir bağlamda anlamını onlardan almaktadır (Powell, 2012: 6).

2.1. Kişisel Bilgi Çerçevesinde Güvenlik

İnsanlık tarihinde bilginin korunmasında ve güvence altına alınması ile ilgili bilinen ilk bulguları MÖ. 2000'li yıllarda Mısır toplumuna ait bazı kalıntılarda bulunan belgelerde, kriptoloji[7] tarihinin ilk kayıtlarına rastlandığı iddia edilmektedir (Çeşmeci, 2009:20-21). Bu dönemde geliştirilen şifreleme yöntemleri; sadece söz konusu bilgiyle ilgili kişilerin anlayabileceği simgeler, ifadeler ve yazıların kullanımı ile yazılmaktaydı. Bu tekniğe "scytale" tekniği denilmektedir. Bu teknikte şerit şeklinde bir kağıdın bir silindire sarılarak yazılması ile oluşturulmaktadır. Ayrıca Roma İmparatoru Jül Sezar'ın yazılarında her harfin alfabede kendisinden sonra gelen üçüncü harfle yer değiştirdiği metodun kullanıldığı bilinmektedir (Yiğitbaşı, 2015: 57).

Kişisel güvenliğin ve huzurun önemi ve tanımlanmaları özellikle son yıllarda hızlı bir değişim içerisinde bulunmaktadır. Bu sürecin tarihteki önemli dönüm noktalarından birisi 19. Yüzyılda ivme kazanmış olan teknolojik gelişmelerdir. Özellikle İkinci Dünya Savaşı döneminde ve sonrasında bilgisayarında icat edilmesi ile birlikte insanın güvenliğinin sağlanmasında gerekli olan koşulların ve bu koşulların sınırlarının nasıl çizileceği konusuna ilişkin bir çok girişimde bulunulmuştur. Fakat net bir tanım oluşturulamamasının yanı sıra güvenliğinin sağlanması gereken yeni ve önemli bir koşul olarak kişilere ait veri veya bilgilerin korunması sorunsalı da eklenmektedir. Teknolojinin ve özellikle bilgi aktarımının oldukça hızlı olduğu bu dönemde kişinin güvenliğinin sağlanmasında kişiye ait özel verileri ve bilgilerin de korunması en az kişi/birey güvenliği kadar zorlaşmaktadır.

2.1.1. Kavramsal ve Kuramsal Olarak Güvenlik

Varolan her canlının öncelikli amacı varlığını korumak ve sürdürmektir. Bir canlı olarak insanlar için geçerli olan bu durum insanlardan meydana gelen devletler için de geçerli olmaktadır. Yani varlığını korumak ve sürdürmek güvenlik kavramının

[7] Şifre Bilimi.

da özünü oluşturmaktadır (Sancak, 2015: 124). Nitekim, Abraham Maslow'un ihtiyaçlar hiyerarşisindeki[8] fizyolojik ihtiyaçların hemen sonrasında yani ikinci basamakta 'güvenlik gereksinimi' yerini almaktadır. Güvenlik ihtiyacı oldukça karmaşık olmasının yanı sıra "kesinlik, istikrar, destek, koruma, korku, endişe ve kaostan kurtulma, yapı, düzen, yasa, sınırlar vb." gibi kavramları da kapsamaktadır. Nitekim, temel bir ihtiyaç karşılanmazsa, bireyin gelişimi engellenmiş olacağı için bu özel ihtiyacı karşılama çabası sınırlanmaktadır. Temel ihtiyaçlardan biri olan güvenlik gereksinimi yiyecek ihtiyacından daha öncelikli ve güçlü olmamasına rağmen fizyolojik ihtiyacı doyrulan insanın güçlenmeye başlayan ve karşılanması gereken ikinci gereksinimi haline gelmektedir. Bundan dolayı fizyolojik ihtiyaçlarla beraber güvenlik ihtiyacı da sağlanmaz ise hayatın sürdürülebilirliği de olmayacaktır (Maslow, 1943).

Bunun yanı sıra güvenlik kavramının tanımlanması da en az güvenliği sağlamak kadar zor bir durumdur. Fakat insanlığın ilk dönemlerinde güvenliğin sınırları kolay bir şekilde belirlenebilmiştir. Yani ilk çağlarda insanların yaşamlarını sürdürebilmeleri için asgari düzeyde kendilerini koruması ya da dışarıdan gelebilecek herhangi bir saldırıya karşı kendilerini ve sorumlu olduğu kişileri korumak ya da savunmak olarak anlamlandırılmıştır. Fakat insanların birleşimi ile oluşan kabilelere ve hatta kent devletlerinden başlayarak günümüzdeki halk egemenliğinin önemli olduğu devlet yapısına kadar olan süreçte güvenlik kavramı farklı şekillerde ve yapılarda sınıflandırılıp ele alınmıştır. Bu sebeplerden ötürü güvenliğin farklı açılardan tanımları ele alınmaktadır.

Güvenlik, sosyal bilimlerde yeni bir kavram değildir. Aslında güvenlik, ulus devletlerin ortaya çıktığı ve sürdürüldüğü uluslararası sistemin temel bileşenidir. Ancak modern insan güvenliği kavramı, temelde bireyin güvenliği yerine devletin güvenliğine odaklanan geleneksel güvenlik paradigmasının içsel zayıflığını

[8] Amerikalı psikolog Abraham Maslow, "İnsan Motivasyonunun Bir Teorisi" başlıklı 1943 tarihli bir makalede, insanın karar vermesinin bir psikolojik ihtiyaçlar hiyerarşisi tarafından desteklendiğini teorileştirdi. İlk makalesinde ve 1954 tarihli Motivation and Personality adlı kitabında Maslow, beş temel ihtiyacın insan davranışsal motivasyonunun temelini oluşturduğunu öne sürdü. Bu

tanımlamaktadır. Geleneksel olarak baskın güvenlik kavramı, devlet merkezliydi. Desteği ve meşruiyeti devletlerin araçlarını genişletmekte ve devlet egemenliği ilkesini sürdürmekteydi. Platon'un İdeal devleti, Aristoteles'in Devlet Adamı, Hobbs'un Leviathan kavramı, Machiavelli Prensi ve her şeyden önce Marksçı proletarya diktatörlüğü kavramı devletin nihai hedefini ya da sonunu bireyin ve topluluğun güvenliği ve korunması olarak vurgulamaktadır. Ancak bu teorilerin hiçbiri insan güvenliğine bağımsız bir kimlik ve/veya varoluş verememekteydi ve insan güvenliği üzerine kavramsal çerçeve geliştirememiştir. Bunun yerine güvenlik, güvenlikle ilgili sorunlara askeri merkezli çözümlerle vurgu yapan ulusal güvenliğin ayrılmaz bir parçası olarak tasarlanmıştır. Örneğin; Birleşmiş Milletler (BM) sistemi halkın güvenliğini korumak için kurulmuş olsa da, BM güvenlik ilkesi başlangıçta yapıların ve modern devlet uygulamalarının egemenliğine yönelik tehditleri ele alabilmektedir. Bireylerin güvenliğini ayrı ayrı ele almamaktadır (Menon, 2007: 2).

Bu bağlamda hem bir kavram hem de uygulama aracı olarak insan güvenliğinin kökenini ve gelişiminin çeşitli aşamalarını incelemek önemli olduğu belirtilmektedir. İnsan güvenliği kavramsal netlik ve entelektüel söylem için özel bir paradigmadan yoksun olduğundan kavramın tarihsel gelişimini kesinlik ve açıklıkla analiz etmek zor olmaktadır. İnsan güvenliğinin belirli sınırları bulunmamaktadır. Bireysel ve kolektif varoluşun güvenliğini etkileyen her şey insan güvenliği altına girebilmektedir. Bu sebepten ötürü kavramın kapsamı belirsizlikle dolu olduğu iddia edilmektedir. Bu sınırlamanın üstesinden gelmek için kavramın kapsamını BM, insan güvenliği kavramını ve etrafında faaliyet gösterilen ana akım tartışmalarını sınırlandırmaya çalışmaktadır. Çünkü politika oluşturma ve uygulama aracı olarak insan güvenliğinin önemi ilk kez UNDP İnsani Gelişme Raporu 1994 tarafından ifade edilmektedir. Eş zamanlı olarak Kanada, Japonya ve Norveç iç ve dış politika seçeneklerinde insan güvenliği merkezli yönetişim girişimlerini önermiştir. Bununla birlikte, kavramın kökenini ve gelişimini analiz ederken, BM yorumlarının ve son politika tartışmalarının ötesine geçmek uygunsuz olmaktadır. İnsan güvenliğine yönelik endişeler ve geleneksel güvenlik merkezli kavramları eleştirme girişimi, evrensel olarak kabul

edilmemekte ve tartışılmamakta olmasına rağmen soğuk savaş döneminde dahi gündemde bulunmuştur (Bakan ve Şahin, 2018: 144-145).

Dolayısıyla insanlık tarihi geliştikçe güvenlik kavramının kapsamı da genişlemektedir. Güvenliğin günümüzde spesifik olarak sınırlarını belirlemek ve aynı zaman da soyutsal olarak tanımlamasını yapmak oldukça zor ve karmaşık olduğu söylenmektedir. Fakat başlangıç olarak "korku, tehdit ve tehlikelerden uzak olma durumu" şeklinde tanımlanılan güvenlik kavramı, son yıllara kadar sosyal bilimlerin ve fen bilimlerinin birçok dalının araştırma alanına girmekteyken teknolojik gelişmelerle birlikte bilgisayarın da icadı ile güvenlik araştırmaları teknoloji için de tanımlanmaya başlanmıştır. Fakat her bilim dalında güvenlik kavramının tanımlanması farklı açılardan ele alınmaktadır (Uğuz, 2016: 86-87).

Güvenlik, toplumun siyasi örgütlenmesini belirleyen bir ihtiyaçtır. Güvenliğin sağlanması, devletin en temel amaç ve işlevlerinden biri olarak kabul edilmektedir. Konuyla ilgili literatür, öncelikli değerler ve hedeflerin bir kataloğunu içermektedir. Güvenlik kavramı: "*Nüfusun biyolojik olarak hayatta kalması, bir etnik grup olarak ulus ve bir kurum olarak devlet, devletin toprak bütünlüğü, bağımsızlığı ve egemenliği, iç istikrar ve karmaşık, sosyo-ekonomik sürdürülebilir kalkınma vb*." kavramları da kapsamaktadır. Böylece güvenlik, ulusal değerlerin ve çıkarların mevcut ve potansiyel tehditlere karşı korunmasını ve savunulmasını ve engelsiz bir kalkınma için iç ve dış koşulların yaratılmasını amaçlayan bir devlet kuruluşu olarak tüm toplumun temel ulusal misyonu haline gelmektedir. Ancak gergin durumlarda veya çatışmalarda güvenliği sağlamak, tüm araçların ve güçlerin tabi olduğu bir hedef noktası olmaktadır (Erdoğan , 2013).

Güvenlik; Osmanlıca ve temelde Arapça'dan gelen asayiş kelimesi ile ifade edilerek "emniyet" kelimesinden ayrı kullanılmaktaydı. İngilizcede de emniyet "safety" kelimesi ile ifade edilirken, güvenlik "security" sözcüğü ile ifade edilmektedir. "Security" ise iki Latince sözcüğün "se"(olmaksızın ya da yok) ve "cura"(endişe ya da korku) birleşimi olan, İngilizce ve Fransızca (securité) dahil olmak

üzere çeşitli Avrupa dillerinde varlığını sürdüren Latince isim securitas'tan türemiştir (Payam, 2018: 18). Latince'de “se” yok anlamında iken “cura” 'ilgi', 'korku', 'kaygı' anlamına gelmektedir. Bu nedenle güvenlik kelimesi başlangıçta korku veya endişenin olmaması olarak tercüme edilmektedir. Etimolojik anlamın, tehdit eksikliği ve varlığın kesinlik duygusu nedeniyle güvenliğin, yetkilendirici karakteri ile ilgili olduğu söylenmektedir. Böylesi bir perspektiften bakıldığında güvenlik, bir varlığın en önemli ihtiyaçlarından biridir. Aynı zamanda birey, kurum veya devlet olması farketmeksizin eylemlerinin en önemli amaçlarından biridir (Arends, 2009: 5-7).

Bunların yanı sıra güvenlik hakkında konuşulmaya başlandığı zaman ilk olarak kavramın tanımının ne olduğu sorulmaktadır. Ama böyle bir soru sormak başlangıç olarak yanlış olmaktadır. Çünkü güvenlik diye bir şeyin günlük hayattaki kullanımı dışında da var olup olmadığı tartışma konularından birisidir. Diğer bir deyişle, güvenlik, günlük söylemdeki ifadesinden bağımsız olan gerçek bir varoluş durumuna da atıfta bulunmaktadır. Bu sebeple ontolojik[9] güvenlik, oldukça farklı şekillerde tasavvur edilmeye çalışılmaktadır. Örneğin; Uluslararası İlişkiler teorisinde Gerçekçilik ve İdealizm arasındaki büyük tartışmada, ya şimdiki zamanın göreceli bir durumu ya da geleceğin mutlak bir koşulu olarak düşünülmektedir. Ancak her iki durumda da güvenliğe yapılan atıflar, belirli bir nesnelliği ifade etmeye çalışmaktadır. Bu düşünme şeklinin incelenmesi gereken en az iki sonucu bulunmaktadır. Birincisi, güvenlik nesnel olarak bilinebilen ve bu nedenle özenle ölçülmesi, izlenmesi, akıl ve bilimsel araştırma yoluyla iyileştirilmesi gereken bir şey olarak düşünülmektedir. İkincisi, güvenlik normatif bir kaliteye ulaşır; aktif olarak hedeflememiz gereken bir "iyi şey" olarak görünmektedir (Boemcken ve Schetter, 2009).

Aslında bu düşünceye göre güvenlik oldukça yakın zamana kadar, Uluslararası İlişkiler’in akademik disiplini tarafından tekelleştirilmekte olan bir örnek olabilmektedir. Uluslarası İlişkiler teorisyenleri tarafından güvenlik kavramının oldukça sınırlı bir alanda kullanılması ve ayrıca politikacıların da bu kavramı siyasi

[9] Ontolojik Türk Dil Kurumu (2021) sözlüğüne göre “varlık bilimi ile ilgili” ya da “varlık bilimine ait” anlamına gelmektedir.

alanda kullanması, güvenlik kavramını askeri güçle eş anlamlı olarak kullanılmasına yol açmaktaydı. Yani askeri güç ne kadar elverişli ve sürdürülebilir olursa güvenlikte aynı derece elverişli ve sürdürülebilir olmaktaydı (Powell, 2012: 10).

Böyle bir perspektiften bakıldığında, genel güvenlik tanımına genellikle belirli bir nesneye yönelik tehditlerin yokluğunda veya en azından olası olmadığında karşılaşıldığı düşünülmektedir. Örneğin, David Baldwin güvenliği zekice "edinilmiş değerlere düşük hasar olasılığı" olarak tanımlamaktadır. Benzer şekilde Lawrence Krause ve Joseph Nye için güvenlik: "*Bir halkın hayatta kalması için gerekli olduğunu düşündüğü temel değerlerin asgari kabul edilebilir seviyelerine yönelik akut tehditlerin yokluğuydu*". Bu tür güvenlik tanımları, terimin altında yatan özü bir şekilde yakalamaya çalışmaktadır. Ancak yine de oldukça farklı şekillerde kavramsallaştırılabilmektedir. Belirli bir akademik ve / veya politik proje bağlamında güvenlik kavramına geçmek için ele alınması gereken en önemli soru, güvenliğin kimin için olduğu sorusu sorulabilmektedir. Bu soruya genellikle cevap olarak: Bazılarına, tüm bireylere, bazı durumlara ya da tüm durumlara atıfta bulunmaktadır. Bununla birlikte güvenliğin çok çeşitli alanlara örneğin; hayvan yaşamı, biyosfer veya fiziksel altyapı gibi alanlara dahi eşit şekilde uygulanabileceği unutulmamalıdır (Boemcken ve Schetter, 2009).

Türk Dil Kurumunun (2020) "Güvenlik" tanımında "*Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet*" olarak genel bir açıklaması yapılmaktadır. Yine de Soğuk Savaş'ın büyük bir bölümünde güvenlik çalışmaları temelde kontrol, tehdit veya güç kullanımı etrafında dönen konulara odaklanmaktaydı. Sonuç olarak, devletler hem gücün ana kullanıcıları hem de güç kullanımının ana hedefleri olarak görüldüğünden, uluslararası sistem özünde devlet merkezli kabul edilmektedir. Arnold Wolfers' ın "Ulusal Güvenlik" makalesi, Soğuk Savaş sırasında en önemli rakip güvenlik tanımlarına net bir genel bakış sağlamıştır. Wolfers'a (1952) göre güvenlik, Uluslararası İlişkilerde çok önemli bir kavramdır. Ancak doğası gereği son derece öznel de olabilmektedir.

Son yıllarda güvenlik kavramına ve özellikle de insan haklarıyla ilişkisine artan bir ilgi bulunmaktadır. Dünyanın dört bir yanındaki terörist saldırılarına yanıt olarak, uluslararası düzeyde bir dizi yeni güvenlik yasası çıkarılmaktadır. Bu tedbirler, insan hakları üzerindeki etkileri nedeniyle eleştirilmekte, medyada, hükümette, akademide ve mahkemelerde insan hakları ve güvenlik arasında kurulacak uygun denge hakkında tartışmalara yol açmaktadır. Fakat diğer taraftan bireyin ve toplumun güvenliğinin esas olduğunu savunan devletler bu eleştirileri almalarına rağmen kendi toplumları için gerekli güvenlik yasalarını çıkarmaktadır.

Güvenlik kavramının farklı bağlamlardaki farklı insanlar için farklı şeyler ifade ettiği iddia edilmektedir. Farklı öncüllerden başlayarak, farklı vizyon ve beklentilere sahip olarak, bir güvenlik sorununun algılanması, incelenmesi ve analizinden farklı paradigmalar türetilerek farklı çözümlere yol açabilmektedir. Böylesine karmaşık bir durumda, "Güvenlik nedir?" sorusuna yanıt vermeyi özellikle de ilgili çıkarların farklılaşması nedeniyle son derece zor kılmaktadır. Bu talihsiz durum, performansı ölçme, suçu araştırma ve sorumluluğu atfetme ihtiyacının ele almayı zorunlu kıldığı metodoloji ve gerekçelendirme problemlerini ortaya çıkarmaktadır. Güvenlik metodolojisinin kararları, önlemleri ve performanslarının, güvenlik tanımının olmaması durumunda hiçbir anlamı bulunmamaktadır (Sancak , 2015).

Aslında geleneksel bir güvenlik tanımı ile bireylerin, bilgilerin ve varlıkların bireysel güvenlik veya toplum sağlığı için korunmasında özel hizmetlerin sağlanması olabilmektedir. Ayrıca, özel veya ticari güvenlik, bir kuruluşun varlıklarına istenmeyen, yetkisiz veya tahrip edici zararların önlenmesinde ücretli hizmetlerin sağlanması olarak kabul edilebilmektedir (Brooks, 2010: 2).

Bu konu daha gerçekçi bir şekilde ele alınırsa çok boyutluluğundan dolayı güvenliğin tanımlanamayacağı görüşü akademide, mahkemede ya da sahada kabul edilememektedir. Sokrates'in 2.400 yıl önce belittiği gibi, "*terimlerin ortak bir anlamı yoksa, gerçeği yalandan ayırt etmek imkansız*" olarak ifade etmektedir. Dilin hassasiyeti, tüm çalışma alanlarında ortak anlam ve bilgiyi iletmek için gereklidir.

Locke, Frege ve Wittgenstein, biçimsel mantık, kesin tanımlar ve iyi ifade edilmiş cümleler aracılığıyla bunun mümkün olduğunu kanıtlamaktadırlar. Güvenlik kavramının farklı anlamları varsa, insanlar aynı problem üzerinde nasıl etkili bir şekilde çalışabilirler? Örneğin; birisinin veya bir şeyin güvenli olup olmadığı nasıl yargılanabilir? Sübjektif bir güvenlik tanımı, savaş ve suikasttan kaynaklanan saldırgan eylemler için bir bahane olarak güvenliğin esnek bir yorumuna ihtiyaç duyulmasını veya ihlal edilmesini mümkün kıldığından, devletlerdeki iktidarların saldırganlığın ve suçlamanın çıkarına hizmet etmesi mümkün hale gelebilmektedir (Manunta, 1999).

Bunlarla birlikte ise aslında insan güvenliği ile ilgili esasen yedi konu bulunmaktadır. Bunlar ekonomik güvenlik, gıda güvenliği, sağlık güvenliği, çevre güvenliği, kişisel güvenlik, toplum güvenliği ve politik güvenliktir (Torun, 2017: 225).

Ekonomik güvenlikle ilgili kriterlerden bazıları, sigortalı temel gelir ve istihdam ile bu tür sosyal güvenlik ağına erişimi içermektedir. Gıda güvenliği, basitçe temel beslenme ve gıda tedarikine erişimi ifade etmektedir. Sağlık güvenliği daha karmaşıktır ve güvenli suya erişim, güvenli bir ortamda yaşama, sağlık hizmetlerine erişim, güvenli ve uygun fiyatlı aile planlamasına erişim, hamilelik ve doğum sırasında temel desteğe erişim, HIV/AIDS'in önlenmesi veya diğer hastalıklar ve sağlıklı bir yaşam sürmek için temel bilgilere sahip olmak demektir (Erdem, 2016: 261-262).

Çevre güvenliği basittir ve su kirliliğinin önlenmesi, hava kirliliğinin önlenmesi, ormansızlaşmanın önlenmesi, sulanan arazinin korunması, kuraklık, sel, siklon, deprem vb. doğal tehlikelerin önlenmesi gibi konuları kapsamaktadır (Vural , 2018: 25).

Topluluk güvenliği ise geleneklerin, kültürlerin, dillerin ve ortak değerlerin korunmasını kapsar. Aynı zamanda etnik ayrımcılığın kaldırılmasını, etnik çatışmaların önlenmesini ve yerli halkın korunmasını da içermektedir (Hisarlıoğlu, 2019: 1).

Son olarak siyasi güvenlik, insan haklarının korunması ve tüm insanların refahı ile ilgilenmektedir. Aynı zamanda basın özgürlüğü, ifade özgürlüğü ve oy verme özgürlüğü gibi devlet baskısından insanları karşı korumayı da içermektedir. Siyasi gözaltının kaldırılması, hapis, sistematik kötü muamele ve ortadan kaybolma da siyasi güvenlik kapsamında yer almaktadır (Bien-Kacala ve Serowaniec, 2016).

İnsan güvenliğinin yedi unsuru arasında önemli bağlantılar ve örtüşmeler bulunmaktadır. Ancak insan güvenliğinin özellikle son yıllarda en az bu unsurlar kadar önemli olan diğer bir unsuru ise teknolojik gelişmelerle ortaya çıkan kişisel bilgi güvenliğidir. Bilgisayarın ve internetin keşfedilmesi ve her geçen gün daha da gelişmesiyle birlikte kişisel verilerin ve bilgilerin aktarımı ve paylaşılması da aynı oranda hızlanmakta ve yaygınlaşmaktadır. Her geçen gün kişilere ait bilgilerin korunması daha da zorlaşmaktadır. Bu bilgilerin korunamaması ise kişilere maddi ve manevi zararlar vermektedir. Bu sebeplerle birlikte kişilere ait bilgilerin korunması ve aktarımının kontrol altına alınması gerekliliği oluşmaktadır. Güvenliğin bu yeni yönü son yılların en önemli sorunlarından biri haline gelmektedir. Nitekim, bilgi ve özelinde verilerin korunması gerekliği de her geçen gün önem kazanmaktadır (Menon, 2007).

Kısaca, daha önce belirtildiği üzere güvenlik çeşitlerinin, "ekonomik güvenlik, gıda güvenliği, sağlık güvenliği, çevre güvenliği, kişisel güvenlik, toplum güvenliği ve politik güvenlik" her biri en az bir diğeri kadar önemlidir. Bu güvenlik çeşitlerinin sağlanması; birey ve toplum yaşamındaki önem derecesinin tanımlanması oldukça güçtür. Bu sebeple genel olarak güvenlik, fizyolojik ihtiyaçların hemen arkasında yerini alarak önemini belirtmiş olmaktadır.

2.1.2. Bilgi Güvenliği ve Kişisel Bilgi Güvenliği

Bilgi güvenliği kavramı, bilgi güvenliği yönetimi ve enformasyon yönetimi alanlarında oluşturulmaktadır. Ancak henüz ortak olarak üzerinde anlaşılan bir tanımı bulunmamaktadır. Fakat bilgi güvenliğini, önemli bilgiye yönelik tehditleri belirlemek, bilgiyi bu tehditlere karşı korumak, bu bilgiyi korumak için kuruluşlarda alınan yönetim süreci ve eylemler olarak kısa ve genel bir tanım yapılabilmektedir

(Ilvonen, Jussila, Kärkkäinen ve Päivärinta, 2015: 3943). Bunun yanı sıra bilgi güvenliği, bilgileri kötüye kullanma, bozma, ifşa etme, değiştirme vb. amaçlarla yetkisiz erişimden ve herhangi bir şekilde kullanımdan koruyan bir olgu ve genellikle fiziksel ve elektronik biçim için kullanılan genel bir terim olarak da tanımlanabilmektedir.

Bilgi güvenliğine yönelik ilk çalışmaların, askeri amaçlı bilgilerin gizliliğini ve kontrolünü sağlamak için 1970'li yıllarda yapıldığı bilinmektedir. Fakat bu tarihten önce de bilgi güvenliğine konu olabilecek durumlar gerçekleşmekteydi. 1980'li yıllarda ise ticari alanda bilginin bütünlüğünün sağlanmasına yönelik kaygıların oluşması, bilgi güvenliğinin bu boyutunun da dikkatleri üzerine çekmesine neden olmuştur. 1990'lı yıllarda da bilgi güvenliğinin gelişimi sürecinde görülen kaygılar artmaya devam etmiştir. Bu süreçte iletişim teknolojisinin bilgisayar ağları ile gelişimine bağlı olarak tehditlerin çeşitliliğinin artması, bilgi güvenliği konusunda yeni boyutların oluşmasını ve oluşan yeni boyutlar arasındaki karmaşık ilişkiyi açıklayacak bilgi güvenliği modellerinin geliştirilmesini sağlamıştır. 2000'li yıllardan itibaren kişisel haklara yönelik gelişmelere bağlı olarak kişisel verilerin korunması konusu da kamu kurumlarındaki verilerin gizliliğinin korunması kadar önemsenmeye başlanmıştır. AB ülkeleri ve diğer bilgi toplumuna dönüşüm sağlamış diğer ülkelerde bu konuya ilişkin çalışmalar hukuk ve diğer sosyal alanlara da yayılarak disiplinler arası boyutun gelişmesi hız kazanmaktadır. Ancak farklı alanlarda yapılan çalışmaların genellikle bağımsız olarak yürütülmesi ve aralarında yeterli düzeyde iletişim sağlanamaması, bilgi güvenliği zincirinin kırılgan hale gelmesine neden olmaktadır (Henkoğlu, 2015: 25-26).

Bilgi güvenliğinin temelinde "gizlilik" (Confidentiality), "bütünlük" (Integrity), "kullanılabilirlik" (Availability) olmak üzere üç unsur bulunmaktadır. Nitekim veri ve bilgilerin gizliliği, bu veri ve bilgiye yalnızca yetkili kişilerin erişim sağlamasıyla gerçekleşmektedir. Gizliliği korumak için kullanılan en yaygın güvenlik

önlemlerinden bazıları şunlardır: Veriler ve bilgiler önemlerine[10] göre çeşitli düzeylerde kamudan gizlilik oranına göre değişmektedir; çalışanlara işlerinin niteliğine, yetkinliklerine, veri ve birlikte çalıştıkları bilgilerin sınıflandırma düzeyine göre yetki ve erişim hakları verilmektedir; kuruluşun faaliyet alanına özgü yürürlükteki yasalar (örneğin, ticari sırlar yasası) uygulanmaktadır; gizlilik sözleşmeleri imzalanır, şifreler, şifreleme teknikleri, kilitler ve anahtarların yanı sıra kasa kullanılmaktadır (Popescul, 2011: 1339).

Veri ve bilgi bütünlüğü, bunların doğru ve eksiksiz biçimde tutulması gerektiği ve kazara veya kasıtlı olarak izin alınmadan değiştirilmemesi gerektiği anlamına gelmektedir. Veri ve bilgi bütünlüğünü korumaya yönelik hataların oluşmasını önlemek için verileri kontrol etme mekanizmaları, yedeklemeler, erişim kontrolü, çalışanların eğitimi vb. tedbirler de alınmalıdır (Ahmad, Kumar ve Hafeez, 2019).

Erişilebilirlik, yetkili kullanıcıların herhangi bir zamanda verilere ve bilgilere erişimini sağlamaktır. Bunun yanı sıra donanım ekipmanının ve ağların iyi çalışması, yedeklemelerin yasalara uygun bir şekilde çalışması da önemlidir (Baykara, Daş, ve Karadoğan, 2013).

Aslında buraya kadar bilgi ve bilgi güvenliğinin kurumsal düzeyde nasıl olduğu değerlendirilmekteydi. Fakat bu özellikler ayrıca bu kurumları, toplulukları ve hatta devletleri oluşturan en önemli etken olan bireyi de kapsamaktadır. Bunun yanı sıra "özgünlük/gerçeklik" ve "inkar etmeme" gibi iki özellik daha eklenmesi mümkündür. Özgünlük/gerçeklik, bir varlığın iddia ettiği şey olduğunu kabullenme özelliğidir. Yani bir eyleme dahil olan tüm tarafların kimliklerini doğrulayarak iddia ettikleri kişi olduklarını kanıtlamaktır. Bu sebeple bilgi güvenliğinde, verilerin, işlemlerin, iletişimlerin veya belgelerin gerçekliğini, yani bilgilerin gerçek olmasını sağlamak için kimlik doğrulama kodları veya dijital imzalar kullanılmaktadır. Bu

[10] Bilginin ifşa edilmesinin kuruluş veya birey üzerindeki etkisine göre ölçülmektedir.

kullanılan yollar özgünlüğünü ve/veya gerçekliği ispatlamış olmaktadır (Popescul, 2011: 1340).

İnkar etmeme ise, bir olay veya eylemin gerçekleşip gerçekleşmediğini ve kuruluşların ve/veya bireylerin olaya dahil olmasıyla, ilgili anlaşmazlıkları çözmek için iddia edilen bir olay veya eylemin ve onu oluşturan varlıkların gerçekleştiğini kanıtlama yeteneğini ifade etmektedir (Yiğitbaşı, 2015: 61).

Bilgi teknolojisi ve iletişimde inkar etmeme; veriyi gönderen kişiye teslimat kanıtı sağlandığını ve alıcıya gönderenin kimliğinin kanıtının verildiğini garanti etmektedir. Böylece daha sonra verileri işlediğini inkar edememektedir. Elektronik ticarette, dijital imzalar gerçekliği ve inkar etmemeyi sağlamak için kullanılmaktadır (Rohokale ve Prasad, 2016).

Bunların yanı sıra teknolojinin gelişimi ve bilgi depolamanın elektronik ortama geçmeye başlaması ile birlikte çoğu örgütsel faaliyetin de büyük ölçüde bilgi ve iletişim teknolojilerine bağlı olmasından dolayı Bilgi Sistemleri(BS) güvenliği modern işletmeler ve kuruluşlar için önemli bir endişe haline gelmektedir. BS güvenliğinin neredeyse her yönünü kapsayan çok sayıda araç ve mekanizma geliştirildi (İren ve Can, 2017: 27-28). Bununla birlikte, güvenlikle ilgili olayların hacmi ve buna bağlı mali kayıpların hacmi ve ciddiyeti artmaya devam ettiğinden, mevcut güvenlik çözümlerinin fiili etkinliği ciddi bir şekilde sorgulanmaktadır. Güvenliğin öncelikle bir "insan sorunu" ve bir "organizasyon sorunu" olması nedeniyle güvenlik araçları ve mekanizmaları sınırlı bir etkiye sahip olduğu için organizasyon bağlamında BS güvenlik yönetiminin önemi ortaya çıkmaktadır (Belsis, Kokolakis ve Kiountouzis, 2006: 189-190).

Nitekim bu sorunlar veri ve bilgi aktarımında yaşanan kolaylığın giderek artmasıyla birlikte Bilgi Sistemleri güvenliği daha da kritik hale dönüşmektedir. Kurumlarla birlikte bu kurumları oluşturan bireylerin ve bu kurumların hizmet ettiği bireylerin veri ve bilgilerinin korunması da zorlaşmaktadır. Ancak iyi bir bilgi sisteminin kurulması ve bu bilgi sistemlerinin güvenliğinde korunması gereken veri ve

bilgilerin sınırlarının iyi belirlenmesi gerekmektedir. Bu sebeple güvenlik sisteminin birey özelinde koruması gerekenin bilgi veya veri bağlamında iyi bir değerlendirilmesi yapılıp sınırlılıklarının da belirlenmesi gerekmektedir.

2.2. Kişisel Bilgi Çerçevesinde Korunma

Bilgi daha önce de belirtildiği gibi her çağda gücün önemli bir kaynağı olmuştur. Her dönemde tanımlanmaya çalışılmaktadır. Devletler düzeyinde önemli bilgilerin korunması elde edilmiş olan gücün de istikrarını işaret etmektedir. Devlete ait kritik bir bilginin korunamaması, devletlerin itibarlarında zarara yol açabilecek sonuçlar doğurabilmektedir. Fakat son yüzyıldaki teknolojik gelişimler devletlerle ilgili söz konusu bilgilerin korunmasını zorlaştırdığı kadar kişilere ait bilgilerinde korunmasında zorluklar meydana getirmektedir. Devletler sahip oldukları bilgileri koruyamadığı zaman ciddi zarara uğraması gibi kişiler de benzer şekilde kişisel zarara uğramaktadır (Bruyn, 2014).

Bundan dolayı, devletlerin ana aktör olarak hem kendi bilgisini hem de her bir vatandaşının kişisel bilgisini korumasının önemi her geçen gün artmaktadır. Teknolojinin getirdiği bilgi güvenliği zafiyetleri bu sorunun kesin bir çözüme ulaşmasını engellemektedir. Bu sebeple kişisel bilgilerin korunmasına yönelik yapılan düzenlemeler her geçen gün güncellenmekte ama yeterli olmamaktadır (Gürsel, 2016).

Bu çerçevede korunmanın ne demek olduğunun iyi anlaşılması ve korunma eyleminin kişisel bilginin korunmasında ne derece önemli olduğunun bilinmesi gerekmektedir. Bu sebeple korunmanın kavramsal ve kuramsal olarak değerlendirmesi yerinde olacaktır.

2.2.1. Kavramsal ve Kuramsal Olarak Korunma

TDK(2021)'a göre korunmak kelimesi "*kendini korumak, bir yere sığınmak, bir şeyden sakınmak ya da koruma işine konu olmak*" olarak tanımlanmaktadır. Korunma kavramı İngilizce Oxford (2021) sözlüğünde ise "*birinin ve/veya bir şeyin zarar görmediğinden, yaralanmadığından, hasar görmediğinden emin olmak*" şeklinde ifade edilmiştir. İngilizce' de koruma/korunma "protection" ile ifade

edilmektedir. 14. yy. ortalarında İngilizce' de "zarar veya yaralanmadan koruyan sığınak, savunma; muhafaza, vesayet, eylem veya koruma durumu" anlamındaki "protecciоun" kullanılmaktayken daha sonra Fransızcadaki "proteccion" kelimesi "protection, shield" olarak İngilizceyi etkilediği düşünülmektedir. Bunlardan önce ise İngilizcede koruma/korunma anlamında "beorgan" kullanılmaktaydı. Korunma dış veya iç etkenlerden gelebilecek veya gelme ihtimali olan zararlara karşı; kişilerin, kişilere ait bir malvarlığına ve kişilerin sorumlusu oldukları aile, arkadaş, akraba, mal varlığı vb. ilişkili olunan şeylerin bir zarara uğramasını engellemek olarak ifade edilebilmektedir (Graham ve Denning, 1972).

Son yüzyılla birlikte, korunma ve güvenlik ihtiyacı çeşitlilikler göstermeye başlamaktadır. Daha önceleri korunma çoğunlukla maddi saldırılara karşı gelebilecek zararlara konu olurken artık maddi ve manevi her alana karşı korunma süreçlerine yönelik düzenlemelerden oluşmaktadır. Örneğin; elektronik ortamlarda saklanan bilgilerin güvenliğinin sağlanması zorlaşmakta; risk ve tehditlerdeki değişime bağlı olarak her geçen gün daha karmaşık hale gelmektedir. Bununla beraber, internet ile beraber popülerlik kazanan sosyal ağlar ve e-ticaret alanlarının oluşması ile birlikte, kişisel verilerin korunması konusunda da sorunlar ve endişeler artmaktadır. Bu durum, hukuksal dayanakları da bulunan bilgi güvenliği yoluyla bilginin korunmasına yönelik önlemlerin alınmasını zorunlu hale getirmektedir. Bilgilerin ve kişisel bilgilerin korunmasına yönelik bilgi güvenliği önlemleri, bilginin elde edilmesinden imha edilmesine kadar olan tüm süreçler içerisinde aktif olan ve bilginin işlenmesinde rol alan tüm aktörlere belirli ölçülerde sorumluluk yükleyen bir güvenlik zincirini oluşturmaktadır. Bu nedenle etkin teknik önlemlerin yanı sıra, hukuksal sorumluluklar kapsamında veri ve bilgi sorumlusu olarak idari personelin de yükümlülüklerini yerine getirmeleri gerekmektedir (Henkoğlu, 2017: 47-48).

2.2.2. Bilginin Korunması ve Kişisel Bilginin Korunması

Birçok insan için bugünün dünyası, birçok yönden tehditlerle ve tehlikelerle dolu, güvensiz bir yer haline dönüşmektedir. Doğal afetler, şiddetli çatışmalar, kronik ve kalıcı yoksulluk, salgın hastalıklar, uluslararası terör, ani ekonomik ve mali krizler gibi önemli zorluklar meydana gelmektedir. Bunlardan dolayı ise sürdürülebilir kalkınma, barış ve istikrar için beklenti minimum düzeye düşmektedir. Bu tür krizler karışıklıklar meydana getirmesinin yanı sıra insanlara güvensiz bir yaşam alanı ve güvensiz toplumsal ilişkiler meydana getirmektedir. Nitekim güvensizliklerin oluşması ve katlanarak büyümesi insanların hayatlarının tüm yönlerine yayılabilmektedir. Bu sebeple topluluklar yok olabilmektedir ve bu his ulusal sınırların ötesini dahi aşabilmektedir. Bu sebeplerden dolayı bireylerin ve/veya toplumların korunma ihtiyacı doğmaktadır (United Nations, 2016: 5).

Özellikle son yüzyılın başlangıcı ile birlikte bu tehditlerin olma ihtimalleri, gelişmekte olan teknoloji ile doğru orantılı olarak artmaktadır. İster kurumsal olsun isterse bireysel olsun korunmaya duyulan ihtiyaç her geçen gün artarak ilerlemektedir. Nitekim korunma ihtiyacının temel insan haklarından ve temel gerçeklerden birisi olduğu temel gerçeklerden olduğu bilinmektedir. Bunlarla birlikte koruma ise, insan hakları hukuku, uluslararası insani hukuk (silahlı çatışma durumlarında geçerlidir) ve mülteci hukuku uyarınca bireyin haklarına tam saygıyı sağlamayı amaçlayan tüm faaliyetleri kapsamaktadır. Devletler, kendi yetki alanlarındaki insanları korumakta birincil sorumluluğa sahiptir. Ulusal makamlar doğal afet durumlarında etkilenenlere yardım ve koruma sağlamakla sorumludur. Silahlı çatışma durumlarında çatışmanın tüm tarafları yani devletler ve organize silahlı gruplar sivillere saygı göstermeli ve onları korumalıdır. Bu davranış biçimi, sivillerin savaşın etkilerinden kurtulmalarını ve yiyecek, tıbbi ve diğer temel hizmetlere erişimlerini sağlamayı içermektedir. Nitekim söz konusu koruma eyleminin son yüzyıl ile birlikte bilgi ve kişisel bilgiye yönelikte yapılması gerekliliği yadsınamaz gerçeklerden birisi olmaktadır (Eriksoon ve Giacomello, 2007).

Bundan dolayı devletler toplumu genel olarak korumanın yanı sıra her bir bireyin korunma hakkını özel olarak da koruyarak söz konusu bireylerin haklarını gözetmesi gerekmektedir. Devletler kişilerin ya da toplumların haklarını her türlü saldırıya ve gelecek herhangi bir zarara karşı koruması ilk önceliklerden olmalıdır. Teknolojinin hızlı gelişimi, bilgilerin aktarılmasında ve toplanmasında daha önce tahmin edilemeyecek boyutlara ulaşmasına sebep olmaktadır. Özellikle bilgisayar ve iletişim teknolojilerindeki ilerleme, kişilere ait bilgilerin korunmasını zorlaştırmaktadır. Bu koruma eyleminde devletlerin ana aktör olması temel yükümlülüklerinden birisi haline gelmektedir (Hanson ve Dunne, 2009).

Bilginin internet sayesinde kolay aktarılması bu durumun kontrol altına alınmasını neredeyse imkânsız hale getirmektedir. Nitekim bu teknolojik ortamlarda bilgilerin depolanması ve hızlı aktarımı, korunması gereken bilginin güvenliğini oldukça fazla tehdit etmektedir. Genel olarak tanımlanmakta olan bilginin yanı sıra kişisel bilginin korunamaması zafiyeti, sonuçları hesaplanamayan zararlara yol açmaktadır. Fakat çoğu kişisel bilgi sorumluları bireylere gelmesi mümkün olan zararlar hakkında çok bilgi sahibi olmadıkları için kişisel bilginin korunmasında bireysel yeterliliği ve hassasiyeti gösterememektedir. Söz konusu kişisel bilginin, sahibi tarafından korunması için kişilerin sahip oldukları bilgileri teknolojik ortamda paylaşımını veya aktarılmasını engelleyici tedbirleri almakta bilinçlenmeleri gerekmektedir. Buna örnek vermek gerekirse; sosyal medya sitelerine kayıt yapılırken kişilerin kendi verilerini veya kendilerine ait bilgileri bilinçsiz bir şekilde sosyal medya hesaplarına eklemeleri, sonuçları belirlenemeyen zararlara yol açabilmektedir. Örneğin; kişisel bilgilerin çalınması ile bir bankada kişi adına işlem yapılması söz konusu kişiye maddi ve manevi zarar vermektedir (Fabiano, 2019: 58-59).

Nitekim son yıllarda ülkeler bilgiyi ve kişisel bilgiyi korumaya yönelik hızlı adımlar atmaktadırlar. Fakat yaptırımların yeterince uygulanamaması dolayısı ile bu yapılan düzenlemelerin yetersiz kaldığı görülmektedir. Özellikle küresel boyuttaki şirketler bu düzenlemeleri sık sık göz ardı etmektedirler. Bu duruma Cambridge

Analitik Skandalı[11] ve son dönemde daha da sıklaşmakta olan kişisel bilgilerin rıza olmaksızın paylaşılması, sosyal medya uygulamalarında siber saldırılar yoluyla milyonlarca insanın bilgilerinin çalınması olayları verilebilecek örneklerden sadece birkaç tanesidir.

[11]Cambridge Analytica'nın 2014 yılında toplamaya başladığı yaklaşık 50 milyon Facebook kullanıcısının kişisel olarak tanımlanabilir bilgilerinin toplandığı bir veri ihlalidir. Elde edilen veriler, bu kişileri işe alan politikacılar adına seçmenlerin fikrini etkilemek için kullanıldı. İhlali takiben, Facebook, kamuoyundan özür diledi ve Cambridge Analytica'nın verileri uygunsuz bir şekilde topladığını belirtti. Ayrıca ihlal, Facebook'un hisse senetlerinin düşmesine neden oldu.

ÜÇÜNCÜ BÖLÜM
TÜRKİYE'DE VE İRLANDA'DA KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK BİR KARŞILAŞTIRMA

Bilgi güvenliğinin ve kişisel bilginin korunmasına yönelik tanımlamalar ve incelemeler, bilginin aşamalandırılması çerçevesinde kişiye ait bilgiyi; kişisel veri, kişisel enformasyon ve kişisel bilgi basamaklarına ayırarak bilgi ve kişisel bilgi arasındaki karmaşanın giderilmesinde önemli konuma sahiptir. Ancak bütün ülkelerin kişisel bilgiyi korumak için kişisel verileri korumaya yönelik düzenlemeler yapması, kavramın doğrudan kişisel veri üzerinden incelenmesini gerektirmektedir (Hallinan, Friedewald ve MvCarthy, 2012). Bununla birlikte son yıllarda yapılmakta olan veri korumaya yönelik düzenlemeler ve veri güvenliğine verilen önemin artması, bilgi güvenliği hakkında yapılması gereken düzenlemelerden birisi olmaktadır. Nitekim bu doğrultuda veri güvenliği ise "veritabanları gibi veri havuzunuzu güvenlik açığından, hatalı kullanımdan, yetkisiz erişim ve kullanımdan korumak" anlamına gelmektedir (Dhawan, 2014: 1).

Sanayi sonrası toplum düzenine geçişle birlikte bilgi ve iletişim teknolojilerinin (BİT) giderek yaygınlaşması kişisel verilerin toplanması, depolanması, işlenmesi ve dağıtılmasını önemli ölçüde kolaylaştırmaktadır. Veri işleme teknolojisindeki hızlı gelişim ise kamu ve özel sektörün kişisel verilere bakış açısında sürekli bir değişimi doğurmakta; veri koruma politikalarının ve veri güvenliğinin öneminin bu doğrultuda gelişmesini sağlamaktadır. Bundan dolayı kişisel verilerin korunması sorununun bir hukuki düzenleme alanı olarak ortaya çıkması bilgi güvenliğinin temelini oluşturmaktadır. BİT sayesinde hızla gelişen otomatik veri işleme teknolojisinin doğurduğu mahremiyet sorunları, ilk kez 1960'lı yılların sonlarında kişisel verilerin korunmasına yönelik kanunların ortaya çıkmasına neden olmuştur. Sanayi toplumundan bilgi toplumuna geçiş sürecini yaşamakta olan gelişmiş ülkelerde, başta Amerika Birleşik Devletleri (ABD) ve Avrupa Birliği (AB) ülkeleri olmak üzere bireysel hak ve özgürlüklerin zarar göreceğine ilişkin endişeler karşısında bu alanda hayata geçirilen hukuki düzenlemeler eliyle kişisel mahremiyetin korunması amaçlanmaktadır. Bu çerçevede bilgi toplumunun en temel sorunlarından birisi,

bireylerin devlet organları ve diğer kişiler karşısında özel yaşam alanlarına olan müdahalesinin önlenmesi ve kendileri hakkındaki verilerin işlenmesine ilişkin hukuki çerçevenin çizilmesini amaçlayan bir hukuk alanı ortaya çıkmaktadır (Akıncı, 2017:3).

Kişisel verilerin otomatik olarak işlenmesinin geliştirilmesi, işletmelerin kişisel veri toplama ve kullanımına yönelik artan eğilimiyle birlikte verimlilik, kalite ve üretkenlik gibi çeşitli toplumsal faydalar (hem organizasyon düzeyinde hem de bireysel yaşamlarda) anlamına gelmektedir. Öte yandan, bu evrimin aynı zamanda mahremiyet sorunları yarattığı da açıktır. Mahremiyet, batı ülkelerinde temel insan haklarından birisidir. Bu yüzden veri korunması, gizlilik ihtiyaçlarına yanıt veren ve bunlara uyum sağlayan mevzuat tarafından kontrol edilmektedir (Tikkinen-Piri, Rohunen ve Markkula, 2017: 2).

Bu bölümde de kişisel bilgiyi şemsiye kavram olarak esas alıp bu kavram altında korunması gereken kişisel veri hakkında yapılan yasal düzenlemeler, Türkiye ve İrlanda özelinde değerlendirilmektedir. Bunlarla birlikte kişisel verilerin korunmasına yönelik bakışın tarihsel süreç içerisindeki gelişmeleri incelenmektedir. Devamında ise kişisel verilerin korunmasına yönelik oluşturulan mevzuat ve kurumlara yönelik incelemelere yer verilmektedir. Son olarak ise bu iki ülkede kişisel verilerin korunmasına yönelik getirilen eleştiriler ele alınmıştır.

3.1. Türkiye'de ve İrlanda'da Kişisel Verilerin Korunmasına Bakış

Veri korumanın temel amacı, insan haklarının bir çeşidi olarak bireylere kişisel verileri üzerinde kontrol hakkı sağlamaktır. Bu bakış açısı, örneğin: Avrupa Birliği Temel Haklar Şartı'nda bulunabilir: "*Herkes, kendisi ile ilgili kişisel verilerin korunması hakkına sahiptir*" (Kneuper, 2019). Bundan dolayı evrensel olarak birçok ülke ve kuruluş, kişisel verilerin korunmasına yönelik çalışmalar yapmaya başlamıştır. Ayrıca ana sebeplerden bir diğeri ise gelişen teknolojiyle ortaya çıkan e-Ticaret sektörünü destekleyerek ticaretin yeni ve küresel pazar alanına güvenli ortamını sağlayarak sektörün gelişimini hızlandırma isteği olduğu iddia edilmektedir. Diğer bir neden ise, 95/46/AT sayılı Avrupa Birliği Yönergesi'nin şartlarından birisi olan kişisel

verilerin korunmasına ilişkin yeterli şartları sağlamayan ülkelere veri aktarımını yasaklamasıyla Avrupa Ülkeleri ile ticaret yapan ülkeleri kişisel verileri korumak için düzenlemeler yapmak zorunda bırakmıştır (Korkmaz, 2016: 83-84).

Bu doğrultuda ülkeler kişisel verilerin korunmasına yönelik olan çalışmalarını her geçen gün artırmaktadır. Birçok Asya ülkesinde de kişisel verileri korumaya yönelik düzenlemeler yapılmıştır. Bunlardan bazıları ise: 2016 tarihli Filipinler Veri Gizliliği Yasası; Singapur Kişisel Verileri Koruma Yasası; halihazırda tartışılan Hindistan Veri Koruma Yasası; Nepal'in 2007 tarihli Bilgi Edinme Hakkı Yasası biraz farklı odaklanmasına rağmen bir dizi benzer veri gizliliği düzenlemesini içermektedir. Yasal olarak bağlayıcı olmasa da AsiaPacific Economic Cooperation'ın APEC Gizlilik Çerçevesinde (APEC 2015) benzer gereksinimleri belirtmektedir. Bu farklı kanunlarda belirtilen gereksinimler aynı olmamaktadır. Ancak çoğu durumda oldukça benzer durumlar da içermektedir. Çin, burada "Sosyal Kredi Sistemi" ile bireylerin devlet tarafından gözetimini artırdığı için biraz farklı bir durumda bulunmaktadır. Fakat Bu Sosyal Kredi Sistemi, 2018 yılında uygulamaya konulan Avrupa Veri Gizliliği Standardı olan GDPR'ye benzer şekilde özel işletmeler için veri koruma gereksinimlerini de tanımlamaktadır (Greenleaf, 2017).

10 Aralık 1948 yılında Birleşmiş Milletler Genel Kurulu tarafından ilan edilen ve kabul edilen İnsan Hakları Evrensel Beyannamesi'ne göre, Sözleşme'nin 8. Maddesi üye devletlerin vatandaşlarının, özel hayatına ve aile hayatına, konuta ve haberleşmeye saygı hakkını güvence altına almaktadır (Birleşmiş Milletler, 1948). Bu sözleşmeyle birlikte veri korumasının yasal temeli oluşturulmuştur. Bu beyannameden sonra diğer kuruluşlar ve ülkeler de kendilerine göre yasal çerçeveyi oluşturmaya başlamışlardır (Weber, 2017: 2).

Avrupa'da ise; Avrupa İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Avrupa Sözleşmesi[12] 4 Kasım 1950 tarihinde Avrupa Konseyi tarafından hazırlanmış ve 1953'te yürürlüğe girmiştir (Avrupa Konseyi, 1950). Bu sözleşme de:

[12] Avrupa İnsan Hakları Sözleşmesi [AİHS] olarak bilinmektedir.

Temel özgürlüklerin korunmasının sağlanmaya çalışıldığı İnsan Hakları Evrensel Beyannamesi sekizinci maddesinde, konuyla ilişkili olan özel hayatı ve aile hayatını, konut ve haberleşmeşma haklarını koruma altına almaktadır. Kişisel verilerin korunması ile ilgili hazırlanan bu sözleşmeler, hukuksal düzenlemelerin yapılmasının yolunu açtı. 1960'lı yıllarda elektronik veri işleme alanındaki hızlı ilerleme, kamu idarelerinin ve büyük işletmelerin kapsamlı veri bankaları kurmasına ve kişisel verilerin toplanmasını, işlenmesini ve birbirine bağlanmasını iyileştirip artırmasını sağladı (Avrupa Konseyi, 2017). Bu süreç sonrasında bilgi gizliliği konusundaki tartışmalar yoğunlaşmaya başlamıştır. Böylece kişisel verilerin korunmasına yönelik ihtiyaç ortaya çıkmıştır. Burada özellikle kapsamı belirsiz olan özel hayatın yalnızca kamu makamlarının müdahalesine karşı korumaya yapılan vurgu artık yeterli görülmediğinden dolayı Avrupa Konseyi, hem özel hem de kamu sektöründeki kişisel verilerin haksız toplanmasını ve işlenmesini önlemek için belirli ilkeler ve normlar çerçevesi oluşturmaya başlamıştır (Tikkinen-Piri, Rohunen, ve Markkula, 2017: 2-3).

Avrupa'da daha sonra veri koruma ilkelerinin geliştirilmesine yönelik 1981 yılında (Avrupa Konseyi, 1981) Kişisel Verilerin Otomatik İşlenmesinde Bireylerin Korunmasına İlişkin Sözleşme'nin (Sözleşme 108) getirilmesi ve kabul edilmesi gerçekleştirilmiştir. Bununla birlikte sözleşmede belirtilen ilkelerin uygulanması için akit tarafların yerel yasalarına ilişkin gerekli önlemlerin alınması gerektiği vurgulanmıştır (Dove, 2019).

Avrupa Birliği üye devletlerinden olan Güney İrlanda Cumhuriyeti ve Avrupa Birliği üyeliğine aday statüsündeki Türkiye Cumhuriyeti kişisel verilerin korunmasına ilişkin hukuki çerçevelerini oluşturmaktadırlar. Bu hukuki çerçeveler ile birlikte kişisel verilerin korunmasına yönelik kurumsal yapılar kurulmaktadır (Tekin, 2014: 255). Bu yüzden İrlanda, 1988 yılında Veri Koruma Kanunu kabul edilmiştir. İrlanda, yapılan bu kanunun gerektirdiği koşulların oluşturulmasının yanı sıra bunların denetlenmesi için 1989 yılında Veri Koruma Komiserliği kurulmuştur. Bu süreç yıllar içinde değişiklikler gösterdikten sonra 2016 yılında yeni bir Veri Koruma Kanunun kabulü ile daha geniş bir çerçeveye yayılmıştır (Kearney, 2018).

Nitekim Güney İrlanda Cumhuriyeti'nin bu çalışmaya konu olarak seçilmesindeki amaç, IBM'in 1956'da bu ülkede bir merkez oluşturmasına takiben aşamalı olarak birçok teknoloji şirketlerinin de gelmesine sebep olmuştur. Teknoloji şirketlerinin İrlanda'daki varlıklarındaki asıl artışı; İrlanda hükümetinin "Doğrudan Yabancı Yatırımcı (DYY)" adlı vergi politikasıyla yabancı yatırımcıları ülkeye çekmek istemeleri ile başlamıştır. Ayrıca Google'ın 2003'te Dublin'de Avrupa Merkezini kurmaya karar vermesiyle birlikte Facebook, Microsoft, PayPal ve LinkedIn gibi birbirini izleyen ABD firmaları, Dublin'de EMEA[13] veya ABD dışı operasyonları için genel merkezlerin kurmuşlardır. İrlanda büyük teknoloji şirketlerinin merkezi haline gelmeye başlamıştır. Bu sebeple İrlanda mevcut durumda Microsoft, Dell, Intel, IBM, SAP, Facebook, LinkedIn, Twitter, HubSpot ve PayPal gibi dünyadaki en büyük teknoloji şirketlerinin önemli bir varlığına sahip olmaktadır. İrlanda'da bu küresel teknoloji şirketlerinin kurulmasıyla ya da kuruluşlarını tamamladıktan sonra yaklaşık 1000 teknoloji şirketi daha kurulmuştur. Bunlarla birlikte İrlanda Cumhuriyeti teknolojinin gelişimine ve söz konusu şirketlerin Avrupa merkezi haline gelmeye başlamasıyla ülke ihtiyaç duyulan yasal düzenlemeleri dünyadaki birçok ülkeye oranla daha sıkı yapmak durumunda kalmaktadır (Murphy, 2019: 72-73).

Türkiye'de ise kişisel verilerin korunmasına yönelik çalışmalar oldukça geç başlamıştır. Nitekim Avrupa Konseyi bünyesinde yapılmış olan 1 Ekim 1985 tarihli 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinden uzun yıllar sonra Türkiye'nin ilk düzenlemesini 2010 yılındaki referandum ile kabul edilen kanunla yapması Türkiye Cumhuriyeti'nin veri koruma konusunda geride kaldığını göstermektedir. Fakat son yıllarda yapılan düzenlemeler, kişisel verilerin korunmasına yönelik olan faaliyetleri artırmaktadır (Kılınç, 2012: 1092).

[13] Avrupa, Orta Doğu ve Afrika ya da orijinal adının sıkça kullanılan kısaltmasıyla EMEA (Europe, the Middle East and Africa), Avrupa, Orta Doğu ve Afrika'yı ifade eden kısa bir terimdir. Terim, kurumlar ve hükümetler, pazarlama ve iş dünyası tarafından kullanılır. Özellikle Kuzey Amerika'daki şirketler arasında yaygındır (https://worldpopulationreview.com).

İrlanda'ya yönelik uluslararası bazı görüşler de bulunmaktadır. Nitekim 1990'ların sonlarından itibaren İrlanda hükümeti, teknoloji şirketlerinin dikkatini çekmek için zararlı vergi politikaları yapmakla suçlanmıştır. Fakat bu vergi politikaları sonrasında ise birçok büyük teknoloji şirketi İrlanda'da merkezlerini kurmuştur. Bu sebeple İrlanda, Avrupa Birliği'nin teknoloji merkezi haline gelmiştir. Bundan dolayı tüm Avrupa Ülkesi vatandaşlarının da verilerinin korunmasında önemli bir konumda yer almaktadır. Örneğin, 2013'te Almanya Başbakanı Angela Merkel, İrlanda'yı Alman internet kullanıcılarının verilerini korumaktaki hatasından dolayı ulusal televizyonda "Almanya'da büyük veri koruma yasalarımız var. Ancak Facebook İrlanda merkezli olduğundan dolayı İrlanda yasaları geçerlidir" demiştir. Yeşil Parlamento Üyesi Jan Albrecht (2015) ise İrlanda'nın internet şirketlerini cezbetmedeki başarısını, İrlanda'da merkez kurmak isteyen BİT şirketleri için en yararlı koşulları oluşturan neo-liberal bir ucuzluk politikasına dayalı olarak açıklarken, bu vergi ve gizlilik unsurlarını birbirine bağlamıştır (McIntyre, 2020: 2).

Türkiye ise kişisel verilerin korunmasında ilk adımı, 1981 yılında Avrupa Konseyi tarafından hazırlanmış ilk bağlayıcı sözleşme olan Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'yi kabul etmesiyle başlamıştır. Fakat ulusal düzeyde yasalaşması uzun yıllar almıştır. 2008 yılındaki Avrupa Birliği İlerleme Raporuna göre: Kişisel verilerin korunmasına yönelik Türkiye'de tam bağımsız bir veri koruma kurumu kurulmasını ve Avrupa Veri Koruma Denetçisi (Eurpean Data Protection Supervisior-EDPS) gibi bir denetim mekanizmasının oluşturulması gerektiği belirtilmiştir. Avrupa Birliği, 2013 İlerleme Raporunda ise Türkiye'nin veri korunmasına yönelik bir çerçeve kanun bulundurmaması eleştirilmiş ve bu durumun AB ve Türkiye arasındaki ilişkilere zarar verdiği belirtilmiştir. Genel olarak, bu sebep dolayısıyla Türkiye'de kişisel verileri korumaya ilişkin bir kanun ve kurum ihtiyacının ciddiyeti anlaşılmıştır. (Kutlu ve Kahraman, 2017: 47-48).

3.2. Türkiye'de ve İrlanda'da Kişisel Verileri Koruma Mevzuatı ve Gerekçeleri

Türkiye'de ve İrlanda'da kişisel verilerin korunmasına ilişkin yapılmış olan mevzuat çalışmalarının temelinde Avrupa Birliği tarafından hazırlanan direktifler bulunmaktadır. Nitekim AB, asgari standartları ve parametreleri belirlemektedir. Ancak fiili uygulamayı devletlerin kendilerine bırakmaktadır. Bir direktif AB tarafından kabul edildiğinde her üye devletin kanun, yönetmelik veya başka bir girişim yoluyla belirlenen direktifi yürürlüğe koyması gereken bir son tarih de belirler. Bu tarihe göre, AB'ye üye devletler kendilerine uygun yasal çerçeveyi hazırlayıp yürürlüğe koymaktadırlar. Bunun yanı sırra 18 Aralık 2015 tarihinde Avrupa Birliği Daimi Temsilciler Komitesi, veri koruma reformu konusunda Avrupa Parlamentosu ile mutabık kalınan uzlaşma metinlerini onaylamıştır (Skendzic, Kovačić ve Tijan, 2018). Avrupa Konseyi, Parlamento ve Komisyon, 15 Aralık 2015'te nihai bir anlaşmaya vardı. Sonrasında ise Avrupa Parlamentosu, üzerinde anlaşmaya varılan metni 14 Nisan 2016'da onayladı. Yeni genel yönetmeliğin amacı ise insanların akıllı telefonlar, sosyal ağlar, çevrimiçi bankacılık ve küresel transferler dünyasında kendi özel verileri üzerinde daha fazla kontrol sağlamaktır. Kişilerin kişisel verilerinin işlenmesine ilişkin korunması, Avrupa Birliği Temel Haklar Şartı'nda (madde 8) ve Avrupa Birliği'nin işleyişi hakkındaki antlaşmada (madde 16) yer alan temel bir haktır (Voss, 2016).

Avrupa Birliği'nin hazırlamış olduğu Genel Veri Koruma Yönetmeliği'nin (GDPR) amacı, kişisel verilerin otomatikleştirilmiş yollarla işlenen veya işlenmeyen gerçek kişiler için veri koruma düzeyini iyileştirmek ve özellikle bürokrasiyi azaltarak tek bir dijital pazarda ticaret ve serbest dolaşım fırsatlarını artırmaktır (Skendzic, Kovačić ve Tijan, 2018). Avrupa Konseyi bu önemli reformunu ele alırken dikkate aldığı verilerin de belirtilmesi gerekmektedir. Nitekim Avrupalıların % 57'si kişisel verilerin ifşasının önemli bir konu olduğunu düşünmektedir. Ayrıca bu kişilerin yaklaşık % 70'i, bilgilerinin şirketler tarafından toplanmaktaki amaçları dışında kullanılmasına yönelik endişe duymaktadır. Sadece % 15'i çevrimiçi olarak sağladıkları bilgiler üzerinde tam kontrol sahibi olduklarını

düşünmektedirler. Avrupalıların % 90'ı AB'deki tüm ülkelerin aynı haklara ve korumaya sahip olmasının önemli olduğuna inanmaktadır (Avrupa Komisyonu, 2015). Bu oranlar sayesinde AB konseyi, kişisel veriler hakkında düzenlemeler yaparken daha imtinalı olduğu söylenebilmektedir (Díaz, 2016).

Türkiye'de ve İrlanda'da kişisel veri mevzuatı ve yönetmelikleri hazırlanırken, temelde AB tarafından hazırlanmış olan direktifler esas alınarak ulusal düzeyde düzenlemeler yapılmıştır. Nitekim İrlanda yapması gereken düzenlemeleri ivedilikle yapmasına rağmen Türkiye'de bu düzenlemelerin yapılması uzun zaman almıştır. Ancak Türkiye'de 7 Nisan 2016 tarihinde, kişisel verilerin korunmasına ilişkin 6698 sayılı özel bir kanunun yürürlüğe girmesiyle bu eksikliğin giderilmesinde büyük bir adım atılmıştır. Bu kanun, Türkiye'de hem kişisel verilerin korunmasını hem de kişisel verilerin korunmasına ilişkin 95/46/EC sayılı Avrupa Birliği Veri Koruma Direktifindeki standartları detaylı bir şekilde göz önüne alan ilk kanundur (Korkmaz, 2016: 84-85).

Bu kanun yürürlüğü girdiğinden beri kişisel verilerin korunmasında çeşitli adımlar atılmıştır. Bunlardan bazıları ise (Gün ve Partners, 2021):

- Kişisel Verileri Koruma Kurulu oluşturulmuştur;
- Kişisel Verileri Koruma Kanunu'nda yer verilen çeşitli kavramlara ilişkin bir takım kılavuzlar yayımlanmıştır;
- Kişisel Verileri Koruma Kurumu tarafından çeşitli yönetmelikler ve tebliğler (Türk kanunları uyarınca ikincil mevzuat sayılan) hazırlanmış ve 2017 ile 2018 yıllarında yürürlüğe konmuştur. Söz konusu yönetmelikler ile tebliğlerden en dikkat çekenleri şunlardır:
    - ✓ Veri Sorumlusu Sicili Yönetmeliği;
    - ✓ Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi hakkında yönetmelik;
    - ✓ Kişisel verileri koruma kurulu çalışma usul ve esaslarına dair yönetmelik;

- ✓ Aydınlatma yükümlülüğüne ilişkin tebliğ.

- Kişisel Verileri Koruma Kurumu, farklı konulara ışık tutmak amacıyla çeşitli rehberler hazırlamıştır. Söz konusu rehberlerden en dikkat çekenleri şunlardır:
  - ✓ Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler);
  - ✓ Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Rehberi;
  - ✓ Veri Envanteri Hazırlama Rehberi;
  - ✓ Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi.
- Kişisel Verileri Koruma Kurumu, veri ihlaline ilişkin kararlar ve ilkeler yayınlamıştır,
- Kişisel Verileri Koruma Kurumuna veri ihlali bildirimlerinde bulunulmuş ve bu bildirimler kamuya açıklanmıştır.

Nitekim Kişisel Verileri Koruma Kurumu, kişisel verilerin korunmasına ilişkin noksanlıkları gidermeye yönelik düzenli olarak kararlar ve ilke kararları yayınlamaya devam etmektedir.

Türkiye'nin Kişisel Verileri Koruma Kanunu yapmasına ivme kazandıran gerekçelerden birisi Avrupa Birliği 2013 İlerleme Raporudur. Bu raporda, Türkiye'nin veri korunmasına yönelik bir çerçeve kanun bulundurmamasının eleştirilmesi ve bu durumun AB ve Türkiye arasındaki ilişkilere zarar verdiğini belirtmesinden dolayı mevzuat eksikliğinin ciddiyeti anlaşılmış olmuştur. Bu durum sonrasında Türkiye'de ivedilikle mevzuat hazırlıkları başlamıştır (Kutlu ve Kahraman, 2017: 47-48).

Türkiye'de kişisel verilerin korunmasındaki önemli gerekçeleri, Kişisel Verileri Koruma Kanunu'nun (KVKK) hazırlanış amacı ele alınarak da belirlenebilmektedir. Söz konusu kanunun amacına göre (Kişisel Verileri Koruma Kurumu, 2016):

- Kişisel verilerin işlenmesinde, kişilerin temel hak ve özgürlüklerini korumak,

- Kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek (disiplin altına almak),
- Kişilerin mahremiyetini korumak,
- Kişisel veri güvenliğini sağlamak

olarak sayılmaktadır. Bu maddeler ele alınacak olursa kişisel verilerin önemi ve neden korunması gerektiğinin gerekçeleri belirlenmiş olmaktadır. İlk olarak kişinin temel hak ve özgürlüğünün korunması esas alınarak kişisel verinin, kişi rızası olmaksızın kayıt altına alınamayacağına vurgu yapılmaktadır. İkinci olarak da ilk maddesini destekler nitelikte yani kişisel verileri işleyen ve kayıt altına alan gerçek ve tüzel kişilerinde bir otorite hakimiyeti altında olduğunu bilmeleri; kişisel verileri bu çerçevede kanun dışı kayıt altına alınmaması gerektiğini; kişiyi ve kişiye ait verileri koruyarak kişinin temel hak ve özgürlüklerinin güvence altına alınması gerektiği yadsınamaz bir gerçektir.

Üçüncü olarak kişisel mahremiyetin korunması gerektiğini belirterek, kişisel verilerin korunmasının bir temel hak ve hürriyetlerden birisi olan mahremiyeti koruma şartının önemi belirtilmiştir. Bu nedenlere son olarak kişisel verinin kendisinin korunması gereken özel bilgi olduğunu belirtmek için ayrı bir madde de ele alınarak vurgulanmaktadır.

Avrupa Komisyonu tarafından Ocak 2012 tarhinde önerilen GDPR Nisan 2016 tarihinde Avrupa Parlamentosu tarafından kabul edilmiş ve 4 Mayıs 2016 tarihinde Avrupa Birliği Resmi Gazetesinde yayımlanmıştır. 25 Mayıs 2018 tarihinde o dönemdeki 28 AB üye devletinin tamamında uygulanmıştır (Houser ve Voss, 2018). İrlanda'da GDPR'yi desteklemek için Mayıs 2018'de yeni bir Veri Koruma Yasası da yürürlüğe koymuştur. GDPR kapsamındaki veri sahipleri, kişisel verilerinin işlenmesinde yönetmeliğin ihlal edildiğini düşünmeleri halinde denetim makamı olan DPC'ye (Veri Koruma Komisyonu (eski adıyla ODPC)) şikayette bulunma hakkına sahip olmaktadırlar. Bu sebeple Komisyondaki veri kontrolörleri ve işleyicileri, kişilerin verilerinin söz konusu yönetmeliğe uygun olmayan işlemlerle ihlal edildiğini

düşünmeleri halinde etkili adli çözüm bulmakla yükümlülükleri bulunmaktadır. Bunun yanı sıra DPC'nin "*işleme yasağını da içeren geçici veya kesin bir sınırlama getirme*" yetkisi vardır. Başka bir deyişle, kuruluşları etkin bir şekilde tamamen kapatma yetkisine sahiptir. Bundan dolayı DPC, hem GDPR hem de 2018 tarihli DPA' ya (Veri İşleme Sözleşmesi) göre, 20 milyon € 'ya kadar veya küresel yıllık cironun % 4'ü kadar idari para cezası uygulama yetkisi ile 1998 ve 2003 Veri Koruma Yasalarından çok daha yüksek cezalara sahip bir rejimle desteklenmektedir (Murphy, 2019).

İrlanda Veri Koruma Yasasının temel amaçları, Avrupadaki ve özellikle İrlanda'daki bireylerin kişisel bilgilerinin kötüye kullanılmasına veya yanlış kullanılmasına karşı korumak ve gerçek kişilerin temel hak ve özgürlüklerinden olan mahremiyet hakkı gereği kişisel verilerinin korunmasını sağlamaktır. Veri Koruma Yasası bunu iki şekilde yapmaktadır (Houser ve Voss, 2018):

- Bireyler için haklar tesis ederek;
- İşletmeler, kuruluşlar ve hükümet için sorumluluklar oluşturarak ve kişisel verileri, işleme ve saklama yöntemlerine ilişkin yönergeler belirleyerek.

Kişisel veriler, belirli bir kişiyi tanımlayan veya bu kişiyle ilgili açık bir şekilde hakkında olan bilgileri ifade etmektedir. Bu Veri Koruma Yasası ise anonim veya toplu verileri kapsamamaktadır. Kişilerin doğrudan veya dolaylı olarak tanımlamaya sebep olan verileri koruma altına almaktadır.

3.2.1. Türkiye'de ve İrlanda'da Kişisel Verileri Koruma Kanunları

Bir Avrupa ülkesi olan İrlanda' nın iç hukukuna getirilen ilk veri koruma mevzuatı 1988 tarihli Veri Koruma Yasasını, 1981 tarihli Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme sözleşme sonrasında oluşturmuştur. Bu yeni mevzuat, 1989 yılında ODPC'nin (Veri Koruma Komiseri Ofisi) kurulmasına sağlamıştır. 1995 yılında Avrupa Komisyonunun oluşturduğu Veri Koruma Direktifi (Direktif 95/46/EC), 2003 yılında yapılan bazı

değişikliklerle birlikte Veri Koruma Yasası olarak İrlanda iç hukukuna dahil olmuştur (MacIntyre, 1998).

Diğer bir ifade ile İrlanda Veri Koruma Yasası' nın kökeni, Kişisel Verilerin Otomatik İşlenmesiyle ilgili Bireylerin Korunmasına yönelik 1981 tarihli Avrupa Konseyi Sözleşmesine(Sözleşme 108) dayanmaktadır. Bu Avrupa Konseyi sözleşmesi kişisel verilerin korunmasına ilişkin yasal olarak bağlayıcı ilk uluslararası araçtır. 1981 tarihli Avrupa Konseyi sözleşmesi, AB Veri Koruma Direktifi(1995) ve Genel Veri Koruma Yönetmeliği (GDPR) (2016) için başlangıç noktası olmuştur. Bu yönetemelikler Sözleşme 108'den itibaren iki ana hedefi paylaşmaktadır. İlk olarak, ülkeler arasında kişisel verilerin serbest dolaşımını kolaylaştırmaktır. İkinci olarak ise gerçek kişilerin temel hak ve özgürlüklerinden doğan haklarıyla ilişkili olarak kişisel verilerin korunmasını sağlamaktır (Custers, vd., 2017).

Bu gelişmeler sonrasında Avrupa Birliği, verilerin nasıl toplandığını ve kullanıldığını düzenleyen, genel ilkeleri belirleyen, kapsamlı bir veri koruma yasasına (kamu kurumları veya belirli endüstri sektörleriyle sınırlı değildir) dayalı olarak dünya çapında etkili olduğu kanıtlanmış bir Avrupa veri gizliliği modeli ve bağımsız denetim otoritesini oluşturmuştur. (Newman, 2012). Bu model GDPR'ye kadar hala ulusal ayrışma için büyük bir alan bırakmıştır. Nitekim Sözleşme 108 ve Veri Koruma Direktifi doğrudan etkili olamamıştır. Bundan dolayı AB, yerel uygulama mevzuatının gerekliliğini belirtmiş ve nasıl uygulanacakları konusunda devletlere önemli ölçüde takdir yetkisi vermiştir. Bu takdir yetkisi ile AB'ye üye ülkeler arasında hem esasa ilişkin hem de usul kurallarına ilişkin önemli ölçüde farklılıklar meydana gelmiştir (Ducato, 2020).

İrlanda'da ise 25 Mayıs 2018'de yasalaşan 2018 sayılı Veri Koruma Yasası ile yeni bir Veri Koruma Komisyonu (DPC) kurulmuştur. Yeni Komisyon, bireyin kişisel verilerinin korunmasına ilişkin temel haklarının korunmasından sorumlu olan İrlanda'daki bağımsız ulusal denetim otoritesidir. Veri Koruma Komisyonu'nun yasal yetkileri, işleyişi ve görevleri Veri Koruma Yasası'ndan kaynaklanmaktadır. Genel

Veri Koruma Yönetmeliği ve Güvenlik Yönetmeliği'nin yanı sıra 1988 Veri Koruma kanunun ve 2003 yılındaki Avrupa sözleşmesine de dayanmaktadır (Murphy, 2019).

Türkiye'de ise kişisel verilerin korunmasına yönelik çalışmalar, İrlanda ve Avrupa Birliği'ne göre daha geç başlamıştır. Türkiye, Birleşmiş Milletler, Avrupa Konseyi, OECD gibi örgütlerin üyesi olmasına rağmen kişisel verilerin korunmasına yönelik uluslararası kuruluşlarca düzenlenen ve benimsenen ilkeleri Türkiye Cumhuriyeti'nin ulusal hukukuna aktaramamıştır. Avrupa Konseyi tarafından 1981 yılında imzalanan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına ilişkin 108 sayılı Sözleşme" Türkiye tarafından da imzalanmasına rağmen onaylanması 2016 yılına kadar ertelenmiştir (Hoşnut, 2019: 39).

Nitekim Kişisel verilerin korunmasıyla ilgili özel bir kanun hazırlamak için ilk komisyon 1989 yılında kurulmasına rağmen çalışmalarını tamamlayamamıştır. Daha sonra 2000 yılında kurulan ikinci komisyon tarafından üç yıllık çalışma sonucunda Kişisel Verilerin Korunması Kanun Tasarısı hazırlanmıştır. Adalet Bakanlığı tarafından 7 Eylül 2003 tarihinde açıklanan bu tasarı, Avrupa Birliği ilerleme raporları ve e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planları gibi çeşitli belgelerde yer almasına rağmen kanunlaşamamıştır. 2010 yılında yapılan bir referandum sonucunda, 5982 sayılı Kanun Anayasa'nın özel hayatın gizliliğini düzenleyen 20. maddesine "*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*" şeklinde bir fıkra eklenerek kişilerin kişisel verilerinin korunması açıkça anayasal güvence altına alınmaktadır (Korkmaz, 2016: 83).

Bu eklenen kanun fıkrasının esas alındığı Anayasa Mahkemesinin 9 Nisan 2014 tarih ve E:2013/122, K:2014/74 sayılı kararında: "*Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi*

hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması sonucunda, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması, terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artmasına sebep olabileceği" sebebiyle kişisel verilerin geçmişte olduğundan çok daha fazla korunmaya muhtaç olduğu ifade edilmektedir (Kişisel Verileri Koruma Kurumu, 2018).

Nitekim 24 Mart 2016 tarihinde ise Meclis Genel Kurulu'nda kabul edilen "6698 sayılı Kişisel Verilerin Korunması Kanunu" 7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Kanunun yürürlüğe girmesiyle Türkiye'de BİT(Bilgi ve İletişim Teknolojisi) sektörünün, başta AB ülkeleri olmak üzere yurt dışına bilgi toplumu hizmetleri sunabilmesi, kişisel verinin temel girdi olduğu finans, sağlık, sigorta gibi sektörlerde ülkenin iş potansiyelini artırması, sınır ötesi veri paylaşımı ve adli işbirliği kanallarının etkin çalışmasının sağlanması için büyük bir adım atılmıştır. Kişisel Verilerin Korunması Kanunu ile Türkiye' de AB ülkeleri nezdinde veri koruma bakımından güvenilir ülke statüsüne kavuşma konusunda önemli bir kriter yerine getirilmiştir.

3.2.2.Türkiye'de ve İrlanda'da Kişisel Verileri Koruma Yönetmelikleri

Türkiye'de ve İrlanda'da kişisel verilerin korunmasına ilişkin yapılmış olan kanun ve yönetmeliklerin temelinde AB kapsamında bireylerin verilerinin korunması ve gizliliği konularını düzenleyen ve sorumlusu olan 1995 tarihli Avrupa Birliği Veri Koruma Direktifi'nin (Directive 95/46/EC) yerini alacak olan Genel Veri Koruma Yönetmeliği (General Data Protection Regulation 2016/679) bulunmaktadır (Kneuper, 2019).

Genel Veri Koruma Yönetmeliği (GDPR), 25 Mayıs 2018'den itibaren geçerlilik kazanmıştır. Bundan dolayı AB kişisel verilerin işlenmesi için genel bir uygulamaya sahip olmuştur. Bu yönetmelikle beraber AB, veri denetleyicileri ve işlemciler veri güvenliği üzerinde daha kapsamlı yükümlülükler belirlemiş ve veri

sahipleri için güçlendirilmiş korumalar sağlamaktadır. GDPR, AB'ye üye devletlerde bir yasa olarak doğrudan uygulanabilir olmasına rağmen yönetmelikteki belirli konuların ulusal hukukta etkili olmasına izin vermektedir. Bu sebeple İrlanda'nın 2018 Veri Koruma Yasası da GDPR'den daha fazla etki sağlamaktadır (Ryngaert ve Taylor, 2020).

Avrupa'da ve özellikle İrlanda'da bazı durumlarda kişisel veri işlemenin niteliğine ve koşullarına, işlenen kişisel verilerin türüne veya veri koruma sorununun ne zaman ortaya çıktığına bağlı olarak, GDPR geçerli olmamaktadır. Bunun yerine, veri işlemenin düzenlenmesine ilişkin başka bir yasal çerçeve kişisel veriler için uygulanabilmektedir. Örneğin; bir veri koruma şikâyeti ve olası bir yasa ihlali, GDPR'nin 25 Mayıs 2018'de yürürlüğe girmesinden önce meydana gelen bir olayla ilgiliyse GDPR değil 1988 – 2003 Veri Koruma Kanunları geçerli olmaktadır.

Nitekim 25 Mayıs 2018 tarihinde yürürlüğe giren Veri Koruma Yasasıyla kurulan Veri Koruma Komisyonu, İrlanda'da denetleyeceği ve uygulayacağı veri koruma çerçevelerini belirlememektedir. Fakat GDPR, varsayılan olarak kişisel veri işlemenin çoğuna uygulanmaktadır. Ancak İrlanda'da belirli konulara ilişkin kuralların çoğunluğu 2018 tarihli Veri Koruma Yasası'nda belirtilmiştir (Clarke, vd., 2019).

2018 Veri Koruma Yasası ile birlikte ise GDPR yasasının 5. ve 6. bölümlerindeki Kanun Uygulama Direktifi, İrlanda yasalarına aktarılmıştır. Bu bölümlerdeki hükümler, kişisel verilerin ne gibi amaçlarla işlendiği durumlarda, cezai suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai yaptırımların infazı için yetkili veri sorumluları tarafından kişisel verilerin işlenmesine ilişkin İrlanda yasalarını düzenlemektedir.

Türkiye'de ise 2016 yılında kabul edilen Kişisel Verileri Koruma Kanunu'ndan sonra bazı yönetmelikler çıkarılarak veri korumasıyla ilişkili Anayasal ve Kanuni düzenlemeler yapılmıştır. Türkiye'deki bu yönetmelikler ise şunlardır:

- 28 Ekim 2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik;
- 30 Aralık 2017 tarihli Veri Sorumlusu Sicili Yönetmeliği;
- 16 Kasım 2017 tarihli Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esasları Hakkında Yönetmelik;
- 26 Nisan 2018 tarihli Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği;
- 5 Mayıs 2018 tarihli Kişisel Verileri Koruma Kurumu Personeli Teşvik ve Unvan Değişikliği Yönetmeliği;
- 9 Şubat 2018 tarihli Kişisel Verileri Koruma Uzman Yönetmeliği;
- 17 Mayıs 2019 tarihli Kişisel Verileri Koruma Kurumu Disiplin Amirleri Yönetmeliği;
- 21 Haziran 2019 tarihli Kişisel Sağlık Verileri Yönetmeliği.

Bu yönetmeliklerle birlikte, Kişisel Verileri Koruma Kanunu'nda ifade edilmeyen veri koruma yükümlülükleri tamamlanmaya çalışılmıştır.

3.3. Türkiye'de ve İrlanda'da Kişisel Verileri Koruma Kurumlarının Yapısı ve İşleyişleri

Tablo 1. Kurumsal Yapı

Türkiye/ Kişisel Verileri Koruma Kurumu	İrlanda/Veri koruma Komisyonu	Kurumların Özel Durumları
1 Başkan 1 Başkan Yardımcısı ve 8 Kurul üyesi bulunmaktadır.	1 Komiser ve 7 komiser yardımcısı bulunmaktadır.	İrlanda Veri Koruma Komisyonu 3 komiser ile yönetilebilmesi mümkündür. Fakat mevcut durumda 1 komiser bulunmaktadır. İhtiyaç olması durumunda 2 ek komiser atanabilmektedir. Yeni komiser atanması durumunda 1 başkan seçilecektir.
Kurum içerisinde 7 tane birim bulunmaktadır.	Kurum içerisinde 7 tane birim bulunmaktadır.	İrlanda Veri Koruma Komisyonu içerisinde bulunan 7 birim altında toplamda 42 alt birim daha bulunmaktadır.
25 Mayıs 2018 tarihinde Kişisel Verileri Koruma Kanunu'nun resmi gazetede ilan edilmesiyle kurulmuştur.	İlk olarak 1989 yılında Veri Koruma Komiserliği adı altında kurulmuştur. 2018 yılında kabul edilen Veri Koruma Yasası ile beraber Veri Koruma Komisyonu olarak isim değişikliği olmuştur.	
195 çalışanı bulunmaktadır.	145 çalışanı bulunmaktadır.	

Türkiye'de Kişisel Verileri Koruma Kurumu tablo 1'de belirtildiği gibi 25 Mayıs 2018 tarihinde Kişisel Verileri Koruma Kanunu'nun resmi gazetede ilan edilmesiyle kurulmuştur. Bu kurum; bir başkan, bir başkan yardımcısı ve yedi üyeden oluşmaktadır. Ayrıca toplam 195 çalışana sahiptir. Kurum, kanuna göre kendisine verilmiş olan görev ve yetkileri yerine getirmektedir. Kişisel Verileri Koruma Kurumunun üyelerinin görev süresi 4 yıl olsa da istisnai bir durumu da bulunmaktadır. Bu istisnaya göre ilk seçilmiş başkan, ikinci başkan ve kurayla belirlenmiş iki kurul üyesi altı yıl, geriye kalan beş üye dört yıl görev yapmaktadır. Kurul üyelerinin görev süreleri dolmadan görevleri sonlandırılamamaktadır. Üyelerin tekrar seçilme hakkı bulunmaktadır. Herhangi bir sebepten dolayı görev süresini doldurmadan görevi sonlanan üyenin yerine seçilen yeni üye, yerine seçildiği üyenin geriye kalan süresi kadar görev yapabilmektedir (KVK Kurumu, 2018).

Kurulun gündemi ve toplanacağı tarih başkan tarafından belirlenmektedir. Ayrıca başkan tarafından gerek görüldüğü takdirde kurulu olağanüstü toplama yetkisine de sahiptir. Toplantıdan en az üç gün önce gündemdeki 71 konuya ilişkin karar taslakları, kararın alınmasında gerekli olan dokümanlar ile kurumun görüşleri, İnceleme Dairesi Başkanlığı tarafından üyelere verilmektedir. En az altı üyenin katılımı ile gerçekleşecek kurulun, üyelerinin bütün toplantılara katılması istenmektedir. Ancak, Kurul üyeleri görüşülecek konunun kendileriyle, birinci, ikinci ve üçünü dereceden akraba, birinci ve ikinci dereceden kayın hısımlarıyla, evlatlıklarıyla ve eşleriyle veya eski eşleriyle ilişkili olması durumunda toplantı ve oylamaya katılamamaktadır. Bu durum da karar metninde belirtilmektedir. Ayrıca, toplantıya katılamayacak ve geçerli mazeretleri bulunan üyeler bu özürlerini başkanlığa bildirme sorumluluğu taşımaktadır (KVK Kurumu, 2018).

Toplantılar, çoğunlukla kurum merkezinde gerçekleşmesine rağmen ihtiyaç durumunda kurul tarafından başka bir yerde yapılmasına karar verilebilmektedir. Ancak, toplantının fiziki olarak gerçekleşmesi mümkün olmadığında, Başkanın

takdiriyle toplantı gereken güvenlik tedbirlerinin alınmasıyla elektronik ortamda yapılabilmektedir.

Kurul'da kararlar alınmadan önce konular, gündem sıralarına göre görüşülmektedir. Bu görüşmenin ardından, kararların alınması için üyeler, olumlu ya da olumsuz kararlarını el kaldırma şeklinde oylamada belirtmek zorundadır. Çünkü Kurul' da kararlar toplantıya katılan üye sayısının salt çoğunluğuyla verilmektedir. Toplantı sonunda alınan kararların tutanağı tutulmaktadır. Şayet varsa karşı oylar ve nedenleri de tutanağa yazılmaktadır. Kurul görüşmelerinin gizli kalması gerektiği için toplantılarda Başkan, üyeler ve görüşmenin tutanaklarını düzenleyen personel katılmaktadır. Ancak, ihtiyaç halinde Başkan, istisnai olarak tarafları, kişileri veya temsilcileri toplantıya davet edebilmektedir. Yine de kararlar alınırken toplantıya dışardan katılanlar bulunmamaktadır (Değirmenci, 2019).

İrlanda'da ise bu kurum Türkiye'ye göre çok daha önce kurulmuştur. Nitekim İrlanda Veri Koruma Komisyonu ilk olarak 1989 yılında Veri Koruma Komiserliği adı altında kurulmuştur. Bu kurum Tablo 1'de belirtildiği gibi 2018 yılında kabul edilen Veri Koruma Yasası ile beraber Veri Koruma Komisyonu olarak adlandırılmıştır (Voss, 2016).

Veri Koruma Komisyonu (DPC), AB ülkelerinin sınırları içerisinde yaşamakta olan bireylere ait kişisel verilerin korunmasına ilişkin temel hakları korumaktan sorumlu ulusal bağımsız denetim makamı olarak tanımlanmaktadır. DPC, Genel Veri Koruma Yönetmeliği'nin (GDPR) uygulanmasını denetleyen İrlanda'nın ulusal kurumudur. Ayrıca İrlanda'nın e-Gizlilik Düzenlemeleri (2011) ve Emniyet Yönergesi olarak bilinen AB Yönergesi dâhil olmak üzere diğer önemli düzenleyici çerçevelerden kaynaklanan işlev ve yetkileri bulunmaktadır. Bu komisyon yasal yetkilerini, işlevlerini ve görevlerini 2018 tarihli Veri Koruma Yasası, Genel Veri Koruma Yönetmeliği, Kanun Uygulama Yönergesi'nden ve ayrıca Avrupa Konseyi 108. Sözleşmesi'ni yürürlüğe sokan 1988 ile 2003 arasındaki Veri Koruma Yasalarından almaktadır (Kearney, 2018: 137).

İrlanda Veri Koruma Komisyonu son yıllarda çok fazla incelemeye konu olmaktadır. Bunun ana sebebi ise İrlanda Veri Koruma Komisyonu'nun (DPC), Avrupa'daki bireylerin kişisel verilerinin korunmasında Facebook, Google, Tiktok ve LinkedIn dâhil olmak üzere birçok küresel internet şirketinin denetimini Avrupa Birliği adına gerçekleştiren otorite olmasından dolayı önemli bir role sahiptir. Bu yüzden Avrupa Birliği, Veri Koruma Komisyonu'na 2018 yılında kabul edilen GDPR aracılığı ile Avrupa'nın veri koruma kurallarını ihlal eden şirketlere ve kurumlara küresel cirolarının yüzde 4'üne veya 20 milyon Avro'ya kadar (hangisi daha yüksekse) şirketlere ceza verme yetkisi vermektedir (McIntyre, 2020: 12).

2018 yılında kabul edilen İrlanda Veri Koruma Yasası ile Veri Koruma Komiseri Ofisi'nin yerini almak üzere Veri Koruma Komisyonu'nu kuruldu. Eski Veri Koruma Komiseri Helen Dixon, DPC'nin başkanı olarak görevine devam etmektedir. Fakat ofiste yapısal değişiklikler meydana gelmiştir. Bu değişiklik ile beraber komisyonun yönetiminin üç Veri Koruma Komiseri tarafından yönetilebilmesi mümkün olmasına rağmen Helen Dixon şimdilik tek Komiser olarak kurumu yönetmeye devam etmektedir. Ek komiserler atandığı zaman oylama gerektirebilecek durumlar için bir başkan belirlenecektir. Oireachtas[14], Avrupa Parlamentosu veya yerel otoritenin seçilmiş bir üyesi bu kuruma temsilcilik yapabilmektedir. Eğer ek komiser ataması yapılırsa da bu organlar içinden atama yapılacaktır. Ayrıca komiserin altında yedi tane komiser yardımcısı bulunmaktadır. Bu kurum veri koruma yasal çerçevelerine uygun olarak işlenen tüm kişisel verilerin veri denetleyicisidir. Ayrıca komisyon, içindeki ofisleri tarafından kişisel verilerin işlenmesini sağlamaktan sorumludur. Seçilmiş temsilciler ve bu temsilcilere yardımcı olan çalışanlar, kişisel verileri işlerken sorumluluklarının farkında olmalı ve çalışmaları sırasında veri koruma ilkelerine uymalarını sağlamak için prosedürler oluşturmaları gerekmektedir (https://www.dataprotection.ie/).

[14] İrlanda Yasama Organı, meclis.

Tablo 2. Kurumsal Karşılaştırma

	Türkiye Kişisel Verileri Koruma Kurumu			**İrlanda Veri Koruma Komisyonu**		
	2018	**2019**	**2020**	**2018**	**2019**	**2020**
Başvuru Adedi	1.084	2.280	2.297	4.113	9.337	10.151
Sonuçlandırılan	122	1.742	1.370	868	5.496	4.476
Değerlendirilmeye Devam Edilen	188	538	927	550	4.252	Veri yok
Yurtdışından Gelen Başvurular	774	1517	1281	136	457	354
Para Cezası Sayısı	8	24	91	Veri yok		
Uygulanmış Toplam Para Cezası(Birim Para)	870.000	13.105.828	21.390.000	715.000		

Türkiye'de Kişisel Verileri Koruma Kanunu'nun resmi gazetede yayınlanmasıyla kurulan Kişisel Verileri Koruma Kurumu ve İrlanda Veri Koruma Yasası ile birlikte ismi Veri Koruma Komisyonu olarak değiştirilen her iki kurum da 2018 yılında kurulmuşlardır. Bu sebeple tablo 2'de 2018 yılından başlanarak bir karşılaştırma yapılmıştır. İlk olarak bu kurumlara gelen veri mahremiyetini ihmale ilişki başvurulara bakıldığı zaman, kurumların toplumsal ilgiyi her geçen gün üzerlerine çektiği anlaşılabilmektedir. Bu ihlal başvuruları tablo 2'de görüldüğü gibi her yıl artmıştır. Bu durum hem toplumsal farkındalığın arttığı göstermekte hem de her iki ülkede de veri ihlallerinde yapılmış olan kanuni düzenlemelere rağmen artış olduğu görülmektedir (https://www.dataprotection.ie; https://www.kvkk.gov.tr).

Bunun yanı sıra bu artışları karşılaştırırken iki ülkenin de demografik durumunu göz ardı etmemek gerekmektedir. Çünkü Türkiye 83 milyon kişilik bir nüfusa sahipken İrlanda 4 milyon 904 bin kişilik bir nüfusa sahiptir. Ayrıca tablo 2'de de belirtildiği gibi bu iki kuruma gelen ihlal başvurularının bir bölümü yurtdışından gelmiştir. Bu sebeple kurumlara bildirilen ihlal sayılarına bakıldığı zaman yerel halkın, kişisel verilerin korunması ilişkin tam bir farkındalığı olduğu da iddia edilememektedir (https://www.worldometers.info).

DPC'nin bu üç yılda toplam uygulamış olduğu para cezasına bakıldığı zaman aşırı derecede iş dostu ve yaptırım açısından dişsiz olduğu için bazı eleştirilere maruz kalmaktadır. Fakat Veri Koruma Kanunu taraflar arasında dostane kararların alınmasının kolaylaştırılmasını desteklemektedir. Yine de yeni Veri Koruma Komisyonu'na mahkûmiyet ve yaptırımların ayrıntılarını yayımlama yetkisi de dâhil olmak üzere Komisyonun yetkilerini büyük ölçüde aşan, daha sağlam denetim ve yaptırım yetkileri sağlamaktadır. Veri Koruma Kanunu kapsamında verilen ek düzeltici yetkiler ile DPC'nin uygulama etkinliği algısının iyileştirilebileceği düşünülmektedir (Murphy, 2019: 73).

Türkiye'de üç yılda uygulanmış para cezalarına birim ve sayı olarak incelendiğinde İrlanda'ya göre yüksek miktarda ceza uygulamıştır. Bu durum kurumların ihlallerden dolayı çıkan anlaşmazlıkların İrlanda'da alınan dostane kararların sayısının daha çok olduğunu desteklemektedir.

3.4.Türkiye'de ve İrlanda'da Kişisel Verilerin Korunmasında Göz Önünde Bulundurulması Gereken Durumlar

Küreselleşmekte olan dünya düzeni dolayısıyla çeşitli işler ve eylemler elektronik ortamda gerçekleşmektedir. Bu eletronik ortam aracılığıyla gerçekleşen işlemlerden dolayı verilerin aktarımında ve biriktirilmesinde güvenlik sorunları oluşmaktadır. Elektronik ortamdaki zararlı yazılımlar ve bu yazılımları kullanan kişiler tarafından veri aktarım ve biriktirme sürecine yönelik olarak siber saldırılar gerçekleşmektedir. Fakat veriler sadece siber saldırılar aracılığı ile istismar edilmeyip

aynı zamanda verileri toplamakta olan özel şirketler tarafından da istismar edilmektedir. Verilere yönelik olan bu saldırılar özellikle kişisel verilere yönelik de olmaktadır. Kişisel verilere saldırıların olması ve kişi rızasıyla kişisel verilerini elinde bulunduran kurum ve kuruluşlar tarafından da zararlı yönlerde kullanılması bireyler üzerinde ciddi maddi ve manevi zararlı etkiler bırakmaktadır. Bu duruma Türkiye ve İrlanda özelinde bakıldığı zaman ise söz konu bu iki ülkede de benzer sorunlar meydana gelmektedir (Ducato, 2020).

Kişisel verilerin korunmasında yetkili devlet organları ve kamuoyu tarafından göz önünde bulundurulması gereken başlıca bazı durumlar incelenebilmektedir. Bunlar:

- Kişisel verilerin işlenmesinde alınan açık rıza sözleşmelerinin uzun ve karmaşık olması;
- Eğer açık rıza sözleşmesi yüzyüze yapılıyorsa işlemden sorumlu personelin açık rıza sözleşmesi yapan kişiye psikolojik baskısı;
- Kişisel verilerin paylaşımında, yanlış kişilere veya kurumlara elektronik posta gönderilmesi
- Kişisel verileri işlemesine izin verilen kurum ve ya kuruluşların verileri rıza gösterilen süreden daha fazla süre elinde tutması ya da hiç silmemesi;
- Kişisel verilerin korunmasına yönelik yapılmakta olan regülasyonların özel şirketler üzerinde etkisinin yetersizliği;
- Kişisel verilerin işlenmesinin ve aktarımının kontrol altına alınanaması;
- Kişisel veya kurumsal elektronik cihazlarda (Bigisayar, akıllı telefon, tablet vb.) saklanan kişisel verilerin siber saldırılardan korunamaması;

gibi durumlar yalnızca İrlanda ve Türkiye'de değil tüm dünyada göz önünde bulundurulması gerekmektedir.

Bu maddelerin birbirinden ayrı olarak açıklanması bu sorunların anlaşılmasına katkı sağlamaktadır. Bu sebeple, kişisel verilerin işlenmesi için gerekli olan açık rıza şartının sağlanması için oluşturulan sözleşmelerin, uzun ve karmaşık olması bireylerin

sözleşmeleri okumaktan kaçınmasına yol açmaktadır. Bununla birlikte doğması muhtemel olan maddi ve manevi zararların bilinmemesi kişisel güvenliğin sağlanmasında zorluklara da yol açmaktadır. Örneğin; bir bireyin kişisel verisinin işlenmesinde açık rıza göstererek sözleşmeye imza atması bireyin bilmediği ve farkında olmadığı bazı maddelere de onay vermesine yol açabilmektedir (Sharma, 2020).

Açık rıza sözleşmeleri yüz yüze yapılırken sözleşmeyi yapan kurum personelinin, müşteri üzerinde psikolojik baskı uygulayarak sözleşmeyi okumadan imzalatması etik kurallara aykırı olmaktadır. Bunun bir diğer örneği de anket çalışmalarında görülebilmektedir. Nitekim anket çalışması yapılırken anketörün profesyonel olmayan bir şekilde anket yapılan kişiye müdahalede bulunması anket sonucunu etkilediği gibi veri işlenmesinden doğabilecek zararların müşteriye bildirilememesine de yol açabilmektedir (Keser, 2020).

Diğer bir göz önünde bulundurulması gereken konu olarak, bireylerin ve kurum veya kuruluşların elektronik posta aracılığıyla veri paylaşımı yaparlarken e-posta adresinin yanlış yazması söz konusu bireylerin verilerinin kötü niyetli kişiler tarafından elde etmesine yol açabilmektedir (Kneuper, 2019).

Kişisel verileri işlemesine izin verilen kurum ve kuruluşların, bu verileri rıza gösterilen süreden daha uzun elde tutması ya da hiç silmemesi sebebiyle oluşması muhtemel zararların engellenememesi kişisel verilerin korunması konusunda göz önünde bulundurulması gereken konulardan biri olmaktadır.

Son yıllarda, küresel ekonomi adımlarıyla ortaya çıkan büyük şirketlerin kişisel verilerin korunmasında gerekli kurallara uymaması sıkça duyulan bir konudur. İster dünya genelinde olsun isterse Türkiye ve İrlanda özelinde olsun kişisel verilerin korunmasında alınan tedbirlerin büyük şirketleri çok etkilemediği yani bu şirketlerin kişisel verileri koruma politikalarını sık sık ihlal ettiği görülmektedir. Örneğin; son zamanlarda WhatsApp'ın gizlilik politikasındaki dayatmacı sözleşmesi, İrlanda ve Türkiye özelinde öne çıkmasının yanı sıra yaptırım uygulanmasına rağmen bu şirketin

kendi politikalarına devam etmesi, büyük şirketlerin veri koruma konusunda birey çıkarlarını gözetmediğini göstermektedir (Houser ve Voss, 2018).

Gelişen teknoloji ile birlikte veri aktarımının ve işlenmesinin hem hızlanması hem de kolaylaşmasıyla kişisel verilerin korunması da aynı derecede zorlaşmaktadır. Bunun kontrol altına alınamaması kişisel verileri elde eden teknoloji şirketlerinin kişisel enformasyon oluşturmasına sebep olmaktadır. Diğer bir ifade ile bir kişinin beğeni ve ilgi alanlarına yönelik algoritmalar oluşturulmasıyla hem şimdiki bireylerin hem de gelecekteki bireylerin özel yaşam alanlarına müdahale edilerek belirli grupların ya da şirketlerin isteklerine göre düşündürülmelerine ve yaşamalarına yol açabilecek ciddi zararlar oluşturmaktadır (Kutlu ve Kahraman, 2017).

Son olarak ise kişisel veya kurumsal elektronik cihazlarda (Bigisayar, akıllı telefon, tablet vb.) saklanan kişisel verilerin siber saldırılardan korunurken yapılan yetersiz güvenlik önlemleri, verilerin çalınmasına yol açmasıyla söz konusu bireylerin öngörülemeyecek maddi ve manevi zararlar görmesine sebep olmaktadır.

SONUÇ ve DEĞERLENDİRME

Bilgi kavramına bir felsefe disiplini olan epistemoloji açısından bakıldığında bilgi, öncelikle insana aittir; bilgi, insan bilgisidir. Böylece, epistemolojinin konusu olan bilgi, insanın kendi bilgisidir. Bu nedenle, böyle bir bilgi de genellikle akılsal ve zihinsel bir etkinlik olarak anlaşılmıştır. Bu çerçevede bakıldığı zaman "Niçin sadece insan bilgisi ele alınmıştır?" diye sorgulanmıştır. Çünkü insan önce kendi bilgi yetilerini, imkânlarını ve koşullarını inceleme gereksinimi duymaktadır. Bundan dolayı akıl sahibi insan, zihnin veya aklın gücünü kullanarak, bilgi nesnesinin verilerini kavramsal hale getirerek bilgiyi elde etmektedir. İnsan kendine ait olan bilgiye, bilginin nesnesi olan veriyi analiz ederek ulaşabilmektedir. Bilgi insana ait bir özellik olduğu için yalnızca insan bilebilmektedir (Çüçen, 2003: 3).

Daha önce sadece bilgi felsefesinin (epistemeloji) konusu olan bilgi, son yüzyılla birlikte Sosyoloji gibi esnek bilimlerden fizik gibi daha katı bilimlere kadar bütün bilim dallarının ilgi odağı olmuştur. Her bilim dalı kendi ihtiyacına göre tanımlama çalışması yapmıştır. Bu bağlamda ortak bir tanım oluşturulamamıştır. Bilgi anlamsal olarak dinamik bir yapıya sahip olduğu için bilginin tanımı da sürekli güncellenmektedir.

Nitekim bilginin daha iyi tanımlanması ve anlaşılması için kendi içerisinde aşamalandırılmıştır. Bu sebepten dolayı bilgi; "*veri, enformasyon ve bilgi*" olmak üzere ayrı aşamalarda değerlendirilmeye tutulmuştur. İlk olarak ikinci dünya savaşı sonunda bilgisayarın icadı ve bilgi depolama araçlarının gelişmesiyle depolanan işlem görmemiş veya bir analize dahil edilmemiş bilgi, veri olarak isimlendirilmiştir. Veri analiz etme, anlama ve kavrama yoluyla enformasyona dönüşmektedir. Enformasyon ise insanın sahip olduğu tecrübe, hayal yeteneği, analiz etme ve yorumlama vb. bireysel katkılarından geçtikten sonra bilgiye dönüşmektedir. Bunun sonucunda ise insan bilgeliğe ulaşmaktadır.

Bunun yanı sıra bilginin kendi içerisinde bir sınıflandırılması ihtiyacı doğmuştur. Çünkü sınıflandırma bir görme biçimidir. Sınıflandırma ile söz konusu

bilgiyi; en iyi durumda betimleme, açıklama, tahmin, buluşsal yöntemler ve yeni sorular üretilmesi ile belirli sınırlar oluşturulmaktadır. Hatta sınıflandırmalar karmaşık veya açık; bilgi yüklü veya basit olarak ortaya çıkarabilecekleri konusunda sınırlı olabilmektedir. Nitekim çeşitli sınıflandırma yapılarının özelliklerini anlamak yararlı olmaktadır. Böylece onların güçlü yanlarından faydalanabilmekte ve zayıf yönleri üzerinde çalışılabilmektedir.

Bunlarla birlikte bilginin daha iyi anlaşılması ve tanımlanmasını sağlamak için bilgi; kendi içerisinde bilgi ve kişisel bilgi olarak birbirinden ayrılmıştır. Kişisel bilgiyi ise bilginin aşamalandırılmasında olduğu gibi kişisel veri, kişisel enformasyon ve kişisel bilgi olarak ayrımı yapılmıştır. Böylece kişinin kendisi ile ilgili olan veya kişinin kendi üretimi olan bilgi ile hayatın akışında veya toplumsal düzeni sağlamakta, iyileştirmekte vb. durumlarda kullanılan bilgi birbirinden ayrılmıştır. Bundan dolayı kişisel bilgi ve bilgi arasındaki ayrım daha da belirginleşmiştir.

Bilgi insana ait olduğu gibi insanı tanımak için de bilgiye ihtiyaç vardır. Bu yüzden kişileri tanımak için kişi bilgisine gereksinim vardır. 20. yüzyılda teknolojik gelişmelerle kişisel bilginin aktarımı ve kayıt altına alınması kolaylaşmıştır. Bu sebeple güvenli veya güvensiz olduğu ölçülmeden aktarılan kişisel bilginin koruma altına alınması için gerekli hukuksal altyapı ve politika uygulamalarına ihtiyaç olduğunu söylemek mümkündür. Bu hukuksal altyapı ve politikalarla birlikte, toplumsal veya evrensel düzeyde erdem, etik, mahremiyet gibi kavramların da bireylere gönüllü olarak kabul ettirilmesi, kişisel bilgilerin korunmasındaki ana aktörlerden olduğu bilinmektedir.

Bunlarla birlikte kişisel bilgilerin korunması ve güvenliklerinin azami düzeyde sağlanması devletlere insan haklarının zorunlu tuttuğu bir durumdur. Bu sebeple birçok ülke gün geçtikçe kişisel bilgilerin korunmasına ilişkin önlemleri artırmaktadır. Fakat mevcut durumda dünya genelinde devletler “Kişisel Bilgilerin Korunması” olarak isimlendirmek yerine “Kişisel Verilerin Korunması” olarak isimlendirmektedir. Bunun için AB’de, Genel Veri Koruma Yönetmeliği (General Data Protection

Regulation 2016/679) ve AB kapsamında bireylerin verilerinin korunması ve gizliliği konularını düzenleyen ve sorumlusu olan 1995 tarihli Avrupa Birliği Veri Koruma Direktifi (Directive 95/46/EC) en etkili kişisel veri koruma düzenlemeleri olarak bilinmektedir. Bu düzenlemeler diğer birçok ulusal düzeyli yasanında temelini oluşturmaktadır. Bu yüzden Avrupa özelinde AB'ye bağlı bütün devletler, Avrupa Birliği tarafından çıkarılmış olan Genel Veri Koruma Yönetmeliği'ni (General Data Protection Regulation 2016/679) temel almak zorunda olmaktadır.

Türkiye'de ve İrlanda'da yapılan veri korumaya ilişkin düzenlemelerin temelinde Avrupa Birliği tarafından yayımlanmış olan Genel Veri Koruma Yönetmeliği (General Data Protection Regulation 2016/679) bulunmaktadır. Bu yönetmelikle birlikte ayrıca kendi mezuatının yanı sıra veri koruma kurumlarını da kurmuşlardır. İrlanda, iç hukukunda ilk veri koruma mevzuatını 1988 tarihinde Veri Koruma Yasasını 1981 tarihli AB'ye ait 108 sayılı sözleşme sonrasında oluşturmuştur. Bu yeni mevzuatla birlikte 1989 yılında ODPC'nin (Veri Koruma Komiseri Ofisi) kurulması sağlanmıştır. 1995 yılında Avrupa Komisyonunun oluşturduğu Veri Koruma Direktifi (Direktif 95/46/EC) 2003 yılında yapılan bazı değişikliklerle birlikte Veri Koruma Yasası olarak İrlanda iç hukukuna dahil olmuştur (MacIntyre, 1998; Bainbridge, 1996).

İrlanda'da 25 Mayıs 2018'de yürürlüğe giren 2018 sayılı Veri Koruma Yasası ile yeni bir Veri Koruma Komisyonu (DPC) kurulmuştur. Yeni Komisyon, bireyin kişisel verilerinin korunmasına ilişkin temel haklarının korunmasından sorumlu olan İrlanda'daki bağımsız ulusal denetim otoritesi olarak ifade edilmektedir. Veri Koruma Komisyonun yasal yetkileri, işleyişi ve görevleri Veri Koruma Yasası'ndan kaynaklanmaktadır. Veri koruma işlemleri, Genel Veri Koruma Yönetmeliği ve Güvenlik Yönetmeliği'nin yanı sıra 1988 Veri Koruma kanununa ve 2003 yılındaki Avrupa sözleşmesine de dayanmaktadır (Murphy, 2019).

Avrupa Konseyi tarafından 1981 yılında imzalanan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına ilişkin 108 sayılı

Sözleşme" Türkiye tarafından da imzalamasına rağmen kanunlaştırılması 2016 yılına kadar ertelenmiştir (Hoşnut, 2019: 39). 2012 yılında dört yıllık bir çalışma sonrasında 2016 yılında Kişisel Verileri Koruma Kanunu kabul edilmiştir. Bununla birlikte ise Kişisel Verileri Koruma Kurumu da kurulmuştur. Her iki ülkenin de mevcut durumda kişisel verilerin korunmasına yönelik hukuki altyapı ve düzenlemeleri sürekli değişen teknolojik sistemlere rağmen güncellenerek devam ettirilmektedir. Böylece veri korumaya ilişkin eksiklikler her geçen gün azalmaktadır. Fakat bu durum eksikliklere ilişkin eleştirilerin olmadığı anlamına gelmemektedir. Aksine eleştirilerin dikkate alınmasını ve daha fazla veri güvenliğine olan itimadın artırılması gerekliliğinin önemini vurgulamaktadır.

Sonuç olarak, bilginin ve kişisel bilginin tanımlanmasındaki anlam karmaşasının giderilmesi için bu kavram karmaşası gözönünde bulundurularak bilginin ve kişisel bilginin tanımlanmasının, her bilimsel disiplin tarafından ayrı ayrı dikkate alınması gerekmektedir. Çünkü bir kavramın temel tanımı yapılmadan diğer bir disipline uygulanması mümkün değildir. Özellikle bilgi güvenliği konusuyla birlikte bilginin ve kişisel bilginin korunmasında bu kavramsal ayrımların yapılması ile birlikte, korunması gereken bilginin sınırları daha belirgin hale gelecektir. Bu bağlamda, bilginin ve kişisel bilginin güvenliğinin sağlanmasında ve korunmasında önemli bir konuma sahip olan kişisel verilerin korunmasına ilişkin yapılmış olan düzenlemeler, Türkiye ve İrlanda açısından da çok daha önemli hale gelmiştir. Bu sebeple kişisel verilerin güvenliği ve korunmasına ilişkin yapılan ve yapılmak istenen düzenlemelerde kişisel verileri koruma mevzuatı ile korunmak istenen bilginin sınırlarının iyi belirlenmesi önem arz etmektedir. Nitekim, anlaşılmaktadır ki söz konusu ülkelerde de incelenen veri koruma düzenlemeleri, bilgi ve kişisel bilginin güvenliğini ve korunmasını mümkün hale getirmektedir. Ancak bu düzenlemelerin, bilgi ve kişisel bilginin güvenliğinin ve korunmasının sağlanmasında tam anlamıyla yeterli olduğu sonucuna ulaşmak da mümkün görünmemektedir. Hem Avrupa Birliği hem de ilgili ülkelerin bu konuda çok yönlü ve etraflı çalışmalar yapmaya devam etmesi gerektiği anlaşılmaktadır.

KAYNAKÇA

AĞIRALAN, Erkan. (2015). **Bilgi Güvenliği, Kişiisel Verilerin Korunması ve Mahremiyet Etki Değerlendirmesi**. Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü.

AHMAD, Shmmon, Ashak Kumar ve Abdul Hafeez (2019). "Importance of Data Integrity and Its Regulation in Pharmaceutical Industry", **The Pharma Innovation Journal**, Cilt. 8, Sayı. 1, ss. 306-313.

AKÇA, Gürsoy ve Doğa Başer (2011). "“Karanlığın Yokoluşu" Gelişen Teknolojinin Gizlilik ve Mahremiyet Üzerindeki Etkileri", **Muğla Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Sayı. 26, ss. 19-42.

AKINCI, Ayşe Nur (2017). **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, Ankara: İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Bilgi Toplumu Dairesi Başkanlığı.

AKTAN, Coşkun Can ve İstklal Yaşar Vural (2005). **Bilgi Çağında Bilgi Yönetimi**, Konya: Çizgi Kitapevi.

AKTAN, Coşkun Can ve İstiklal Yaşar Vural (2016). "Bilgi Toplumu, Yeni Temel Teknolojiler ve Yeni Ekonomi", **Yeni Türkiye**, Cilt. 1, Sayı. 88, ss. 1-37.

AL-KHOURİ, Ali M. (2012). "Data Ownership: Who Owns 'My Data'?", **International Journal of Management and Information Technology**, Cilt. 2, Sayı. 1.

ALTHOFF, Jochen, Dominick Berrens ve Tanja Pommerening (2019). **Finding, Inheriting or Borrowing? The Construction and Transfer of Knowledge in Antiquity and the Middle Ages**, Verlag, Bielefeld: Majuskel Medienproduktion gmbh.

ARENDS, J. Frederick (2009). "Homeros’dan Hobbes ve Ötesine: “Güvenlik”Kavramının Avrupa Geleneğindeki Boyutları", **Uluslararası İlişkiler**, Cilt. 6, Sayı. 22, ss. 3-33.

ARIKAN, Seda (2018). "Türkçede İkili Karşıtlık Kavramları Olarak “Erdem ve Kusur”", **Uluslararası Türkçe Edebiyat Kültür Eğitim Dergisi**, Cilt. 7, Sayı. 1, ss. 592-606.

ARSLAN , Ahmet (2012). **Felsefeye Giriş**, 16. Baskı. Ankara: Adres Yayınları.

ATILGAN, Doğan (2009). "Bilgi Yönetimi Kavramı ve Gelişimi", **Türk Kütüphaneciliği**, Cilt. 23, Sayı. 1, ss. 201-212.

AVANER, Elif (2018). "Mahremiyet Nedir? Mahremiyetin Sağlık Hizmetleri Penceresinden Görünürlüğü Nasıldır?", **Türkiye Biyoetik Dergisi**, Cilt. 5, Sayı. 3, ss. 110-116.

BAINBRIDGE, David (1996). **EC Data Protection Directive**, Butterworths , London.

BAKAN , Selahattin ve Şonay Şahin (2018). "Uluslararası Güvenlik Yaklaşımlarının Tarihsel Dönüşümü ve Yeni Tehditler", **The Journal of International Lingual, Social and Educational Sciences**, Cilt. 4, Sayı. 2, ss. 135-152.

BAYKARA, Muhammet, Resul Daş ve İsmail Karadoğan (2013). "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi", **1. International Symposium on Digital Forensics and Security**, ss. 231-240.

BEJCZY, Istvan P. Ve Richard G. Newhauser (2005). **Virtue and Ethics in the Twelfth Century**, Boston: Brill Yayınları.

BELSİS, Petros, Spyros Kokolakis ve Evangelos Kiountouzis (2006). "Information Systems Security from a Knowledge Management Perspective", **Information Management & Computer Security**, Cilt. 13, Sayı. 3, ss. 189-202.

BENNET, Alex ve David Bennet (2008). "The Depth of KNOWLEDGE: Surface, Shallow or Deep", Researchgate: https://www.researchgate.net (11.10.2020).

BERGERON, Bryan (2003). **Essentials of Knowledge Management**, New Jersey: John Wiley and Sons.

BIEN-KACALA, Agnieszka ve Maciej Serowaniec (2016). "Concept of Security and Its Types", **Security in V4 Constitutions and Political Practices**, ss.15-21.

BOEMCKEN , Marc von ve Conrad Schetter (2009). "Security", **Friedrich-Ebert-Stiftung**, ss. 1-5.

BROOKS, David Jonathan (2010). "What is Security: definition Through Knowledge Categorization, **Security Journal**, ss. 1-15.

BRUYN, Michelle de (2014). "The Protection Of Personal Information (POPI) Act - Impact On South Africa", **International Business & Economics Research Journal**, Cilt. 13, Sayı. 6, ss. 1315-1340.

BURGIN, Mark (2001). "Data, İnformation, and Knowledge", http://www.researchgate.net/publication/221584166_Data_Information_and_ Knowledge (Erişim Tarihi: 04.08.2019).

CABALLERO, Albert (2013). Information Security Essentials for IT Managers: Protecting Mission-Critical Systems, https://www.booksite.elsevier.com /samplechapters/9781597495332/02~Chapter_1.pdf (Erişim Tarihi: 10.02.2021).

CANBEK, Güral ve Şeref Sağıroğlu (2006). "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme" **Politeknik Dergisi**, Cilt. 9, Sayı. 3, ss. 165-174.

CANLIOĞLU, Gözde (2008). **Değişen Toplum Yapılarında Bilginin Değişen Konumu**, İstanbul: Marmara Üniversitesi.

CANSEVER, Belgin Arslan (2016). "Bilgi Toplumunda Bir Kavram Kargaşası: Bilgi mi? Enformasyon mu?", **Sosyoloji Dergisi**, ss. 41-50.

CLARKE, Niamh vd. (2019). "GDPR: an impediment to research?" **Irish Journal of Medical Science**, ss. 1129-1135.

CUSTERS, Bart vd. (2017). "A Comparison of Data Protection Legislation and Policies Across the EU", **Computer Law and Security Review**, Cilt. 34, Sayı. 2, ss. 234-243.

ÇEŞMECİ, Ümit Mustafa (2009). "Kriptoloji Tarihi", **TÜBİTAK ÜEKAE Dergisi**, Cilt. 1, Sayı. 1, ss. 20-31**.**

ÇİLİNGİR , Lokman (2014). **Felsefeye Giriş**, Ankara: Elis Yayınları.

ÇÜÇEN, Abdulkadir (2003). "Bilgi Kuramına Giriş", **Bilimname**, Sayı. 2, ss. 3-12.

DAWES, Gregory ve James Maclaurin (2012). "What is Religion?: Identifying the Explanandum", https://www.researchgate.net/publication/261216359_What_is_Religion_Identifying_the_Explanandum (Erişim Tarihi:12.05.2020), ss. 1-16.

Data Protection Commission: https://www.dataprotection.ie/ (Erişim Tarihi: 11.02.2020).

DEĞİRMENCİ, Samet (2019). "Avrupa Birliği Bağlamında Türkiye'de Kişisel Verileri Koruma Kurumu", Yüksek Lisans Tezi, Uşak Üniversitesi, Uşak.

Deloiitte, "Privacy and Data Protection in the age of Covid-19", Belçika, https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-risk_privacy-and-data-protection-in-the-age-of-covid-19.pdf (Erişim Tarihi:15.05.2021)

DHAWAN, Sandeep (2014). "Information and Data Security Concepts,Integrations, Limitations and Future", **International Journal of Advanced Information Science and Technology (IJAIST)**, Cilt. 1, Sayı. 2, ss. 1-6.

DIAZ, Efren D. (2016). "The new European Union General Regulation on Data Protection and the legal consequences for institutions", **Church, Communication and Culture**, Cilt. 1, Sayı. 1, ss. 206-239.

DOVE, Edward S. (2019). "The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era" **The Journal of Law, Medicine and Ethics**, Cilt. 46, Sayı. 4, ss. 1013-1030.

DUBOIS, J, ve N. Gershon (1996). **Data and Knowledge in a Changing World**, Paris: CODATA Secretariat.

DUCATO, Rossana (2020). "Data protection, scientific research, and the role of information", **Computer Law and Security Review**.

DURNA, Ufuk ve Yavuz Demirel (2008). "Bilgi Yönetiminde Bilgiyi Anlamak", **Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Sayı. 30, ss. 129-156.

ENGİN, Ali Osman (2005). "Bilginin İnsan Hayatındaki Yeri ve Önemi", **Kazım Karabekir Eğitim Fakültesi Dergisi,** Sayı. 11, ss. 427-453.

ERDEM, Engin İ. (2016). "İnsani Güvenlik Kavramı Bağlamında Çevre Güvenliği", **Gazi Akademik Bakış**, Cilt. 10, Sayı. 19, ss. 255-281.

ERDOĞAN , İbrahim (2013). "Küreselleşme Olgusu Bağlamında Yeni Güvenlik Algısı", **Gazi Akademik** Bakış, Cilt. 6, Sayı. 12, ss. 265-292.

ERIKSOON, Johan ve Giampiera Giacomello (2007). **International Relations and Security in the Digital Age**, Londra: Routledge.

EROĞLU, Şahika (2018). "Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi", **Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi**, Cilt. 35, Sayı. 2, ss. 130-153.

FABIANO, Nicola (2019). "Ethics and the Protection of Personal Data", **Systemics, Cybernetics And Informatics**, Cilt. 17, Sayı. 2, ss. 58-65.

FAIRWEATHER, Abral ve Linda Zagzebski (2001). **Virtue Epistemology: Essays on Epistemic Virtue and Responsibility**, New York: Oxford University Press.

FARABİ. (2001). **El-Medinetü'l Fazıla**, Çev. N. Danışman, Ankara: Milli Eğitim Bakanlığı.

FAYGANOĞLU, Pınar (2019). "Örtük Bilgi ve Örtük Bilgi Paylaşımının Örgütler için Enilikçilik ve Hayatta Kalma Açısından Önemi", **Uluslararası Sosyal Araştırmalar Dergisi**, Cilt. 12, Sayı. 63, ss. 1068-1074.

FELDMAN, Fred (1978). **Introductory Ethics**, Englewood Cliffs: Prentice Hall.

FINN, Rachel, David Wright ve Michael Friedewald (2013). "Seven Types of Privacy", **European Data Protection: Coming of Age**, ss. 1-26.

FLORIDI, Luciano (2011). **The Philosophy of Information**, New York: SPI Publisher Service.

FLORIDI, Luciano (2014). "Philosophical Conceptions of Information", https://www.researchgate.net/publication/220803995_Philosophical_Conceptions_of_Information (Erişim Tarihi: 12.05.2020).

FROOM, Eric (1994). **Erdem ve Mutluluk**, Çev. T. Yörükan, Ankara: Türkiye İş Bankası Kültür Yayınları.

GEISLER, Eliezer (2008). **Knowledge and Knowledge Systems: Learning from the Wonders of the Mind** . London: IGI Publishing .

GHAZIRI, Hassan ve Awad, Eliaz (2004). **Knowledge Management**, New Jersey: Prentice Hall Publicing.

GRAHAM, G. Scot ve Denning, Peter J. (1972). "Protection: principles and practice", A**ssociation for Computing Machinery**, ss. 417-429.

GREENLEAF, Graham (2017). **Asian Data Privacy Laws - Trade and Human Rights Perspectives**, Sydney: Oxford University Press.

GRUSCHKA, Nils, Vasileios Mavroeidis ve Kamer Vishi (2018). "Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR", https://www.researchgate.net/ (Erişim Tarihi: 02.03.2021).

GÜÇLÜ, Nezahat ve Sotirafski Kseanela (2006). "Bilgi Yönetimi", **Türk Eğitim Bilimleri Dergisi**, Cilt. 4, Sayı. 4, ss. 351-371.

GÜNAY, Durmuş (2019, 05 16). "Örtük Bilgi, Kendi Anlamının Kaderini Yaşar", http://hertaraf.com /haber-prof-dr-durmus-gunay-ortuk-bilgi-kendi-anlaminin-kaderini-yasar-1497 (Erişim Tarihi: 16.05.2019).

GÜRSEL, İlke (2016). "Protection of Personal Data in Internaional Law and the General Aspects of Turkish Data Protection Law", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt. 18, Sayı. 1, ss. 33-61.

HALLINAN, Dara, Michael Friedewald ve Paul mvcarthy (2012). "Citizens' perceptions of data protection and privacy in Europe", **Computer Law and Security Review**, Cilt. 28, Sayı. 3, ss. 263-272.

HAMMOND, Percy (2019). "Personal Knowledge and Human Creativity", http://polanyisociety.org/TAD%20WEB%20ARCHIVE/TAD30-2/TAD30-2-full-pdf.pdf#page=24 (Erişim Tarihi: 06.05.2020), ss.24-34.

HANSON, Marianne ve Tim Dunne (2009). "Human Rights in International Relations", http://www.researhgate.com/publication/43525803_Human_Rights_in_International_Relations (Erişim Tarhi: 20.10.2020), ss. 61-76.

HEADRİOK, Daniel R. (2006). **Enformasyon Çağı: Akıl ve Devrim Çağında Bilgi Teknolojileri 1700-1850**, Çev. Z. Kılıç, İstanbul: Kitap Yayın Evi.

HENKOĞLU , Türkay (2017). "Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme", **Türk Arşivciler Derneği Arşiv Dünyası Dergisi**, Cilt. 17, Sayı. 18, ss. 46-56.

HENKOĞLU, Türkay (2015). "Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler İle Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasinin Geliştirilmesi", Doktora Tezi, Hacettepe Üniversitesi, Ankara.

HESS, Charlotte ve Elinor Ostrom (2007). **Understanding Knowledge As a Commons From Teory to Practice**. Cambridge: MIT Yayınları.

HEY, Jonathan (2004). "The Data, Information, Knowledge, Wisdom Chain: The Metaphorical Link", https://www.jonohey.com/files/DIKW-chain-Hey-2004.pdf (Erişim Tarihi: 06.06.2020).

HİSARLIOĞLU, Fulya (2019). "Toplumsal Güvenlik", **Güvenlik Yazıları**.

HOEGL, Martin ve Anja Schulze (2005). "How to Support Knowledge Creation in New Product Development: An Investigation of Knowledge Management Methods", **European Management Journal**, Cilt. 23, Sayı. 3, ss. 263-273.

HOŞNUT, Yasime (2019). "Uluslararası Düzenlemelerde ve Türkiye'de Kişisel Verilerin Korunması", **Yeni Medya**, Sayı. 6, ss. 32-45.

HOUSER, Kimberly A. Ve W. Gregory Voss (2018). "GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy", **Richmond Journal of Law & Technology**.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en, "What is personal data?", (Erişim Tarihi: 20.05.2019).

https://www.dataprotection.ie (Erişim Tarihi: 20.07.2021).

http://www.disual.net/index.php/tr/hakkimizda/bizden-haberler/11-haberler/436-10-maddede-kisisel-verilerin-korunmasi-kanunu, 10 Maddede Kişisel Verilerin Korunması Kanunu, (Erişim Tarihi: 25.05.2019).

https://www.kvkk.gov.tr (Erişim Tarihi: 20.07.2021).

https://www.mevzuat.gov.tr (Erişim Tarihi: 07.05.2019).

https://www.worldometers.info (Erişim Tarihi: 15.07.2021).

https://www.worldpopulationreview.com/country-rankings/emea-countries (Erişim Tarihi: 12.04.2021).

ILVONEN, Ilova vd. (2015). "Knowledge security risk management in contemporary companies – toward a proactive approach" **48th Hawaii International Conference on System Sciences**, Hawaii: IEEE Computer Society, ss. 3941-3951.

International Baccalaureate Organization, “Theory of Knowledge Guide”, https://toktopics.files.wordpress.com/2020/02/tok-guide-from-2020.pdf

İNCE , Mehmet ve Ercan Oktay (2006). "Bilginin Bir Stratejik Güç Olarak Önemi ve Örgütlerde Bilgi Yönetimi", **Selçuk Üniversitesi Karaman İ.İ.B.F. Dergisi**, Cilt. 12, Sayı. 10, ss. 15-29.

İREN, Ecem ve Özgü Can (2017). "Bilgi Sistemlerinde Güncel Güvenlik Problemleri ve Önerilen Çözümler", **Tubav Bilim Dergisi**, Cilt. 10, Sayı. 2, ss. 27-42.

JAATINEN, Miia ve Rita Lavikka (2008). "Common Understanding as a Basis for Coordianation", **Corporate Communications: An International Journal**, Cilt. 13, Sayı. 2, ss. 147-167.

JAHNS, Gerhard (2006). "The History of Information Processing" , https://www.researchgate.net/publication/273895669_The_History_of_Information_Processing (Erişim Tarihi: 08.07.2020).

JENSEN, Hans Siggard (2000). "A History of the Concept of Knowledge", **Zagreb International Review of Economics and Business**, Cilt. 3, Sayı. 2, ss. 1-16.

JOUINI, Mouna, Latifa A. Rabai ve Anis Ben Aisa (2014). "Classification Of Security Threats in İnformation Systems", **Science Direct**, Sayı. 32, ss. 489-496.

KARP , Peter ve David Wilkins (1989). **An Analysis of the Distinction Between Deep and Shallow Experts System**, Urbana: İllionis Üniversitesi.

KEARNEY, Sarah (2018). "Data Protection and Privacy for Media and Individuals Under Irish and EU Law", **Irish Communications Review**, Cilt. 16, Sayı. 1, ss. 136-146.

KESER, Yıldırım (2020). "Tüketicinin Kişisel Versinin İşlenmesinde Açık Rıza", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Cilt. 28, Sayı. 3, ss. 1181-1215.

KESGİN, Ahmet (2009). "Etik Üstüne", **Dini Araştırmalar**, Cilt. 12, Sayı. 35, ss. 143-160.

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

KİRSH, D. (2009). "Knowledge, Explicit vs Implicit", **Oxford Companion to Consciousness**, ss. 397-402.

Kişisel Verileri Koruma Kurumu (2018). **100 Soruda Kişisel Verilerin Korunması Kanunu**, Ankara: KVKK Yayınları.

Kişisel Verileri Koruma Kurumu (2018). https://www.kvkk.gov.tr/ (Erişim Tarihi: 10.06.2019)

KNEUPER, Ralf (2019). "Data Protectıon In The Eu And Its Implıcatıons On Software Development Outsıde The EU", **Journal of Institute of Science and Technology**, Cilt. 1, Sayı. 24, ss. 1-5.

KORKMAZ, İbrahim (2016). "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", **Türkiye Barolar Birliği Dergisi**, Sayı. 124, ss. 81-152.

KRANICH, Nancy (2003). "The Information Commons - A Public Policy Report", https://www.researchgate.net/publication/42764447_The_Information_Commons_A_Public_Policy_Report (Erişim Tarihi: 13.09.2020).

KURT, Ali Osman ve Mehmet Emin Güler (2017). "Anadolu'da İlk Tapınak: Göbeklitepe", **Cumhuriyet İlahiyat Dergisi,** Cilt. 21, Sayı. 2, ss. 1107-1138.

KUTLU, Önder ve Selçuk Kahraman (2017). "Türkiye'de Kişisel Verilerin Korunmasının Analizi", **Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi**, Cilt. 5, Sayı. 4, ss 45-62.

LEE, Wanbil L., Wolfgang Zankl ve Henry Chang (2016). "An Ethical Approach to Data Privacy Protection", **Isaca Journal**, Sayı. 6, ss. 1-9.

LUKÁCS, Andrienn(2016). "What is Privacy? The History and Definition of Privacy", https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf (Erişim Tarihi: 13.03.2021), ss. 256-265.

MACINTYRE, Alasdair (1998). **A Short History of Ethics-A History of Moral Philosophy from the Homeric Age to the Twentieth Century**. Londra: Routledge and Kegan Paul Ltd.

MACLELLAN, Effie ve Rebecca Soden (2007). "The Significance of Knowledge in Learning: A Psychologically Informed Analysis of Higher Education Students' Perceptions", **International Journal for the Scholarship of Teaching and Learning**, Cilt. 1, Sayı. 1.

MADDEN, Andrev D. (2000). "A Definition of Information", **Aslib Proceedings**, Cilt. 52, Sayı. 9, ss. 343-349.

MANUNTA, Govanni (1999). "What is Security", **Security Journal**, ss. 57-67.

MASLOW, Abraham H. (1943). "A Theory of Human Motivation", **Psychological Review**, Sayı. 50, ss. 370-396.

MCDOWELL, John (1979). "Virtue and Reason", **Oxford Journals**, Cilt. 62, Sayı. 3, ss. 331-350.

MCINTYRE, Dr. Tj (2020). **Regulating the Information Society: Data Protection and Ireland's Internet Industry**, The Oxford Handbook of Irish Politics.

MEDENİ, İhsan Tolga ve Ziya Aktaş (2019). "Veri Toplumundan Bilgi Toplumuna Dört Düzeyli Bir Toplum Modeli", http://www.emo.org.tr/ekler/fdac58e60abb571_ek.pdf (Erişim Tarihi: 15.09.2019).

MÉNARD, Martine C. (2006). "Privacy Protection Through Security", **Privacy Protection for E-Services**, Ed. G. Yee, Londra: Idea Group Publishing, ss. 115-140

MENON, Sudhan (2007). "Human security: Concept and practice", Ahmedabad, https://www.researchgate.net/publication/24113083_Human_security_Concept_and_practice (Erişim Tarihi: 05.01.2021).

MERT, Muhit (2003). "Kelamcıların Bilgi Yanımları Üzerine Bir Tahlil Denemesi", **Ankara Üniversitesi İlahiyat Fakültesi Dergisi**, Sayı. 1, ss. 41-67.

MIILARD, Christopher ve Kuan Hon (2011). "Defining 'Personal Data' in e-Social Science", https://www.researchgate.net/publication/228280110_Defining_'Personal_Data'_in_eSocial_Science#:~:text='processing'.,identification%20number%20or%20to%20one (Erişim Tarihi: 20.09.2020).

MONTOLİO, Daniela ve Elissa Trujillo (2012). "What Drives İnvestment İn Telecommunications? The Role Of Regulation, Firms' İnternationalization And Market Knowledge". **Documents de Treball de l'ıeb**.

MOOR, James H. (1990). "The Ethics of Privacy Protection", **Library Trends**, Cilt. 39, Sayı. 1, ss. 69-82.

MURPHY, Maria Helen (2019). "The Irish Adaptation of The GDPR: The Irish Data Protection Act 2018", **Blog Droit Europeén**, ss. 72-79.

NALBANTOĞLU, Lerzan ve Asilhan Özkaya (2019). "Kişisel Verilerin Korunması: Bilinmesi Gerekenler", https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/legal/KisiselVeriler.pdf (Erişim Tarihi: 25.10.2020).

ORMAN, Enver. "Bilgi Felsefesi", **İstanbul Üniversitesi Açık ve Uzaktan Eğitim Fakültesi**, http://auzefkitap.istanbul.edu.tr/kitap/felsefe_ao/bilgifelsefesi.pdf (Erişim Tarihi: 12.06.2020).

ÖSTLING, Johan vd. (2018). "Circulation of Knowledge: Explorations in the History of Knowledge", https://www.academia.edu/35557992/The_history_of_knowledge_and_the_circulation_of_knowledge_An_introduction (Erişim Tarihi: 02.01.2021), ss. 9-33.

ÖZKARAL, Tuğba Cevriyeli (2015). "Eskiçağda Yazı, Kitap ve Kütüphanenin Oluşum Süreci; Günümüz Eğitimine Katkıları", **Selçuk Üniversitesi Edebiyat Fakültesi Dergisi**, Sayı.34, ss.371-384.

ÖZKEÇECİ, İlhan, Nesli Gül Durukan ve Hakan Alacalı (2018). "XVII-XIX. Yüzyıllarda Osmanlı Dönemi Konut Mimarisinde İç Mekân Tavan Süslemelerine Genel Bir Bakışı", **İnsan&insan**, ss. 214-232.

ÖZSAĞIR, Arif (2008). "Bilgi Üretimi ve Bilginin Ürüne Dönüştürülmesinde Teknoparkların Önemi", **Mevzuat Dergisi**, Cilt. 11 Sayı. 125.

PAYAM, Mehmet Murat (2018). "Emniyet, Güvenlik, Kent Emniyeti ve Kent Güvenliği: Kavramsal Bir Analiz", **Avrasya Terim Dergisi**, Cilt. 6, Sayı: 1, ss. 15-25.

https://mytok.blog/2020/06/20/aok-history/. "Personal Knowledge: Historical Background", (Erişim Tarihi: 12.05.2019).

POLANYI, Michael (1966). "The Logic of Tacit Inference" **Philosophy**, ss. 1-18.

POLANYI, Micheal (2005). "Personal Knowledge Towards a Post-Critical Philosophy", **Routledge & Kegan Paul Ltd**.

POPESCUL, Daniela (2011). "The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation. Innovation and Knowledge Management, A Global Competitive Advantage", **Kuala Lumpur, Malaysia: Proceedings of The 16th International Business Information Management Association Conference**, ss. 1338-1345.

POWELL, Rahada (2012). "The Concept of Security", **Socia-Legal Review,** https://www.researchgate.net/publication/263662107_Security (Erişim Tarihi: 12.07.2020) .

PROSSER, William L. (1960). "Privacy", **California Law Review**, Cilt. 48, Sayı. 3, ss. 383-423.

RICH, Karen. "Introduction to Ethics", ss. 3-31, https://samples.jbpub.com/9781449649005/22183_CH01_Pass3.pdf (Erişim Tarihi: 04.05.2021).

ROHOKALE, Vandana ve Prasad, Ramjee (2016). "Cyber Security for Smart Grid - The Backbone of Social Economy", **Journal of Cyber Security**, Sayı. 5, ss. 55-76.

ROTHSCHİLD, Emma (1995). "What is Security", **The MIT Press**, Cilt. 124, Sayı. 3, ss. 53-98.

RUKANCI , Fatih ve Hakan Anameriç. "Bilgi Toplumu ve Toplumun Bilgilenmesinde Kütüphanelerin Rolü", https://www.researchgate.net/ publication/28808417_Bilgi_Toplumu_ve_Toplumun_Bilgilenmesinde_Kutuphanelerin_Rolu (Erişim Tarihi:04.05.2020) ss. 1-11.

RYNGAERT, Cedric ve Mistale Taylor (2020). "The GDPR As Global Data Protection Regulation?" **American Journal of International Law**, Sayı. 114, ss. 5-9.

SANCAK , Kadir (2015). "Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenlğin Dönüşümü", **Sosyal Bilimler Dergisi**, ss. 123-134.

SATIJA, Mohinder P. (2015)." Information, Knowledge, Wisdom: A Progressive a Value Added Chain", **International Journal of Knowledge Content Development & Technology**, Cilt. 5, Sayı. 2, ss. 65-74.

SCARDAMALİA, Marlene ve Carl Bereiter (2010). "A Brief History of Knowledge Building", **Canadian Journal of Learning and Technology**, Cilt. 36, Sayı. 1.

SHARMA, Sanjay (2020). **Data Privacy and GDPR Handbook**. New Jersey: John Wiley and Sons Yayınevi.

SHI, Yue (2018). "Data Security and Privacy Protection in Public Cloud", https://www.researchgate.net/publication/329705635 (Erişim Tarihi: 20.02.2021).

SKENDZIC, Aleksandar, Bozidar Kovačić ve Edward Tijan (2018). "General data protection regulation - Protection of personal data in an organisation", https://www.researchgate.net/publication/326708317_General_data_protection_regulation_-_Protection_of_personal_data_in_an_organisation (Erişim Tarihi: 15.03.2021).

SOKHANVAR, Shahran, Judy Matthews ve Prasad Yarlagadda (2014). "Importance of Knowledge Management Processes in a Project-based organization: a Case Study of Research Enterprise", **12th Global Congress on Manufacturing and Management,** ss. 1825-1830.

SOLOVE, Daniel J., Neil M. Richards (2010). "Prosser's Privacy Law: A Mix acy Law: A Mixed Legacy ed Legacy", **California Law Review**, Sayı. 98, ss. 1887-1924.

SCHUMAKER , Peter P. (2011). "From Data to Wisdom: The Progression of Computational Learning in Text Mining", **Communications of the IIMA**, Cilt. 1, Sayı. 11, ss. 38-48.

TAN, Charlene ve Lachlana Crawford (2006). "Knowledge and Inquiry: An Introduction to Epistemology". **Prentice Hall**.

TEKİN, Nurullah (2014). "Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", **T.C. Uyuşmazlık Mahkemesi**, ss. 222-262.

TEKİN, Ömer Akgün vd. (2012). "Beş Faktör Kişilik Özellikleri Ve Örgütsel Çatışma Yönetimi Arasındaki İlişkiler: Ankara'daki Beş Yıldızlı Otel İşletmeleri Üzerine Bir Uygulama", **Journal of Yasar University**, Cilt. 7, Sayı. 27, ss. 4611-4641.

TENNIS , Joseph T. (2008). "Epistemology, Theory, and Methodology in Knowledge Organization: Toward a Classification, Metatheory and Research Framework", **The Information School of the University of Washington**, ss. 102-112.

TIKKINEN-PIRI, C., Rohunen, A., & Markkula, J. (2017). "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies", **Computer Law and Security Review**.

TORUN, Zeynep (2017). "Doktrinde İnsan Güvenliği Kavramı: Destekleyenler ve Eleştirenler", **Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt. 19, Sayı. 1, ss. 223-241.

TÖRE, Nazlı (2007). "Sanal Ortamda Telif Haklarına Uygulanacak Hukuk", **TBB Dergisi**, Sayı. 72, ss. 297-326.

Türk Dil Kurumu: http://www.tdk.gov.tr (Erişim Tarihi: 12.08.2020).

TRIPODI, Leandro (2019). "Five Laws of Ethics", http://www.researchgate.com/publication/325253974_Five_Laws_of_Ethics (Erişim Tarihi: 25.01.2021).

UÇAK, Nazan Özenç (2010). "Bilgi: Çok Yüzlü Bir Kavram", **Türk Kütüphaneciliği,** Cilt. 24, Sayı. 4, ss. 705-722.

UÇAK, Nazan Özenç (2000). "Bilgi Üzerine Kuramsal Bir yaklaşım", **Bilgi Dünyası**, Cilt. 1, Sayı. 1, ss. 143-159.

UĞRAŞ, Tuğba (2015). "Bilgi Tüketicileri ve Üreticileri", **Bilgi yönetimi, Bilgi Üreticileri, Büyük Veri, İnovasyon ve Kurumsal Zeka**, Ed: Sevinç Gülseçen, İstanbul, Ankara, İzmir, Adana, Papatya Bilim Üniversite Yayıncılığı, ss. 17-29.

UĞUZ, Ayşegül (2016)." Liberalizmde Güvenlik Kavramı ve Uluslararası Güvenliğe Getirilen Çözümler", **V. Türkiye Lisansüstü Çalışmaları Kongresi - Bildiriler Kitabı II**, ss. 85-98.

United Nations. (2016). "Human Security Handbook/An integrated approach for the realization of the Sustainable Development Goals and the priority areas of the international community and the United Nations system", **United Nations**.

USANMAZ, Baran. "Kişisel Verilerin Korunması Neden Önemlidir?", http://www.halklailiskiler.com.tr/Kisisel_verilerin_korunmasi_neden_onemlidir..php (Erişim Tarihi: 02.12.2019)

ÜNAL, Yenal (2009). "Bilgi Toplumunun Tarihçesi", **Tarih Okulu,** Sayı. 5, ss.123-144.

VAN, Mert. "Kişisel Verilerin Korunması", http://www.wyg.com.tr/Portals/0/KVKK_Brosur.pdf (Erişim Tarihi: 15.05.2019).

VOSS, W. Gregory (2016). European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. The Business Lawyer(72), 221-233.

VURAL , Çağla (2018). "Çevresel Güvenliğin Gelişimi", **Ankara Üniversitesi Çevre Bilimleri Dergisi**, ss. 20-38.

WEBER, Mark C. (2017). "Protection for Privacy under the United Nations Convention on the Rights of Persons with Disabilities", **Laws**, Cilt. 6, Sayı. 10.

WONG, Rebecca (2012). "The Data Protection Directive 95/46/EC: Idealisms and Realisms", https://www.researchgate.net/publication/228120853_The_Data_Protection_Directive_9546EC_Idealisms_and_Realisms (Erişim Tarihi: 21.03.2021).

YİĞİTBAŞI, İsmet (2015). "Bilginin Korunması", **Bilgi Yönetimi,Bilgi Türeticileri, Büyük Veri, İnovasyon ve Kurumsal Zeka**, Ed: S. Gülseçen, İstanbul: Papatya Yayıncılık. Ss. 57-78.

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

YOUNG, James O. (2001). **Art and Knowledge**, London: Routledge Yayınları.

YÜKSEL, Mehmet (2003). "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi", **Ankara Üniversitesi SBF Dergisi**, Cilt. 58, sayı. 1, ss. 181-213.