



**KTO KARATAY
ÜNİVERSİTESİ**

T. C.
KTO Karatay Üniversitesi
Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı Yüksek Lisans Programı

**TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI
HAKKI**

Nur Halet AVCIOĞLU

KONYA
Temmuz, 2018

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI HAKKI

KTO Karatay Üniversitesi Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı Yüksek Lisans Programı

Nur Halet AVCIOĞLU

Tez Danışmanı
Dr. Hikmet TÜLEN

Yüksek Lisans Tezi
KONYA, 2018

KABUL VE ONAY

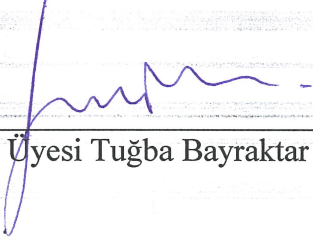
Nur Halet AVCIOĞLU tarafından hazırlanan “Türk Hukukunda Kişisel Verilerin Korunması Hakkı” başlıklı bu çalışma, 23/07/2018 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından yüksek lisans tezi olarak kabul edilmiştir.



Dr. Öğr. Üyesi Hikmet Tülen (Danışman)

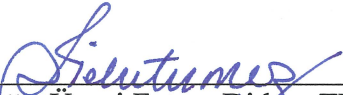


Dr. Öğr. Üyesi Ayşegül Çoban Atik



Dr. Öğr. Üyesi Tuğba Bayraktar


Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.



Dr. Öğr. Üyesi Fatma Didem TUNÇEZ
Enstitü Müdürü V.

ETİK BEYAN

KTO Karatay Üniversitesi Sosyal Bilimler Enstitüsü Tez/Proje Hazırlama ve Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İmza

Temmuz,2018

Nur Halet AVCIOĞLU

TEŐEKKÜR

Çaędaő yaőamda benlięini tım geliőmelere karőı korumak zorunda olan modern insanın kendine ait tım kodları hassas biçimde koruması ve korumak istemesi oldukça doęaldır. Bu durumda devletler, sistemler ve dięer bireylere karőı benlięini oluőturan verileri koruma refleksinin hukuk dzenlerinde yer bulmasıyla insan; kiőisel verilerin korunması hakkına, bu hakkın gereklilięine ve bu gereklilięin yasalaőmasına adım adım Őahit olmuőtur.

Bu çalıőmamızda bireyin kendine özgü çemberinin esasları olan kiőisel/hassas veri kavramını açıkladık. Çalıőmada bu kavramın temelinde geliően kiőisel verilerin korunması hakkı ve de bu hakkın ulusal ve uluslararası dzenlemelerdeki yeri ve dzenlemeleri üzerinde duruldu.

Çalıőmanın srekli geliőmekte olan kiőisel veri hakkı ve bu hakkın çevresinde geliően kiőisel veri hukukuna ynelik geliőmeleri ve uygulamaları anlatmaya çalıőan bir bakıő aşıyla yazıldıęını belirtmek isterim. Bu alanda yapılan ve yapılacak çalıőmaların Tırkiye'nin insan hakları aşıından devamlı devinim halinde ve çaęa ayak uydurmak aşıından olumlu geliőmeler gosterir vaziyette olmasını saęlayacaktır.

Nur Halet AVCIOęLU

ÖZET

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI HAKKI

AVCIOĞLU, Nur Halet
Yüksek Lisans, Kamu Hukuku Bölümü
Tez Danışmanı: Dr. Hikmet TÜLEN
Temmuz, 2018

Küreselleşme ile birlikte, veri yayılımı daha kolay hale gelmiş bu durum kişilerin en temel haklarından biri olan kişisel verilerini koruma hakkını da riske atmıştır. Bu durum kişisel verilerin korunması için ulusal ve uluslararası düzenlemeleri de zorunlu hale getirmiştir. Bu çalışmanın amacı Türk hukukunda kişisel verilerin korunması hakkı için yapılan düzenlemeleri incelemektir. Yapılan incelemeler neticesinde Türkiye'nin bu düzenlemeleri yapmak konusunda dünyanın diğer ülkelerine göre epey geç kaldığı görülmüştür. Yapılan kanuni değişiklik ise yalnızca özel sektörde kişisel verilerin işlenmesini kapsamaktadır. Çalışmada kanunun etkilerine ilişkin bir anket ya da mülakat yapılmamış, konu hakkında literatür taraması sunulmuştur.

Anahtar Kelimeler: Kişi, Kişi Hakkı, Hukuk, Kişisel Veri

ABSTRACT

RIGHT OF PROTECTING THE PERSONAL DATA IN TURKISH LAW

AVCIOĞLU, Nur Halet
Master of Public Law
Supervisor: Dr. Hikmet TÜLEN
July 2018

With the globalization the information expansion has been very easy and this has been caused risk about the right of personal data protection. This situation showed that international and national legislates should be done for protection the human right. The goal of this study is to survey the legal arrangements in Turkey about the protection of personal data. The research showed that Turkey is a bit late about the arrangements according to other countries. The regulation only frames the private sector's personal information records. The study does not contain a questionnaire or an interview ,literature review presented about the subject.

Keywords: Person, Personal Right, Law, Personal Data

İÇİNDEKİLER

KABUL VE ONAY	i
ETİK BEYAN.....	ii
ÖNSÖZ	Hata! Yer işareti tanımlanmamış.
ÖZET.....	iv
ABSTRACT.....	v
KISALTMALAR LİSTESİ.....	x
TABLolar LİSTESİ.....	xi
ŞEKİLLER LİSTESİ	xii
GİRİŞ	1
__1. BÖLÜM	4
__KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASI.....	4
__1.1. Kişisel Veri Kavramı.....	4
__1.1.1. Kişisel Veri Tanımı.....	4
__1.1.2. Kişisel Verinin Unsurları	6
____1.1.2.1. Veri.....	8
____1.1.2.2. Bilgi.....	9
____1.1.3.3. Kişisel Veri Ve Kişilik Hakkının Temelindeki Unsurlar.....	9
1.2. Veri Hukukunda Kişi Kavramı	11
__1.2.1. Kişi.....	11
__1.2.2. Veri Hukukunda Kişi Ayrımı.....	12
1.3. Kişisel Verilerin İşlenmesi.....	12
1.4. Kişisel Verilerin Korunması	13
1.4.1. Kişisel Verilerin Korunması Hakkının Hukuki Niteliği	15

1.4.1.1. Mülkiyet Hakkı Görüşü.....	16
1.4.1.2. Fikri Mülkiyet Hakkı Görüşü.....	16
1.4.1.3. Özel Hayatın Gizliliği Hakkı Ve Kişisel Verilerin Korunması	17
1.5. Hak Kavramı	18
1.6. Yasal Düzenleme Kavramı	18
1.7. Özel Hayatın Gizliliği Hakkı Ve Kişisel Verilerin Korunması Gereksinimi..	19
1.7.1. Genel Olarak	19
1.7.2. Özel Hayatın Gizliliği Hakkı	21
1.7.2.1. Düşünce Özgürlüğü.....	22
1.7.2.2. Bilgi Edinme Hakkı.....	22
1.7.3. Kişisel Verilerin Korunmasının Nedenleri ve Gereksinimi.....	23
1.7.3.1. Gözetim ve Denetim	25
1.7.3.2. Teknolojideki Gelişmeler.....	26
1.8. Kişisel Verilerin Korunması Bağlamında Temel İlkelerin İncelenmesi	26
1.8.1. Kişisel Verilerin Hukuka Uygun İşlenmesi İlkesi	27
1.8.2. Kişisel Verinin İşlenmesinde İlgilinin Bilgilendirilmesi İlkesi	27
1.8.3. Kişisel Verilerin İşlenmesinde Bilgi Edinme, Düzeltme, Sildirme, Engelleme Hakkı İlkesi	29
1.8.4. Veri Güvenliği İlkesi.....	30
1.8.5. Amaçla Bağlılık İlkesi.....	30
1.8.6. Ölçülülük İlkesi.....	32
1.8.7. Sorumluluk İlkesi	33
<u>2. BÖLÜM</u>	<u>34</u>
<u>KİŞİSEL VERİ HUKUKU, ULUSLARARASI DÜZENLEMELER VE TÜRK HUKUKUNDAKİ YERİ</u>	<u>34</u>
2.1. Kişisel Veri Hukukunun Tarihsel Gelişimi.....	34

2.1. Genel Olarak	35
2.2. Uluslararası Belgelerde Kişisel Verilerin Korunmasına İlişkin Temel Düzenlemeler	36
2.2.1. Temel İnsan Haklarında Düzenlenmesi	37
2.2.2. Ekonomik İş birliği ve Kalkınma Teşkilatı (OECD)	38
2.2.3. Avrupa Konseyi ve Avrupa Birliği	41
2.2.4. Birleşmiş Milletler	46
2.3. Ulusal hukukta kişisel verilerin korunması hakkı.....	49
2.3.1. Anayasal Düzenleme.....	50
2.3.2. Uluslararası Yükümlülükler.....	51
2.3.3. Kanuni Düzenlemeler	54
2.3.3.1.Genel Olarak	54
2.3.3.2. Kişisel Verilerin Korunması Kanun Tasarısı	54
2.3.3.3. 6698 Sayılı Kişisel Verilerin Korunması Kanunu	60
2.3.3.4. Diğer Kanunlarda Kişisel Verilerin Korunması Hakkı.....	68
2.3.4. Yönetmelikler.....	76
2.4. Kişisel Verileri Koruma Kurum ve Kurulu.....	80
2.4.1. Kurul'un Çalışma Esasları	81
2.4.2. Kurul'un Görevleri.....	82
2.4.3. Kurum Tarihçesi, Başkan ve Üyeleri	83
2.5. 5237 Sayılı Türk Ceza Kanunu'na Göre Kişisel Verilerin Korunmasına İlişkin Suç Tipleri.....	84
2.5.1. Kişisel Verilerin Kaydedilmesi Suçu (Md. 135).....	85
2.5.2. Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu (Md.136)	85
2.5.3. Verilerin Yok Edilmemesi Suçu (Md.138)	86
2.6. Kişisel Verilerin Korunmasına İlişkin Anayasa Mahkemesi Kararları.....	86

SONUÇ	89
KAYNAKÇA.....	93
ÖZGEÇMİŞ	100



KISALTMALAR LİSTESİ

AK	: Avrupa Konseyi
BM	: Birleşmiş Milletler
EC	: European Control
KVKK	: Kişisel Verileri Koruma Kanunu
Md.	: Madde
MÜHF-HAD	: Marmara Üniversitesi Hukuk Fakültesi -Hukuk Araştırma Dergisi
OECD	: The Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Örgütü)
AÜSBF	:Ankara Üniversitesi Siyasal Bilgiler Fakültesi
TAAD	:Türkiye Adalet Akademisi Dergisi
TBB	: Türkiye Barolar Birliği Dergisi
TCK	:Türk Ceza Kanunu
TDK	: Türk Dil Kurumu
S.K.	: Sayılı Kanun

TABLÖLAR LİSTESİ

Tablo 1. Kişisel Verilerin Korunmasına İlişkin Uluslararası Yasal Düzenlemeler ...	36
Tablo 2. Kişisel Verilerin Korunmasına İlişkin Ulusal Düzenlemeler	50



ŞEKİLLER LİSTESİ

Şekil 1. Kişisel Veriler	5
Şekil 2. Özel Nitelikli Kişisel Veri/ Hassa Veri/Duyarlı Veri	6
Şekil 3. Kişisel Verileri Korumanın İşletmelere Sağladığı Avantajlar	24
Şekil 4. OECD, AK ve BM Bünyesinde Kişisel Verilere İlişkin Yapılan Yasal Düzenlemeler	35
Şekil 5. AK Bakanlar Komitesi Tavsiye Kararları.....	42



GİRİŞ

Kişi, ister gerçek, isterse tüzel olsun; kendine ait doğal haklara sahiptir. Bunlardan ilki kuşkusuz varlığını sürdürme/ yaşama hakkıdır. Kişisel verilerinin hukuka aykırı olarak alınması ve/veya paylaşılması onun yaşamını tehdit eden boyutlara varabilecektir. Örneğin bir kadının bedeni ile ilgili bir bilginin paylaşılması, namus cinayetlerine neden olabilmektedir. Ya da bir şirketin muhasebe bilgilerinin paylaşılması spekülasyonları ve hatta iflası beraberinde getirebilecektir.

Benzer biçimde kişilerin bilgi edinme hakkı, bedensel bütünlüğünü koruma hakkı, özel hayatını gizli tutma hakkı vardır ve bunlar temel kişilik haklarıdır. Temel kişilik hakları hem ulusal düzeyde yasalar ve ilgili mevzuat, hem de uluslararası düzeyde sözleşmeler ile güvence altına alınmaktadır. Bu haklar, kişisel verilerin korunması ihtiyacını da doğuran en önemli haklardır.

Teknolojinin gelişmesi, insanları, kurumları ve hatta ülkelerin tüm organizasyonlarını birbirleri ile yakınlaştırmış, dünyayı, bilginin çok kolay yayıldığı bir köye dönüştürmüştür. Kişinin kendisini belli edecek bilgileri kendisine özeldir ancak bilginin kolay aktarımı, kişiye has özel bilgilerin de çok kolay yayılmasına olanak tanımaya başlamıştır. Bu durum zamanla kişinin toplumdan dışlanması, işini kaybetmesi, yargılanması, kınanması, dolandırılması, bilgilerinin suç malzemesine dönüştürülmesi gibi tehditleri ortaya çıkartmış, hatta skandalları da beraberinde getirmiştir.

İnsanın doğal olarak kendisini, malını, şerefini koruma hakkı mevcuttur. Bunların kendi rızası dışında bilginin paylaşılması ile riske girmesi, kişinin maddi ya da manevi zarara uğraması mümkündür. Bu nedenle devletler kişinin kendisine özgü bilgileri koruma haklarının kanunlar ile güvence altına alınması için çeşitli düzenlemelere başlamışlardır. Özellikle Avrupa Birliği, bu konuda hassas olduğunu açıklamış hem üye devletleri hem de müzakere sürecindekileri gerekli koruma

önlemlerini alması konusunda uyarılmıştır. Elbette bu noktada kişi denildiğinde akla sadece insan gelmemelidir. Tüzel kişilerin verilerinin paylaşılması da ekonomik ve ticari problemler yaratabilecektir. Dolayısıyla tüzel kişi ile ilişkili herkesin zarar görme riski ortaya çıkmaktadır. Bu nedenlerle kişisel verilerin korunması konusu içinde kurum ve kuruluşlar da değerlendirilmelidir.

Türkiye, çeşitli dönemlerde kişinin kendisine özgü bilgilerini koruma altına almak için düzenlemeler yapmıştır. Bunlardan en önemlisi 2010 yılında Anayasa değişikliği yapılmasına yönelik hazırlanan kanundur. 5982 sayılı bu kanunun 2. Md. ile T.C. Anayasasının 20. Md. değiştirilmiş ve kişilerin kişisel verilerini korumayı isteme hakkının olduğu ibaresi getirilmiştir. Kişisel verilerin korunması, aslında anayasal dayanağına bu hüküm ile kavuşmuş değildir; daha öncesinde bu önemli hak anayasal temelini, özel yaşamın gizliliği (Md..20) ve kişinin maddi ve varlığını geliştirme hakkı (Başlangıç, par.6; Md. 5;Md. 17/1) olmak üzere, haberleşme hürriyeti (Md.22), düşünce ve kanaat hürriyeti (Md..25) gibi çeşitli temel hak ve özgürlüklerde bulmuştur (Küzeci,2014:3).ancak elbette bunun altını diğer hükümler ile doldurmak, hukuki süreçlere rehberlik edecek kanunları hazırlamak gerekmekte olduğu kanun koyucu tarafından göz önüne alınmıştır.

24.03.2016 yılında 6698 sayılı Kişisel Verileri Koruma Kanunu kabul edilmiştir. Bu çalışma, kanunla birlikte yasal zemine kavuşan kişisel verilerin korunması hakkını, Türkiye’de ve dünyada kişisel veri kavramının ne olduğunu, nasıl işlenmesi, korunması ve hangi şartlar altında kaydedilmesi ya da silinmesi gerektiğine dair bilgileri içermektedir. Birinci bölümde veri, bilgi, kişisel veri, kişi ve benzer kavramların açıklamaları yapılmıştır. Bu sayede gündelik yaşamda bireyin hangi bilgilerin kendisine özel veri olduğunu kavraması mümkün olabilecek, hassas verileri ayırt etmesi mümkün olacak ve kavram karmaşası ortadan kalkacaktır. Bu bölümde ayrıca kişisel verilerin hangi standartlar altında toplanması ve işlenmesi gerektiğine ilişkin standartlar ve ilkeler araştırılmıştır.

Çalışmanın ikinci bölümünde Türkiye ve dünyada kişisel verilerin korunmasına ilişkin düzenlemelerin ayrıntıları verilmiş ardından 24.03.2016 tarihli 6698 sayılı Kişisel Verileri Koruma Kanunu’nun yasalaşma süreci, içeriği ve bu kanunun uygulanmasında birinci dereceden sorumlu olan Kişisel Verileri Koruma

Kurumu'nun görevleri, çalışma esasları, karar alma süreci ve üyelerinin nasıl seçildiğine ilişkin bilgiler verilmiştir

Bu çalışma, ülkemizdeki kişisel verilerin korunmasına yönelik mevzuatın anlaşılması, gerçek ve tüzel kişilerin kendilerine ait veriler konusunda ne tür haklarının olduğunu anlaması ve dünyadaki uygulamalar karşılaştırıldığında Türkiye'nin yerinin ne olduğunun kavranması açısından önemlidir.



BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASI

1.1. Kişisel Veri Kavramı

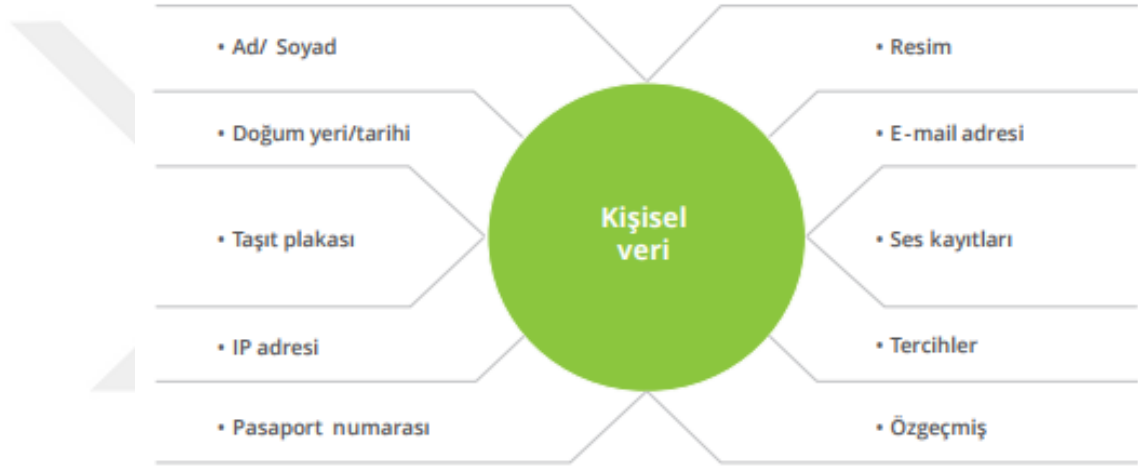
Özellikle teknolojinin gelişmesi, insanların kendilerine saklamak isteyebileceği bilgilerin bile kolaylıkla dışarı çıkmasına neden olabilmektedir. İşte bu nokta da, kişisel veri, bunun korunması, korunma hakkı gibi kavramlar daha önemli hale gelmiştir ve bu kavramlar günlük yaşamda da sıklıkla duyduğumuz kelimelere dönüşmüştür. Bu başlık altında, kişisel veri kavramı ve onunla ilişkili unsurlar incelenmektedir.

1.1.1. Kişisel Veri Tanımı

Türk Dil Kurumu, “kişisel” kelimesini, “*kişiye ilişkin, kişinin kendi malı olan, şahsi ve zati*” şeklinde; “veri” kelimesini ise “*bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done*” ve “bilgi, data” şeklinde açıklamaktadır (TDK, 2018). Bir bilgide, kişilerin varlığı söz konusu olduğunda bu bilgi “*isme bağlı veri*” veya “*bireysel veri*” haline gelmektedir. Bu bilgiler, gerçek ve/ya tüzel kişiler tarafından depo edilebilmekte ve zaman zaman çeşitli nedenlerden dolayı üçüncü taraflar ile paylaşılabilir. Özellikle devletin pek çok kurumunda veriler toplanmaktadır. Bu bilgiler, kişinin diğerlerinden ayırt edilmesine yardımcı olduğunda ise “kişisel veri” haline gelmektedir (Karabulut, 2014: 5).

Kişisel verilerin tam tanımını yapmak için OECD tarafından 1980 yılında yayımlanan “*Kişisel Verilerin Sınır aşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri*” içindeki tanıma da bakmak gerekmektedir. Burada kişisel veri, “*belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgiler*” olarak ifade edilmektedir (Kuşkonmaz, 2013: 4). O halde kişisel veri için bireyin belirleyiciliğini sağlayan tüm bilgiler açıklamasını yapmak yanlış olmayacaktır. Kişisel verilere ilişkin

bir başka açıklama da 6698 Sayılı *Kişisel Verilerin Korunması Kanunu*'nda bulunmaktadır ve burada, kişisel veri için “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” tanımlaması yer almaktadır (6698 S.K. Md.3). Bireyin kimlik bilgileri, etnik kökeni, sosyal statüsü ve sosyal kimliği, gelir durumu, akli durumu, sağlık bilgileri gibi, bireyin diğerlerinden ayırt edilmesine yardımcı olacak spesifik bilgilerin tümü kişisel veri sınırları içinde yer almaktadır (Dinkçi, 2014: 3).



Şekil 1. Kişisel Veriler

Kaynak: Nalbantoğlu, Özkaya. 2016: 4.

Kişisel verilerden bahsederken hassas veri kavramını da açıklamak gerekmektedir. Hassas veri, kimi kaynaklarda duyarlı veri (Kaya, 2011: 318) ya da özel nitelikli kişisel veri (Nalbantoğlu, Özkaya.2016: 5) olarak da adlandırılmaktadır. Hassas verileri, açığa çıkmaları halinde bireyin toplumdaki yerini ve diğer insanların kişiye bakış açısını değiştirebilecek veriler olarak tanımlamak yanlış olmayacaktır. Kişi, hassas verileri ortaya çıktığında ötekileştirme ile karşı karşıya kalabilecektir (Henkoğlu, 2015: 18).

Örneğin kişinin inançları, politik düşünceleri, cinsel yaşam biçimi, etnik kökeni gibi veriler, kişinin yaşadığı toplum içindeki pozisyonunu ve de sosyal ilişkilerindeki standartları değiştirme riskine sahiptir ve bu nedenle “hassas veri” sınıfına girmektedir (Kaya, 2011: 318).



Kaynak: Nalbantoğlu, Özkaya 2016: 5

1.1.2. Kişisel Verinin Unsurları

Kişisel verilerin unsurları, bir bilgiyi kişisel hale getiren niteliklerdir. Bir bilginin kişisel veri sayılabilmesi için “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” tanımlaması yapılmıştır (6698 S.K. Md.3) ve bu tanımlamaya göre dört unsuru vardır¹:

¹ İlgili Maddelerin tamamı 6698 Sayılı Kanun ile AB Adalet Komisyonu’nun 4/2007 Sayılı Görüşlerinden Derlenmiştir. Detaylar için: Article 29 Data Protection Working Party, EU, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (Erişim tarihi:23.05.2018)

i. Kimliđi Belirli veya Belirlenebilir Kiřiye Ait Bilgi:

Adından da anlaşılacağı üzere, bireyin toplumun diđer fertlerinden ayrılmasına olanak tanıyan her türlü bilgi onun kimliđinin belirlenmesine yarayan bilgi anlamındadır. Kimliđin belirlenmesine yönelik yapılan her tarif bir nevi kişisel veridir. İsim ve soy isim başta olmak üzere, özellikle internet ortamında, bağlanılan bilgisayarın kimlik bilgileri de kimlik belirleyici bilgidir. Ayrıca bir başka kişinin, birini bulmak için sorgulayacağı her türlü bilgi, kimliđi belirlemeye yönelik bilgiler arasında yer almaktadır.

ii. Gerçek Kiřiye Ait Olma:

6698 Sayılı Kanun, bir bilginin kişisel bilgi olması için gerçek kişiye ait olması gerektiđini, kişisel veri tanımında açıkça ifade etmektedir. Buradan hareketle tüzel kişilerin kimliklerini belirten bilgilerin kişisel veri olmayacağını düşünmek yanlış olmayacaktır.

Ancak bu duruma ilişkin, 2013/84 Esas ve 2014/183 Karar sayısına sahip Anayasa Mahkemesi kararı, kişisel bilgilerin aslında sadece gerçek kişilere ilişkin kimlik belirleyici bilgiler olamayacağını göstermiştir. 2014 yılında verilen kararda, “...Tüzel kişilerin reklam ve tanıtım amacıyla da olsa fiziki ve elektronik adreslerinin rızaları dışında bir başka özel hukuk tüzel kişisi ticari işletme tarafından ticari amaçlarla kullanmak üzere yasayla yetkilendirilmesi, adaletsiz ve hakkaniyete aykırı olduğundan, hukuk devleti ilkesiyle bağdaşmaz...” ifadelerine yer verilmiştir. (Www. Anayasa.gov.tr., Erişim tarihi:24/04/2018)

iii. İlişkin olma:

Bir şey ile ilgili olan bilgi, o şeye ilişkin bir bilgidir. Yani, bir bilginin kişisel veri olarak kabul görmesi için, o bilginin kişiye ilişkin olması ve de belirli veya kimliđi belirlenebilir nitelikte olmak koşuluyla bir kişiye ilişkin “her türlü

bilgi” veya “*bütün bilgiler*” olması (Akgül,2016:9) durumunda kişisel veri tanımındaki bilgi ve ilişkin olma niteliklerini kapsayacağı kabul edilir. Bu durumun dışında kalan ve kişiye ait olmayan ve ilişik kurulamayan bilgilerin kişisel veri değerinde görülmesi imkansızdır.

iv. Her Türlü Bilgi:

Her türlü bilgi, bireyin saklamak isteyebileceği tüm bilgileri ifade etmektedir ve bu durum bireye göre geniş bir yelpazeye yayılabilecektir. Bir şahsın ya da örgütün, izin vermediği, kendisi ile ilgili tüm bilgiler onun saklama hakkına sahip olduğu verileri göstermektedir. O halde, birinin diğerlerinden ayrışmasına yarayacak her bilgi, aslında kişisel veridir.

1.1.2.1. Veri

Veri, işlenmemiş ancak bilgiye dönüştürülmesi mümkün olan gerçeklerdir. Bilgi ve enformasyonu yaratmak için veri denilen hammadde kullanılmaktadır (Zins, 2014). Bateson veriyi, “*bir sistemin iki durumu arasında görülen veya tanınan bir farklılık*” olarak açıklamaktadır. Verilerin tasnif edilmesi, özetlenmesi, düzeltilmesi ve belirli formüller içinde kullanılması ile enformasyon oluşturulmaktadır. Cummings verinin yorumsuz ve içeriksiz” olduğunu belirtmektedir (Yılmaz, 2009: 98) O halde veri, tek başına kullanılamamaktadır ancak bilgi ve enformasyon oluşturmaya yaramaktadır demek mümkündür.

Uluslararası belgeler incelendiğinde, veri, enformasyon ve bilgi kavramlarının birbiri ile karıştığı görülecektir. O nedenle bu kavramların doğru açıklanması konunun doğru açıklanması açısından çok önemlidir. Ancak bu kavramların birbirleri ile bağı ve doktrinde tartışmaların olması, kavramların net biçimde birbirlerinden ayrılmasını da engelleyen bir durumdur. Özellikle uluslararası mevzuatta kişisel veri kavramı açıklanırken bu kavramların sıklıkla ilişkili şekilde anlatıldığı görülecektir.

1.1.2.2. Bilgi

Bilgi, verinin işlenmiş ve kullanıma hazır hale getirilmiş halidir. Verinin kullanılması ile enformasyon oluşmaktadır. Buradan hareketle bilgi/enformasyonun, kişilerin zihinlerinde değişiklik yapabilecek, düşünsel yapısında şekil değişikliği oluşturabilecek veri olduğunu söylemek yanlış olmayacaktır. O halde verinin, düşünsel alanda kullanılabilir ve düşüncüyü değiştirebilir hale gelmesine bilgi adı verilmektedir. İnsanlar, bir şeyi yapmak konusunda karar verirken, bilgiye başvururlar. Bilgiye dışarıdan erişim mümkündür ve bilgi paylaşılabilen bir şeydir. Bilginin paylaşılabılır olması, onun somut bir şey olduğunu gösteren en önemli etmendir. Bu nedenle bilginin güvenliği sağlanmalı, istenilen hallerde paylaşılması mümkün hale getirilmelidir (Henkoğlu, 2015: 17).

1.1.3.3. Kişisel Veri Ve Kişilik Hakkının Temelindeki Unsurlar

Kişilerin korumak istedikleri ve onlar için en değerli olan olgu yaşamdır. Yaşam hakkı, kişinin tüm haklarının temelinde yer almaktadır çünkü yaşamın olmadığı yerde hiçbir hakkın önemi olmayacaktır. Yaşam hakkı, kişinin kendisinin ve diğerlerinin yaşamına kast etmesinin önüne geçilmesini sağlamaktadır. Yaşama hakkı, kişinin tüm haklarının ve toplumsal düzenin başlangıç noktasıdır (Savcı, 1980: 15).

Yaşam hakkından sonra bir diğer temel hak olan kişilik hakkı, kişinin beden bütünlüğünü koruma hakkıdır. Kişinin bedeni üzerindeki her noktada hakkı mevcuttur. Kişinin bedenine karşı işlenen maddi ve manevi suçlar kişilik hakkının ihlal edilmesi durumunu doğurmaktadır. Kişiyeye yapılan saldırılar, izinsiz tıbbi müdahaleler, bedensel sorunları ile ilgili bilginin sızdırılması gibi faaliyetler, beden bütünlüğüne hakkına saygısızlık ve saldırıdır. (Ayözger, 2016: 59).

Temel kişilik hakkına dahil olan ve kişilik hakkının önemli bir konusunu oluşturan bir diğer hakkın da sağlık hakkı olduğunu da belirtmek gerekmektedir. Sağlıklı olma, kişinin bedensel bütünlüğünü koruması hakkının yanı sıra onun fiziksel, psikolojik ve sosyolojik açıdan da iyilik halinde olması durumudur. Kişilik haklarına yapılan bir saldırı, onun bedensel sağlığını bozmasa da onun psikolojisini ve toplumdaki

uyumluluk halini bozabilecektir. Bu noktada kişisel verilerin gizliliğini korumak büyük önem taşımaktadır (Temiz, 2014: 166).

Başka bir kişilik hakkı da addır. Ad; kişinin kim olduğunun ayırt edilmesinin yanı sıra, hangi aileye mensup olduğunu da göstermektedir. Kişinin adının yanlış yerde kullanılması, adının lekelenmesi gibi hareketler hukuka ve kişilik hakkına aykırı olacağı gibi, kişisel verinin korunması kapsamına girebilecek durumlar da doğurabilecektir (Ayözger, 2016: 60).

Kişisel verilerin korunmasının temelindeki en önemli noktalardan biri de şeref ve haysiyetin korunması amacını taşımaktadır. Kişinin toplum içindeki yeri, sahip olduğu saygınlığı koruma hakkı mevcuttur. Kişinin sırf insan olarak doğuştan kazandığı itibar ve saygınlık olduğu gibi, toplum içindeki davranış, yetenek ve sosyal pozisyonuna bağlı olarak kazandığı itibar ve saygınlığı da vardır ve insanlar bu konuda özenli davranmalıdırlar. Şeref ve haysiyet, tüzel kişiler için de geçerli bir durumdur. Kişisel verilerin yanlış toplanması, işlenmesi ya da izinsiz paylaşılması, şeref ve haysiyet hakkına zarar verme olasılığını da barındırmaktadır (Ayözger, 2016: 61).

Son olarak kişinin resim ve sesinin de koruma alanında olduğunu söylemek gereklidir. Çünkü ses de resimler de kişinin diğer insanlardan ayırt edilmesini sağlamak için kullanılacaklardır. Bunlar bireyin dış yaşama yansıttığı görünümleri ve sesleridir. Kişi sesi, kelimeleri söyleyişi, sessizliği, fotoğrafları, video kayıtları, karikatürü ya da buna benzer kendini ifade etme araçları ile toplumda yer sahibi olmaktadır. Bireyin görüntü ve sesinin ondan izin alınmadan kaydedilmesi, işlenmesi ya da paylaşılması onun kişilik haklarını ihlal etmek anlamına gelmektedir. Ancak bu noktada kamuya mal olmuş kişilerin istisna olduğunu da açıklamak gerekmektedir. Örneğin siyasi parti liderinin ses ve görüntüleri radyo ve televizyonlarda gösterilebilecektir. Bunun nedeni kişinin halk tarafından tanınmasına yardımcı olmak, halkın ona göre kendi kararını vermesini sağlamak ve şeffaflıktır. Fakat burada da kişinin hakları mevcuttur. Bir ünlü birey, özel hayatının gizliliğini ihlal edecek görüntü ve seslerin kaydedilmesi karşısında da hak sahibidir. Kişilerin görüntü ve seslerinin alınmasında ve paylaşılmasında kamu yararı esas olmalıdır. Bütün bunların yanı sıra, kişilerin rastlantı sonucu resimlerinin çekilmesi, onların kişilik haklarını ihlal etmek sayılmayacaktır. Ancak tesadüfen çekilmiş olsa bile bunların reklam ya da tanıtım

amaçlı kullanılması ve/veya işlenmesi yine kişilik hakkı ihlali kapsamında değerlendirilmelidir (İmre, 1974: 165).

1.2. Veri Hukukunda Kişi Kavramı

Hukuk, kişi var oldukça var olmaya devam edebilecek bir kavramdır. Bu nedenle kişi tanımının en doğru yapıldığı yer hukuk kurallarıdır. Bu başlık altında hukuka göre kişi ve kişi ayrımı kavramları açıklanmaktadır.

1.2.1. Kişi

Kişisel veriden bahsedebilmek ve bunun hukuki tanımını yapabilmek için, veri hukukunda kişinin ne olduğu ve nasıl açıklandığını da anlamak gerekmektedir. Hukuksal alanda kişi, birey olan ve bireye özgü haklardan faydalanabilen anlamına gelmektedir. Hukuk, kişi olma hakkını insana vermektedir. Kanun koyucu, toplum ihtiyaçlarına cevap verebilmek için, hak ve yükümlülükleri diğer bazı insan veya mal topluluklarına da yöneltmiştir. Türk Medeni Kanunu'nda kişi ve kişilik kavramlarına geniş şekilde yer verilmiştir. Kişi, hak ve yükümlülükler sahibi olan hak süjesidir (Dinkçi, 2014: 7).

Kişi olmadan hukuk olmayacaktır ve bu nedenle kişi, hukukun en önemli kavramlarından biridir. Kişi, haklara ve borçlara sahip olabilmektedir. Hak ehliyetine sahip olan ve bunu genişletebilen tüm varlıklar hukuksal anlamda kişidir. Bu noktada, kişi kavramının doğal bir kavram olmadığını ve aslında temelini hukuka dayandığını da söylemek gerekmektedir. Ayrıca kişilerin sadece insanlardan oluşmadığını, organizasyonların da hak ve borçları olabileceğinden dolayı kişi olduğunu belirtmek lazımdır. Bu nedenle hukukta gerçek ve tüzel kişi kavramları mevcuttur. Hukukun aradığı koşullara ve niteliklere sahip insan toplulukları olan organizasyonlar, tüzel kişilerdir.

Gerçek kişi, hakları ve borçları olabilen fakat bunun yanı sıra bir bilince sahip olan varlıkları, yani insanları işaret etmektedir. Geçmişte bakıldığında, bazı dönemlerde, toplumda düşük statüye sahip insanların hukuki açıdan kişi olarak görülmediği fark edilecektir. Ancak modern toplumda, ayırım yapılmaksızın tüm insanlar kişidir. Tüzel kişiler, ortak bir amacın gerçekleştirilmesi amacıyla örgütlenmiş

bulunan kişi ya da mal topluluklarıdır. Tüzel kişiler, kamu hukuk tüzel kişileri ve özel hukuk tüzel kişileri olarak iki alt gruba ayrılmaktadır (Bük, 2015: 16).

1.2.2. Veri Hukukunda Kişi Ayrımı

Veri Hukuku'nda kişi kavramı gerçek ve tüzel kişi olarak ikiye ayrılmaktadır. Kişisel veriler denilmesi ve hukuki açıdan bunun korunmasının bir hak olarak görülmesinin temelinde gerçek kişilerin bilgilerinin korunması isteği mevcuttur. Aslında burada korunmasından bahsedilen bilgi, bireyle ilişkili olandır. Avrupa Veri Koruması Direktifinin tanımlar başlığı altındaki 2.maddesinde kişisel veri, *“kimliği belirli veya belirlenebilir gerçek kişiye ait (natural persons) bilgi”* şeklinde tanımlanmıştır. Yine, 1. maddesinde Direktifin amacının *“üye ülkelerdeki gerçek kişilerin (natural persons) temel haklarını ve özgürlüklerini korumak”* olduğu ifade edilmektedir (Dinkçi, 2014: 8).

Konu Türk mevzuatında da aynı şekilde işlenmiştir ve bu durum tüzel kişilere ilişkin bilgilerin veri hukukunun konusu olup olmadığını tartışmalı hale getirmektedir. Kimi ülkeler, kişisel verileri sadece insanlara özgü bilgiler olarak nitelendirilirken, kimi ülkelerde bu durum tüzel kişiler için de geçerlidir ve kişi ayrımı ülkelerin mevzuatına göre değişiklik göstermektedir (Kılınç, 2012: 1094).

1.3. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi, bir verinin kişi ile ilişkilendirilmesi için gerçekleştirilen veri oluşturma, bunları elde etme, bunlar ile işlem yapma ya da bunlar üzerinde işlem gerçekleştirme gibi faaliyetlerdir. 95/46 sayılı Yönerge, kişisel verilerin işlenmesi konusunda *“Otomatik ya da otomatik olmayan prosedür yoluyla gerçekleştirilen, kişisel verilerin toplanması, elde edilmesi, kaydedilmesi, organize edilmesi, saklanması, değiştirilmesi, okunması, sorulması, kullanılması, transfer yoluyla başkalarına verilmesi, yayılması ya da hazır bulundurulması için yapılan işlemlerle bunun yanı sıra verilerin kombinasyonu ya da ilişkilendirilmesi ve hatta bloke edilmesi, silinmesi ya da yok edilmesi suretiyle gerçekleştirilen her türlü işlem”* açıklamasını yapmaktadır (Boz, 2014: 11).

Kişisel verilerin işlenmesine ilişkin bilgiler ve rehberlik, Kişisel Verilerin Korunması Hakkında Kanun'un 4. Md. verilmektedir. Bu madde, işleme esnasında dikkat edilmesi gereken ilkeleri sıralamaktadır (6698 S.K. Md.4):

- a. Kişisel verilerin işlenmesi esnasında hukuki kurallar göz önünde tutulmalı ve işlem kanunlara uygun olmalıdır.
- b. Bilgiler doğru ve güncel olmalıdır.
- c. İşlenme, belirli ve açık amaçlar için gerçekleştirilmesi gereken bir faaliyettir.
- ç. Veriler, işlendikleri amaçla ilgili olmalıdır. Ayrıca sınırlı ve ölçülü olmaları gerekmektedir.
- d. İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

1.4. Kişisel Verilerin Korunması

Kanunlar ve uluslararası otoriteler, insanlara kişisel verilerini koruma hakkı vermektedir ve bu da kişilerin kişisel verilerinin korunmasını isteme şansı anlamına gelmektedir. Aksi takdirde, kişiler, bilgilerini verdikleri diğer birey ya da kurumlara bağımlı olacaktır ve temel haklarını kullanmaları tehlike altına girecektir. Kurumlarda yöneticiler, bilgilerine sahip oldukları kişilerin verilerini koruma sorumluluğuna sahiptirler. Kanunlar ve insan hakları, kişisel verilerin korunması konusunu tartışmaya mahal vermeyecek şekilde düzenlemektedir (Çokmutlu, 2014: 39).

Kişisel verinin korunması, hukukta “veri koruma” olarak adlandırılmaktadır. Özellikle sanayi devrimi, iş ilişkisi kuran insanlar arasında bilgi paylaşımını daha kolay ve de gerekli hale getirmiştir ve kişinin kendisine ilişkin bilgileri korumak isteği artmakta ve bunu hak olarak talep etme konusu önem kazanmaya başlamıştır. Bugün kişisel veriler ile bireyler ve tüzel kişiler borca sokulabilmekte, hukuk dışı faaliyetlerde bu veriler kullanılabilenekte, veriler toplumda bölünme ve ötekileştirmelere neden olabilmektedir. Tüm bu nedenler, kişilerde, kişisel verilerini paylaşırken, paylaştıkları

kişi ya da kurumun bunu neden istediğini i ve ne amaçla kullanacağını öğrenme isteğini oluşturmaktadır (Dinkçi, 2014: 12).

Kişisel verilerin korunması konusunda kısaca kişinin unutulma hakkını da açıklamak yerinde olacaktır. Bir sebeple bireyin kişisel verilerinin açığa çıkması, onun topluma karışmasını engelleyebilecektir ve bu durumda birey, “unutulmayı” isteyebilir. Bu durumda unutulma hakkından da söz etmek, konunun anlaşılması açısından önemlidir. Unutulma hakkını kullanmak aslında kişinin affedilme hakkını kullanması olarak açıklanabilecektir. Kişinin geçmişte yaşadığı sorunların bugün karşısına çıkmaması, onun unutulması anlamına gelmektedir. Kişiler geçmişlerinde suç işlemiş ve bu suçları affedilmiş, cezaları kaldırılmış, ya da cezaları infaz edilmiş olabilmekte, ancak bu durum bugün iş bulmada, yasal işlemler gerçekleştirilmede ya da kurumlar ile ilişki kurmada sorun teşkil edebilmektedir. Bu durum yaşamı boyunca kişiyi izleyen ve onun gelişmesine, ticari ve hukuki kimliğine zarar verebilmektedir (Ayözger, 2016: 47).

Unutulma hakkı bir diğer anlamda da kullanılmaktadır. Örneğin sosyal medya ya da diğer dijital platformlarda sorunlar yaşayan, istenmeyen görüntüleri ortaya çıkan, paylaşılan, onurunu zedeleyen durumlar ile karşılaşan kişilerin de unutulma haklarını kullanmaları beklenebilmektedir. Özellikle kişinin özel yaşamının ondan izinsiz şekilde sosyal medyada bahsi geçmesi söz konusu olabilmektedir veya kişi kendi rızası ile kendine ilişkin bilgileri paylaşabilmektedir ancak zaman içinde bundan rahatsız olabilmektedir. Bu tür durumlarda, kişinin ilgili bilgiye erişimi engellemeyi isteme hakkı mevcuttur. Ancak bazı bilgilerin de kamunun bilinçlendirilmesi için paylaşılması gerekmektedir. Bireye ilişkin bilgilerin “kamu yararına” paylaşılması yaklaşımı bu sebeple önem kazanmıştır. Kişinin, onun toplumdan dışlanmasına neden olabilecek şekilde kişisel verilerinin açığa çıkarılmasına karşı, yaşam standartlarını devam ettirebilmek ve sosyal olanaklardan faydalanmak için kişi, kendisine ait verilerin silinmesini ve ulaşılmaz hale getirilmesini isteyebilmektedir. İlk defa 2012 yılında teklif edilen bu yasal düzenleme, 2014 yılında Avrupa Adalet Divanı tarafından kabul görmüş ve bir hak olarak tescil edilmiştir (Küveli, 2016: 231).

Bu karara karşı çıkanların da düşüncelerine yer vermek konuya objektif yaklaşmak açısından önemlidir. Avrupa Birliği Adalet Divanı, Mario Costeja isimli

şahsın adının arama motorunda sorgulanması ile yıllık vergi borcu nedeni ile evinin satışa çıkarılacağı haberinin 10 yıl sonra bile hala var olduğunu görmesi üzerine, bu durumu özel hayatın gizliliğinin ve kişisel verilerin korunması hakkının ihlali olarak değerlendirmiştir. Ancak bunun yanı sıra kamuya mal olmuş kişilere ilişkin bilgilere sınırlama getirilmesinin, insanları bilgilendirme açısından olumsuz olacağını ve istisna uygulanması gerektiğini savunmuştur. Geçmişe yönelik bilgilerin, kamuya mal olmuş kişiler için, doğru olması halinde gazetecilik amaçları için kullanılması hallerini istisna olarak kabul etmiştir. Avrupa Birliği verdiği direktiflerinde ise unutulma hakkının kişisel verilerin silinmesi konusu ile birlikte ele alınması gerektiğini savunmaktadır (Ayözger, 2016: 49).

Unutulma hakkına ilişkin Türkiye’de de Yargıtay’ın verdiği ve akademik çevrelerde “devrim niteliğinde” olarak tanımlanan bir karar mevcuttur. Bir davada, cinsel saldırı mağduru davacının yargılama süresince aktardığı saldırıya ilişkin bilgilerin, mağdur ve sanık isimleri rumuz kullanılmadan bir kitapta yayınlandığı için, mağdur şikayetçi olmuştur. Davalılarca iddia edilen ve Yargıtay tarafından kabul olunan “eserin, bilimsel eser haline geldikten sonra kamuya mal olduğu ve kural olarak ancak kendi ilkeleri çerçevesinde sınırlamalara tabi olacağı” ifadesi, YHGK’nın kararında “bilim özgürlüğü ile kişilerin, kişilik değerlerinin karşı karşıya geldiği durumlarda bu değerlerin üstün tutulması gerekeceği” gerekçesi ile reddedilerek davacı lehine manevi tazminat koşullarının oluştuğuna karar verilmiştir. (Küpeli, 2016: 234).

1.4.1. Kişisel Verilerin Korunması Hakkının Hukuki Niteliği

Kuşkusuz, kişisel verilerin korunmasına ilişkin hukuki açıklamaların en önemlisi konuya ilişkin kanunlardır. Bu kanunların hangi hukuksal çıkarılara hizmet ettiğine ilişkin küresel akademik çevrelerde tartışmalar mevcuttur. Herkes kişilerin kendilerine ait bilgilerin saklanmasını isteme konusunda hemfikirdir ancak bunun hangi hak temeline dayandığı konusunda bir uzlaşma mevcut değildir. Tartışmaların en yoğun olduğu üç temel başlık mülkiyet hakkı görüşü, fikri mülkiyet hakkı görüşü ve özel hayatın gizliliği hakkı görüşüdür.

1.4.1.1. Mülkiyet Hakkı Görüşü

Kişisel bilgilerin denetimi kişiye bağlıdır ve mülkiyet hakkı görüşünün temelinde de bu düşünce bulunmaktadır. Bilgi bir çeşit varlıktır ve bu varlığın idaresi kişiye aittir. Bilgi mülkiyetine sahip birey bunu saklamak ya da paylaşmak konusunda serbesttir. Kişisel verilerin bir mülkiyet hak alanı içinde bulunduğu görüşüne sahip hukuki düzenlemeler özellikle Amerika Birleşik Devletleri'nde karşımıza çıkmaktadır. Avrupa'da da bu görüşün temel alındığı düzenlemelerin olduğunu söylemek mümkündür. Avrupa'da bu düşünce biçimi daha çok sosyal değerlere göre, ABD'de ise ekonomik ve teknolojik değerlere göre şekillenmiştir. Dünya genelindeki yasal düzenlemelere bakıldığında, ABD'de kişisel verilerin korunmasına ilişkin yasal düzenlemelerin oldukça düşük düzeyde olduğunu söylenebilir. Ülkedeki düzenlemelerin temeli anayasa değildir ve daha çok özel sektörde veya yerel yönetim düzeyinde şekillenmiştir (Clarke, 2000).

Mülkiyet hakkı görüşüne sahip taraflar, bilginin ekonomik değerine dikkat çekmektedirler. Kişisel verilerin ekonomik değerinin olması bile onların sahibine bunlarla ne yapmak istedikleri konusunda haklar vermektedir ve kişi bunların hangi şartlarda saklanması ya da paylaşılması gerektiği konusunda yetkilidir. Özellikle şirketler hem tüzel kişiliklerinin hem de bünyelerindeki personelin kişisel verilerini mal varlığı olarak görmektedirler ve sahiplerinin de izni ile bunu pazarlama eğilimine girebilmektedirler. Ayrıca bu şirketler müşterilerinin bilgilerini de şirketlerinin hizmet ve ürünlerini geliştirmek için kullanmaktadırlar. Bu tutum bir veri pazarı oluşturmuştur. Günümüzde pek çok insan, özellikle elektronik ortamda, farkında olmadan şirketlere, kendilerine ait verileri kullanma hakkını vermektedirler (Kuşkonmaz, 2013: 20).

1.4.1.2. Fikri Mülkiyet Hakkı Görüşü

Bu görüşün de temelinde bilginin ekonomik değeri mevcuttur. Fakat bu görüşe sahip taraflar bilginin bu değerinin kişi tarafından hızla kaybedilebileceğinin de altını çizmektedirler. Özellikle internet bu bilgilerin değerlerinin kişi tarafından kaybedilmesi konusunda hızlandırıcı bir araçtır (Schwartz, 2004: 2074).

Kişisel verilerin fikri mülkiyet hakkı görüşü ile açıklanması; kişisel veri sahibinin kendisine ilişkin veriler üzerindeki hakları ile fikri mülkiyet hukukundaki eser sahibinin meydana getirdiği eser üzerindeki manevi hakları arasındaki benzerlik açısından değerlendirilmektedir. Bu noktada fikri mülkiyet hakkı ile kişisel verilerin korunması hakkının aynı olmadığına da altını çizmek gerekmektedir. Fikri mülkiyet hakkı içine giren varlıklar, kişilerin çalışmaları ve çaba harcamaları sonucunda ortaya çıkan ürünlerdir. Ancak kişisel bilgiler kişinin sadece var olması ve yaşamsal tercihleri ile bile ortaya çıkabilmektedir. Kişisel bilgiler, insanın insan olmasında ötürü sahip olduğu doğal bilgilerdir. (Kuşkonmaz, 2013: 22).

1.4.1.3. Özel Hayatın Gizliliği Hakkı Ve Kişisel Verilerin Korunması

Özel hayat denildiğinde toplumda akla genellikle kişinin cinsel yaşamı gelmektedir. Ancak özel hayat, kişinin kendisine saklamak istediği bilgilerin tamamıdır ve temelinde insanın sosyal bir yaşam içinde, sadece kendisini ilgilendirdiğini düşündüğü verilerin olması bulunmaktadır (Korkmaz, 2014: 100).

Kişinin kendisi ile ve toplumla ilişkisi ayrıdır. İnsan, diğer insanlar ile bilgiyi paylaşmaya ihtiyaç duyan bir varlık olmasına karşın kendi kendisi ile ya da kendisi için özel olan bireylerle zaman geçirme ve paylaşım yapmaya da ihtiyaç duymaktadır ve buna da özel hayat adı verilmektedir (Çelik, 2017: 392).

Kişinin özel hayatının, sır alanı içerisinde kabul edilen, cinsel hayatı, dinsel tercihleri, ırksal kökeni gibi konulara ilişkin kişisel veriler, hassas veri olarak kabul edilerek daha özel bir korumaya tabi tutulmuş ve özel hayatın çekirdek alanı kabul edilmiştir. Ayrıca, kişinin özel hayat alanına müdahale edilebilmesi için ağırlıklı bir kamu yararının varlığı gerekmekte ve bu durumda dahi kanunla çizilen çerçeveye dikkat edilmesi zorunludur.

Özel hayatın gizliliği temel bir insan hakkıdır. İnsan onuru ile ifade özgürlüğü gibi diğer değerleri yücelten ve kapsayan bir kavram olan özel hayatın gizliliği kavramı aynı zamanda modern çağın en önemli insan haklarından biri olmaktadır. Kişisel verilerin oluşması, korunması, hak olarak hayatımıza dahil olmasıyla özel

hayatın gizliliği kavramını birbirinin içine geçmiş hak ve kavramlar olan gören bu görüşe göre kişisel verilerin korunması hakkı da özel hayatın gizliliği hakkının çekirdek alanına dahil edilmelidir.

1.5. Hak Kavramı

Hak sözcüğünün gerçek ile doğruluk/dürüstlük olarak iki anlamı mevcuttur. Hak, hukuksal açıdan birinin bir şeyi yapma yetkisinin bulunması anlamına gelmektedir. Haklar, hukuk ile korunmaktadır ve hukuk, hak sahibine bunu kullanma yetkisini vermektedir. Hak, kişiye sağlanmakta ve ona bundan faydalanma şansı vermektedir. Hakkın var olması için hukuki bir düzenleme olması şarttır. Aksi takdirde insanlar çıkar sağlayabilecekleri şeylerden mahrum olacaktır. Haklar, hukuku referans olarak göstermektedir (Boz, 2014: 13).

Hukuk, hak kelimesinin çoğul halidir. Hakkın kullanılabilmesi için kişinin toplumsal düzeni bozmaması, başkalarına zarar vermemesi, toplum kurallarının ve kanunların dışına çıkmaması gerekmektedir (Kudat, 2014: 98). Bireyin hakkını kullanabilmesi için, içinde bulunduğu toplumun hukuk kurallarında talep etme yetkisinin var olması gerekmektedir. Örneğin kişisel verilerin korunması hakkının kullanılabilmesi için kişilere bu hakkın verilmiş olması ve bunun hukuken güvence altına alınmış olması lazımdır. Bu hakkın ihlal edilmesi karşısında yasal yaptırımların olması şarttır. Bu sayede kişiler haklarının iade edilmesi ve korunması konusunda hak talebinde bulunabileceklerdir (Boz, 2014: 14).

1.6. Yasal Düzenleme Kavramı

Yasal düzenlemenin ne olduğunun açıklanabilmesi için öncelikle yasa ve yasal kavramlarının sözlük anlamlarını incelemek gerekmektedir. Türk Dil Kurumu Güncel Türkçe Sözlükte yasa için, “değişmeyen, olağanın dışına çıkmayan ve mecburiyet gösteren kural” ile “Devletin yasama organları tarafından konulan ve uyulması gereken kurallar bütünü, kanun” tanımlamaları yapılmıştır. Aslında her iki tanımdan da anlaşıldığı üzere, yasalar konulan, kimse ve hiçbir koşul için esnetilmeyen kurallar bütünüdür demek yanlış olmayacaktır. Yasal ise aynı kaynaktan “yasanın, dinin ve

kamu vicdanının doğru bulduđu, yasalara uygun, kanuni, meşru, legal” şeklinde tanımlanmaktadır (TDK, 2018).

Yasal düzenlemeler, hukuk devletinde, yetki sahibi otoriteler tarafından yasalara uygun şekilde yapılan meşru düzenlemelerdir. Yasal düzenlemeler; *anayasa, kanunlar, kanun hükmünde kararname, uluslararası antlaşmalar, tüzükler ve yönetmeliklerden* oluşmaktadır. Yasal düzenlemeler birbirlerini tamamlar nitelikte, yazılı ve belirli bir hiyerarşik düzene sahiptir. Ülkelerin anayasaları en üstün ve en birincil yasal düzenlemeleridir ve tüm diğer yasal düzenlemeler buna göre yapılmaktadır. Anayasa, tüm yasaların üstündedir. Devletler, vatandaşlarının ödev, sorumluluk ve haklarını yasal düzenlemeler ile güvence altına almaktadırlar. Yaşam düzenindeki değişimler, yasal düzenlemelerin de zamanla güncellemesini gerekli kılmaktadır (Boz, 2014: 14).

1.7. Özel Hayatın Gizliliği Hakkı Ve Kişisel Verilerin Korunması Gereksinimi

1.7.1. Genel Olarak

İnsanların kendilerine ait alanlarının ve düşüncelerinin olması modern dünyada henüz yeni bir kavramdır. Özellikle küreselleşme ve teknolojik gelişmelerin hız kazanması neticesinde, bilgi ekonomik bir değer kazanmış, bunun yanı sıra bilgi hırsızlığı kişileri bazı sorunlar ile karşı karşıya getirmiştir. İşte bu noktada insanlar, kendileri ile ilişkili verileri kendilerine saklama gereksinimi duymaya başlamış ve bununla ilgili haklar talep etmişlerdir. Bugün bilgi, her türlü organizasyon ve kişi için güç anlamına gelmektedir ve her türlü üretimin ana ham maddesidir. Her gün milyarlarca yeni veri girişi ve paylaşımı gerçekleşmektedir ve bunların içinde bireye özgü verilerin de yeri oldukça büyüktür. İnsanların ve organizasyonların kişisel verileri , günümüzde dijital ortamda kolaylıkla takip edilmekte ve bu veriler ile insanlar etiketlenilmektedir. İnternet ortamındaki reklamların hangi insanlara gösterileceğine bile onların kişisel verilerine göre karar verilmektedir (Solove, 2004: 1-2).

Özel bilgilerin kolaylıkla paylaşılmasının insanların üzerinde negatif yönlü psikolojik etkilerinin olabileceği de unutulmamalıdır. Kişi, kendisini sürekli takip ediliyormuş gibi hissedecek ve her zaman taciz edilme duygusu ile yaşayacaktır. Bunun kanıksanmasının sosyolojik sorunlar yaratacağı da unutulmamalıdır. Devletin kişisel verileri saklaması bile kimi zaman rahatsız edici olabilmektedir. Örneğin insanların hemen her yerde T.C. Kimlik Numaraları ve isimlerinin sorulması, bu bilgileri kolay ulaşılabilir hale getirmektedir. Bir insan, başka bir insanın ne şartlarda çalıştığını öğrenmek için örneğin SSK dökümünü bulması bugün şartlarında basit olan ve kolaylıkla öğrenebilecek bir bilgidir ve bu, kişiler için rahatsız edici olabilir. Kişi, çalışma koşullarını saklama isteği duyabilmekte ancak bunu gerçekleştirememektedir. İnsanlar arasında dürüst ve sağlıklı ilişkilerin kurulabilmesi, onların birbirlerine güvenerek, kendiliğinden kendileri ile ilgili bilgileri paylaşmasıyla mümkündür (Ketizmen ve Ülküderner, 2007: 191).

Hukuki açıdan bakıldığında, kişisel verilerin kişiye özel kalması konusundaki hak, özgürlük ve yasal düzenlemelerin iki uçlu olarak tartışılmaya devam ettiği görülecektir. Kimi hukukçular, kişinin kendisi ile ilişkili bilgileri saklamaları gerektiğini düşünürken diğerleri kamu düzeni ve kamudaki bazı süreçlerin devam etmesi için bilgilerin paylaşılması gerektiği görüşündedirler. Bu tartışmalar özel hayat kavramının her zaman istenilen ölçüde özel ve gizli kalamayacağını göstermektedir.

Kişilerin kişilik hakları, onların hukuk kurallarını yapmasında ve uygulamasında çıkış noktasıdır. Ancak kişilik haklarının kişiler arasında çakıştığı noktaların olduğu da gözden kaçırıl mamalıdır. Örneğin bir siyasetçinin ödül alırken çekilen bir fotoğrafının paylaşılması haber niteliği taşıırken, bir vatandaşın fotoğraflarının ondan izinsiz paylaşılması kişilik hakkının ihlali anlamına gelmektedir. Özel hayat başta olmak üzere, kişisel veri kavramını da doğuran kişilik haklarının bilinmesi, kavramları daha iyi açıklamak, hakları öğrenmek ve kişisel verinin sınırlarını kavramak açısından önemlidir.

1.7.2. Özel Hayatın Gizliliği Hakkı

Kişisel veriler kavramının ve hukukunun ortaya çıkmasına neden olan olgu kişinin özel hayatıdır. Özel hayat kavramı sıklıkla konuşulan ancak ne olduğu konusunda pek çok kişinin fikir sahibi olmadığı ve sınırlarının belirsiz olduğu bir konudur. Özel Yaşam'ın tanımlanmasının güç olması ve bu güçlüğü özellikle kamusal alan ile özel alan arasındaki sınırlarının belirsizliği sebebiyle her somut olayda olayın kendi koşullarına göre bir değerlendirmesi gerekmektedir ve yine her olayda özel yaşam/alan kavramı tekrar tanımlanmalıdır. (Küzeci, 2014 :5)

Modern yaşamda insan kendisine ait alanı savunma isteği duymaktadır. Ev, araba, iş yerindeki masa, sosyal medya hesapları gibi, kendisine ait eşya ve yaşam unsurlarının bulunduğu noktalar, özel hayatın temellerini oluşturmaktadır (Salihpaşaoğlu, 2013: 227). Özel hayat dört temel unsurun bir araya gelmesi ile ortaya çıkmıştır (Bük, 2015: 12-13):

i. Herkesin bölgesel mahremiyeti vardır ve konutu ve üzeri gibi alanlar dokunulmazdır. Kişi kendi rızası ile ancak mahremiyet bölgesine diğer insanları kabul edebilecektir.

ii. Kişilerin haberleşme gizliliği hakkı mevcuttur. Onların iletişim kanallarının izlenmesi, dinlenmesi ve kayıt altına alınması, haberleşme gizliliğinin ihlalidir.

iii. Kişinin vücudunun mahremiyeti mevcuttur. Genetik testi, kızlık testi gibi testler, kişinin rızası olmadan uygulanamayacaktır.

iv. Kişinin veri mahremiyeti hakkı vardır. Kişisel bilgileri toplamak, saklamak, işlemek ve paylaşmak, veri mahremiyetine aykırıdır.

Özel hayat insanların toplu yaşamaya başladıkları sürelerden beri var olan, dönemine göre sınırları değişim gösteren bir unsurdur. Duerr, iç mekan duvarları olmayan en ilkel evlerde bile kişilerin özel alanlarını oluşturan hayali duvarların olduğundan söz etmektedir. Bugün de evlerde, ortak alanlarda (örneğin yemek masası) ev üyelerinin oturacakları yerler belirlenmiştir ve sözsüz bir anlaşma bulunmaktadır. İlkel toplumlardan bugüne, özel hayata saygı ve bireyin mahremiyetinin korunabilmesi için toplumsal kurallar oluşturulmuş, zaman içinde bu kavramlar

yasalar ile sabitlenmiştir. İnsanların inandıkları dinlerde de mahremiyete saygı söz konusudur. Örneğin İslam ve Musevilik, izinsiz bir başkasının odasına girilemeyeceğini ve hatta bakılamayacağını belirten kutsal metinlere sahip dinlerdir (Salihpaşaoğlu, 2013: 228-229).

1.7.2.1.Düşünce Özgürlüğü

Kişisel verilerin korunması ve paylaşılması söz konusu olduğunda, düşünce özgürlüğünden de söz etmek lazımdır. Düşünceler kişinin iç dünyasında oluşan düşünce ve fikirlere dir. Herkesin bir konu hakkında istediği şekilde düşünmesi bir haktır ve hukuk bunu koruma altına almalıdır. Kişinin düşünceleri de kişisel verileridir ve bunları düşündüğü, düşüncelerini ise açıkladığı için kınanmaması ya da baskı altında hissetmemesi gerektiği unutulmamalıdır.

Kişisel verilerin korunması ile düşünce özgürlüğü arasında sıkı bir ilişki olduğunu da söylemek lazımdır. Kişinin düşüncesini açıklamasının özgürlük olarak sayılması pozitif bir etkiye sahiptir. Ancak bunun negatif etkilerinin de olması riski mevcuttur. Örneğin devlet, kişilerin düşüncelerini açıklaması için onlara baskı yapamayacaktır ya da onu taraf seçmeye zorlayamayacaktır. Yani, kişi kendisine ait kişisel verilerin ve bu verilerin içinde yer alan düşüncelerin açıklanmasına zorlanamayacağı gibi, kişi kişisel verilerini kime, hangi oranda açıklayacağı konusunda da özgürdür. Kimi durumlarda kişinin düşünce hakkı ile kişisel verilerin gizliliği hakkı çatışmaktadır. Örneğin basın, düşünce özgürlüğü adı altında, magazinsel haberleri paylaşarak diğer kişilerin kişisel verilerini ortaya koyabilmektedir. Bu noktada önemli olan yasaların, kişisel düşünceler ve düşünce özgürlüğü ile kişisel verileri gizleme hakkı arasındaki terazi olma görevi görmesidir. (Ayözger, 2016: 52).

1.7.2.2. Bilgi Edinme Hakkı

İnsan, etrafında olup biteni gözlemleyerek, dinleyerek ya da yaşayarak öğrenmekte, kişiliğini ve fikirlerini buna göre zaman içinde şekillendirmektedir. Bunun en önemli nedeni, insanı diğer canlılardan ayıran düşünme yeteneğidir ve bu durum doğaldır.

Modern insan, çevresinde olan biten her şeyin, doğrudan ya da dolaylı olarak kendisini etkileyeceğinin bilincindedir ve bununla ilgili bilgi talep etmektedir. Devlet yönetimleri, halkı ve kişileri bilgilendirmek durumundadır. Bilgi paylaşımı ve bilgi edinme hakkının kişiler tarafından kullanılması, şeffaf bir yönetimin ve demokratik bir toplumun en önemli şartlarıdır. Kamu kurum ve kuruluşlarının ellerinde bulundurdukları her türlü bilgi ve belge ile vatandaşlardan elde ettiği bilgileri resmî sır olma niteliğinden çıkartarak erişime açmaları bilgi edinme hakkının temelidir. Bu sayede toplumda örgütler, kamu kurumları ve özel kuruluşlar işlevlerini yerine getirebilmekte, hesap verebilirlikleri artmakta ve toplumun yararına çalışmaya devam etmektedirler. Bilgi edinme hakkı, toplum yararının temel öğelerinden biridir (Demirel, 2015: 146).

Bilgi edinme hakkının, kişisel verilerin korunması konusu ile kesiştiği nokta, negatif bilgi edinme hakkının kullanılmaya başladığı noktadır. Kişisel verilerin toplanması ve işlenmesi esnasında uygulanan politikalar sebebiyle, kişi bilgi edinme hakkını kullanabilmektedir. Bu sayede hukukun kendisine verdiği diğer hakları da kullanma imkanına sahip olabilmektedir. Türkiye’de bilgi edinme hakkı, 09/10/2003 tarihli 4982 sayılı Bilgi Edinme Kanunu ile güvence altına alınmıştır (Ayözger, 2016: 53).

1.7.3. Kişisel Verilerin Korunmasının Nedenleri ve Gereksinimi

Kişisel veriler özellikle işletmelerin müşteri hedeflerini belirlemesi, onlara isteklerine uygun ürün ve hizmetler sunması, rekabet avantajı sağlaması gibi faaliyetleri için pazarlanan ürünlere dönüşmüştür. Bu durum aslında insanların inisiyatiflerine göre tüketim yapmaları önünde bir engeldir. İnsanlar, verilerinin kullanıldığı üretim ortamında bilinçsiz tüketiciler haline gelmektedirler. Tüm bu nedenler, kişisel verilerin korunmasını gerekli kılan en önemli etmenlerdir (Kuşkonmaz, 2013: 13).

İnsanların kişisel verilerinin korunmaması, siber suçları da beraberinde getirmektedir. Örneğin kredi kartı, telefon ve adres bilgileri, sosyal medya hesapları ile e-posta şifreleri gibi bilgiler, kolaylıkla internet ortamında hırsızlık yapılmasını

kolaylaştırmaktadır. Bugün insanların paralarını çalmak için ortalama gibi siber suç faaliyetleri gerçekleştirilmektedir ve alışveriş siteleri, bankalar ve verilerin saklandığı kuruluşların müşteri kaybetmemeleri için verileri güvende tutması ve bunun için müşterilerine güvence vermesi bir zorunluluk haline gelmiştir (Computerworld, 2016). Günümüzde artık hiçbir yasal düzenleme olmasa bile, kişisel verilerin kullanılması konusunda müşterilerine güven veren işletmelerin pek çok çıkarı mevcuttur:



Şekil 3. Kişisel Verileri Korumanın İşletmelere Sağladığı Avantajlar

Kaynak: Nalbantoğlu, Özkaya.2016: 3.

Kişisel verilerin korunması, kişinin sosyal yaşam rutinini devam ettirebilmesi ve ilişkilerinde kendi istekleri doğrultusunda paylaşım yapabilme özgürlüğünün sağlanması için de önemlidir. İnsanlar, kendileri ile ilgili bir bilgi yüzünden dışlanabilmekte, işlerinden atılabilmektedirler. Örneğin pek çok transseksüel birey, bu durum ortaya çıktığı için iş ortamında mobbinge maruz kaldıklarını belirtmektedirler. Ayrıca siyasi düşünceler, etnik köken, dil, ırk, sağlık durumu gibi farklılıklar, insanların birbirleri ile ilişkilerine yön verebilen bilgileri içermektedir.

İnsanlar çok basit nedenler ile dışlanmakta ya da eşitsizlikle karşılaşabilmektedirler (Boğaziçi Üniversitesi Sosyal Politika Forumu, 2010). Bu noktada tüzel kişilerin kişisel verilerinin neden korunması gerektiğine ilişkin sorgulama da yapmak gerekmektedir. Kimi iş sözleşmeleri ve şirketler arası alışverişlerde ticari bilgiler, patentler, icatlar, devredilmiş ya da belirli süreliğine kullanım lisansı verilmiş ürün ve yöntemler, fikri mülkiyet hakkı kapsamına girebilecek bilgiler paylaşılabilir. Bu durum devlet ve özel sektör arasında da paylaşılabilir ve bunlar tüzel kişinin kişisel verileridir. Bunların paylaşılması özellikle rekabet ortamında ilgili tüzel kişiyi zor bir duruma düşürecek, avantaj kaybı anlamına gelecektir. Bilgi, ticari faaliyetlerin gerçekleştirilmesi öncesi ve sırasında büyük bir önem taşımaktadır. Projede yapılacak ürün ya da verilecek hizmetin, pazara sunulmasından önce taşıdığı özellikler, düşünülen tasarımı, ürünlerin diğerlerinden farkı ve fiyat politikası, pazarlama stratejileri gibi bilgilerin dışarıya verilmesi, ticari kayba sebep olabilecektir. Bunların korunması için organizasyonlar arasında gizlilik sözleşmeleri yapılmaktadır (Şenbaş, 2013: 12-13).

1.7.3.1. Gözetim ve Denetim

Bugün pek çok insan bir gözetim topluluğu içinde yaşadığını düşünmektedir. Kamu ve özel kuruluşlar, bireyleri gözetim altına almak istemektedirler ve bunun nedeni siyasal düzenlemeler, ekonomik faaliyetler ve toplum düzenidir. Ancak kişisel olarak bakıldığında bu durum hoş karşılanmamaktadır. Bu noktada, kişisel verilerin neden korunması gerektiğine yanıt verebilmek için gözetimin ne olduğuna cevap vermek gerekmektedir.

Gözetim, iki taraflı bir sistemde birbirini izleme anlamına gelmektedir. Gözetimde kurallara göre ve sistematik bir izleme söz konusudur. Gözetim sayesinde yapılan faaliyet kurallara uygun ilerlemekte ve verimlilik sağlanmaktadır (Sönmez, 2016: 265) Ancak gözetim kimi zaman düzeni sağlamak amacı ile yapılmamaktadır. Kişisel veriler ve bireyin yaşam biçiminin gözetlenmesi, ona taciz edilmesi hissi verebilmektedir.

Denetim ise çok eski tarihlerde ortaya çıkan ve bir faaliyetin doğru yapılıp yapılmadığına dair izlemeye olanak sağlayan, insanların bir arada düzen içinde yaşamasının bir koşuludur. İktisadi yaşam, insanlar arasında haksızlıkların yapılmasının önüne geçilmesi için denetimin öneminin artmasına neden olan en önemli olgudur. Denetim bugün yasalar ile güvence altına alınmıştır. Kanunlara aykırı olan tüm eylemler, bunları denetlemeye yetkilendirilmiş kurumlar aracılığı ile denetlenmekte ve usulsüzlüklerin tespit edilmesi halinde yaptırımlar uygulanmaktadır (Bozkurt, 2013: 56).

1.7.3.2. Teknolojideki Gelişmeler

2000 yılında Türkiye’de 2 milyon olan internet kullanıcısı sayısı, 2010 yılına dek yüzde 1650 artış göstermiş ve 35 milyona ulaşmıştır. Bu, elektronik ortamda yalnızca ülke içinde bile günlük olarak çok fazla bilginin taşındığı anlamına gelmektedir. Aynı kullanıcıların dünyanın her yerinden diğer kullanıcılar ile etkileşime girdiği de unutulmamalıdır (Özbilgin, 2011;7).

Yeni teknolojilerin yaygınlaşması kişilerin ve kurumların korunması gereken verilere ilişkin endişelerini de artırmaktadır. Bu sebeple teknolojideki gelişmeler değerlendirildiğinde ve iletişim ağlarının genişlemesi sebebiyle kişiler bu alanlarda kendilerine ait verilerin korunması gereğini hissetmektedir.

1.8. Kişisel Verilerin Korunması Bağlamında Temel İlkelerin İncelenmesi

Kişisel bilgilerin işlenmesi ve işlenme esnasında gerçekleşen tüm faaliyetlerin nasıl yapılacağına dair detaylar ilgili mevzuatta açıklanmaktadır ve verilerin saklanması bu kuralların dışında gerçekleştirilemeyecektir

24 Mart 2016 tarihinde kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu temel ilkeleri listelemektedir (6698 K.V.K.K. 2.Bölüm, Md.4-5).

1.8.1. Kişisel Verilerin Hukuka Uygun İşlenmesi İlkesi

Verilerin saklanması en önemli şartı tüm işlemlerin hukuki düzenlemelere göre gerçekleştirilmesidir. Tüm faaliyetlerin pozitif hukuk kurallarına göre yapılması şarttır. Bunun gerçekleşmesi için ön koşul, işleme işleminin tanımlanması ve amacının belirlenmesidir. Hukuka uygunluk yalnızca T.C. Mevzuatına göre değil, uluslararası düzenlemelere göre gerçekleştirilmektedir. Tüm mevzuat sistemleri, hukuka uygun işlenmenin sağlanması için en önemli koşulun dürüstlük olduğunu vurgulamaktadır (Bkz 6698 S.K.; AB Direktifi vb. gibi).

Dürüstlük, verilerin gerçeği yansıtacak biçimde işlenmesinin yanı sıra işleme amacının veri ile ilişkili kişiye de doğru aktarılması anlamına da gelmektedir. Sahibinin neden kullanılacağını anlamadığı kişisel verilerin hiçbir suretle işlenmesi kabul edilemez. Ayrıca veri işlemekten sorumlu kişi ya da birimlerin, bireyin kişiye özel verilerinin işlenmesi sürecinde özel hayatın gizliliği ilkesine sadık kalması da bir zorunluluktur. Kişinin bilgilerinin kişinin özel hayatın gizliliği hakkını, maddi ve manevi bütünlüğü ile özerkliğini makul olmayan nedenlerle ihlal eden bir hareketten kesinlikle kaçınması gerekmektedir (Kuşkonmaz, 2013: 88-89).

Kişisel verilerin toplanması esnasında kişiye neden toplandığı açıklanmalı ve kişi istediği zaman veri toplama ve koruma politikalarını sorgulayabilmeli, verilerini değiştirebilmeli ve bunu zaman kaybetmeden ve mali yük altına girmeden başarabilmelidir (Kılınç, 2012: 1111). Ayrıca hangi amaçla olursa olsun, verilerin toplanması hukuki amaçlar dışına çıkmayacaktır. Hangi sebepler ile verilerin toplanabileceği, hangi koşullarda istisnaların olabileceği gibi detaylar ülkelerin mevzuatlarında açıklanmaktadır ve tüm kurum ve kuruluşlar buna uymalıdır. Ayrıca, çeşitli nedenlerle ayrımcılığa sebebiyet verebilecek hassas veriler gerekmedikçe kişiden alınmamalıdır (Bük, 2015: 29).

1.8.2. Kişisel Verinin İşlenmesinde İlgilinin Bilgilendirilmesi İlkesi

Verilerin işlenmesi öncesinde ve esnasında bunların asıl sahibi kayıtsız şartsız bilgilendirilmelidir. Aksi takdirde kişi kendisine ait verilerin yönetimini de kaybetmiş

ve/veya kandırılmış olacaktır. Konuya ilişkin tüm hakların korunabilmesi için verilerin ne şekilde ve ne amaçla işleneceği konusunda kişilerin tam bilgi sahibi olmaları gereklidir (Yüksel, 2012: 117). Bireyin kişisel verilerinin işlendiğinden haberdar edilmesi ya da veri toplamanın koşulları hakkında düzenli ve kapsamlı olarak bilgilendirilmesi ilkesi, aynı zamanda verilerin işlenmesinde dürüstlük ilkesine uyulmasının da bir gereğidir. Sürekli iletişim, verilerin güncel ve doğru kalmasının yanı sıra veri sahibinin bilgilendirilmiş halde kalmasının da temelini oluşturmaktadır. Veriler üzerindeki hak sahibi kişinin asgari şu konularda bilgilendirilmesi şarttır (Karabulut, 2014: 40-41):

- i. Verileri işleyecek olan sorumlunun ya da bu merciiyi temsil edenlerin kimliği;
- ii. Verilerin hangi amaçla işleneceğinin bilgisi;
- iii. Verileri kabul edenler hakkında bilgi;
- iv. Kişinin sorulara cevap verme konusunda özgür olduğu, cevap verme ve vermeme durumunda ne tür olasılıklar ile karşılaşabileceği
- v. Kişinin kendisine ilişkin bilgiler hakkında sürekli bilgi alma özgürlüğünün olduğu ve gerekli hallerde bunlarda değişiklik yapabileceği bilgisi.

Görüldüğü gibi kişilerin kendisine ait bilgileri üzerinde işlem yapılması onların toplanması, saklanması, paylaşılması ve diğer işlemler esnasında kişinin bilgilendirilmesi, onun rızasının alınması gerekliliğine dayanmaktadır. Kişiyi kendisi ile ilgili ne tür bilgilere sahip olunduğu/ ihtiyaç duyulduğu, bunlar ile ne yapılacağı ne kadar süre kişisel bilgilerin kullanılacağı ve kişinin bunlar karşısında ne tür haklara sahip olduğunun bilgisi verilmeli, gerekli hallerde yazılı rızası alınmalıdır. Fakat burada altının çizilmesi gereken bir nokta vardır. Kişiyi; verilerin neden kullanılacağı, nasıl işleneceği ve diğer konular ile ilgili bilgi verilmemesi halinde onun bununla ilgili bilgi talep etmesi gerekmektedir. Ayrıca kişinin bu bilgilerin erişilebilir ve işlenebilir olmasına rıza göstermesi esnasında hiçbir baskı altında kalmaması, tamamen kendi iradesi ile buna rıza göstermiş olması şarttır (Ayözger, 2016: 120-121).

1.8.3. Kişisel Verilerin İşlenmesinde Bilgi Edinme, Düzeltme, Sildirme, Engelleme Hakkı İlkesi

Kişisel verilerini paylaşan bireylerin bu bilgileri istediği zaman sildirme, düzeltme, bilgi edinme, engelleme hakkı saklıdır ve bu haklar yasal olarak kendine zemin bulur. İnsanların, kendileri ile ilişkili verilerin kayıt altında olup olmadığını ve bunların kaydı yapılıyor ve işleniyorsa ne amaçla işlendiğini sorma hakları bulunmaktadır. Her zaman, ilişki içinde olunan her kuruma bu soruları yöneltmek mümkündür ve bu en önemli bilgi edinme hakkıdır. Bir diğer bilgi hakkı ise hali hazırda kaydedilen ve diğer işleme faaliyetlerine maruz kalan bilgiler hakkında nedenleri öğrenmedir. Ayrıca işleme faaliyetlerinin direktiflere ve mevzuata uygun olup olmadığını sorgulama, belirli bir hata ya da sorun söz konusu ise bunu düzelttirme, değiştirtme ya da sildirme hakkı da yine veri sahibinindir (Çokmutlu, 2014: 105).

Tüm bu durumlar tüzel kişiler için de geçerlidir. İşletmeler ya da işletmeler ile devlet arasında veri akışı gerektiren faaliyetler esnasında kişisel verilere ilişkin ilkelerin geçerlidir. Bireyler ve şirketler, verilerinin işlenmesi ile ilgili amacı reddetme ya da bu amaç için veri vermeyi kesme hakkına sahiptirler. Şayet verilerin amaç dışında işlendiğine dair bir kuşku var ise buna ilişkin şikâyet etme haklarının olduğunu da söylemek gerekmektedir. Birey veya tüzel kişi, işlemeyi gerektiren sebepler ortadan kalktığında verilerin silinmesini talep edebilir. Kişisel verilerin aktarıldığı üçüncü kişilerin, kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesinin ve işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerinin silinmesinin veya yok edilmesinin talep edilebileceği hususlarında bilgilendirilmelerini isteme de yine kişiye verilen bir haktır. (Nalbantoğlu, Özkaya2016:15)

Gerçek ya da tüzel kişinin kendisine ilişkin bilgilerini saklama, paylaşma ya da çeşitli şekillerde yönetme hakkı mevcuttur ve aslında bu durum ulusal ve uluslararası hukuk kuralları ile güvence altına alınmaktadır. Kimi kurumların veri toplama amaçları kişiye hizmet etmekte ancak bir süre sonra kişi bu hizmetten faydalanmayı bırakmak isteme hakkına sahip olabilmektedir. Böyle durumlarda gerçek ya da tüzel kişinin verilerinin silinmesi/imha edilmesi konusunda isteği yerine getirilmeli ve kendisine bu konuya ilişkin güvence verilmelidir (Henkoğlu, 2015: 162).

1.8.4. Veri Güvenliđi İlkesi

İnsanların verilerini verdikleri kurumların, onlara verileri hangi amaçlar için aldıkları ve nasıl saklayacakları konusundaki politikalarını açıklamaları gerekmektedir. Verilerin güvenliđi dođal afetler, siber saldırılar, bilgisayar ya da kayıt sistemlerindeki aksaklıklar, dikkatsizlik ya da kötüye kullanım nedeni ile tehlikeye girebilecektir ve tüm bunlar için ayrı önlemler alınmalıdır. Kişi istediđi takdirde bu önlemler hakkında detaylı bilgi edinme hakkına sahip olmalıdır (Kılınç, 2012: 1112).

Veri güvenliđi, bugün özellikle şirketlerin gerçek ya da tüzel kişi olan müşterilerine sundukları bir pazarlama yöntemi haline gelmiştir. Pek çok işletme veri güvenliđini sağlayamaması halinde sorumluluđu olduğunu kabul etmiş ve yasal işlemlerin sonucunda ödemesi gerektiđinin dışında müşterisine yaptırım dahilinde maddi ödemeler yapacağını da taahhüt eder hale gelmiştir. Bu sayede müşterilerinin güvenini kazanmak ve rakiplerini elemek istemektedirler. Özellikle tüzel kişilerin verilerinin bir başka şirket tarafından korunamaması, büyük miktarlarda maddi zararlar anlamına gelebilecektir ve işletmeler arasında gerçekleşen faaliyetlerde kişisel bilgilerin işlenmesi gerektiğinde şirketler birbirlerine zararlarını karşılama sözü verebilmektedirler. Bunun nedeni, işletmelerin verilerinin dışarı aktarılması halinde ne kadar maddi zararlara uğrayacağını günümüzde istatistiksel olarak bilinmesidir. ABD’de Ponemon Enstitüsü tarafından 2007 yılında yapılan bir araştırmada, şirketlerin kişisel verilerinin sızdırılması halinde milyarlarca dolar zarara edildiđi görülmüştür. Ülkemizde kişisel verilerin korunması alanında uzman olan ve faaliyet gösteren Intellect firması da bu bilgiyi desteklemektedir (Vural ve Sarıođlu, 2010: 72). Buradan da görüldüğü üzere, artık kişisel verilerin korunmasını sağlayan işletmeler de mevcuttur.

1.8.5. Amaçla Bağlılık İlkesi

Kurumların kişisel verilere ilişkin politikalarında olmazsa olmaz olan bir konu da amaca bağlılıktır. Kişisel verilerin toplanması ve korunması ile yapılan diđer tüm işlemlerin neden yapılacağı önceden belirlenmeli ve bu amaç kesinlikle hukuki kurallara uygun olmalıdır. Bu amaçlar güvenilir ve meşru olmalıdır. Amaçlar

belirlenirken, veri paylaşımı yapan kişinin kafasında soru işareti bırakacak ifadeler olmamalıdır. Tüm ifadeler somut biçimde ortaya konulmalıdır. Amaçların somut şekilde ortaya konulmaması, bireyin kendine ait veriler konusunda kontrolünü kaybetmesi anlamına gelecektir (Kuşkonmaz, 2013: 89).

Kişilerin verilerinin toplanması ve işlenmesi esnasındaki amaç değişimi söz konusu olduğunda, otomatikman kişinin rızası da ortadan kalkmış olacaktır. Örneğin devletin suçu tespit etmek için aldığı bir DNA örneğini, başka amaç ile kullanması düşünülemez. Fakat amaca bağlılık ilkesi, yeni amacın eski amacı tamamlayıcı şekilde olması halinde istisna haline dönüşecektir ve yeni amaç ile eski amaç arasında belirgin bir ilişki olması halinde yeniden rıza alma şartından söz etmeye gerek yoktur (Ayözger, 2016: 123).

Verilerin kişiye belirtilme amacı dışında kullanılması sosyal problemlerin yanı sıra bilginin suiistimal edilmesi riskini de taşıyabilmektedir. Şayet söz konusu ticari veriler ya da proje verileri gibi tüzel kişilere yönelik bilgiler ise bu durum ilgili şirketin rekabet avantajlarını kaybetmesi anlamına gelebilecektir. Örneğin bir fikrin ya da pazarlama stratejisinin hedeflenen zamandan önce dışarıya aktarılması, başka işletmelerin bu bilgiyi kullanmasına neden olabilecektir. Tüzel kişiler arasında olan bilgi akışında ya da gerçek kişi ile tüzel kişi arasında yapılan iş sözleşmesi, ortaklık ve benzeri faaliyetlerde veri güvenliğinin korunması esnasında amaç dışı kullanım konusuna çok dikkat edilmesi gereklidir.

Bu noktada amacın meşru olması gerektiğinden de söz etmek lazımdır. Bunun dışında kalan ya da net olarak ifade edilmeyen amaçlar hukuka aykırıdır. Amacın hangi şartlarda meşru sayılacağına ilişkin düzenlemeler de 1995/46/EC VKD Md. 7'de açıklanmıştır (Ayözger, 2016: 125).

Amaçla bağlılık başta olmak üzere, diğer tüm ilkelerin sağlanabilmesi, veri güvenliğinin sağlanması ile mümkün olacaktır. O halde veri toplama ve saklama yetkisine sahip tüm organların güvenliğe ilişkin riskleri belirlemesi ve bunlar hakkında önlemleri alması şarttır denebilir. Bu çalışmanın ilerleyen bölümlerinde de görüleceği üzere, kişisel verilerin korunmasına ilişkin ilkelerin tümü, hemen her uluslararası ve ulusal düzenlemede benzerlik göstermektedir.

1.8.6. Ölçülülük İlkesi

Ölçülülük, kişisel verilerin toplanması esnasında aslında sınırların çizilmesine olanak tanımaktadır. Kimi kaynaklarda orantılılık ilkesi olarak da adlandırılan bu ilke, her ne amaçla olursa olsun, toplanan verilerin asgari düzeyde olması amacına hizmet etmektedir. Ölçülülük ilkesi sayesinde, bilgiye erişimin hangi aşamaya kadar gerçekten gerekli olduğuna da yanıt verilmektedir. Özellikle dijital dünyada, uygulamaların çalıştırılması için pek çok izin istenmektedir. Mesut Serdar Çekin, bir cep telefonu fener uygulaması ile bunu örneklendirmektedir. Yazar, bu uygulama için fotoğraflar, rehber, kişiler, mesajlar gibi pek çok yere erişim izni istendiğini hatırlatmakta ve ölçülülük ilkesinin önemine dikkat çekmektedir. Kişilerin, bir uygulama çalıştırmak için gereken tüm iznlere gerçekten ihtiyaç olup olmadığını sorgulayabilmelerinin verilerin ölçülülük ilkesi dahilinde işlenip işlenmediğini kontrol etmek için geçerli olacağını savunmaktadır. (Çekin, 2016: 637).

Ölçülülük ilkesi sayesinde kişisel verinin işlenme amacı ile uygunluğunun olması, veri amacının gerçekleşmesi için gerekli olmasının şartı haline gelmektedir. Bu ilke, gereksiz bilginin toplanmasını ve bilgi kirliliğini de önlemektedir. Bu ilke değerlendirilirken amaç ile kişisel veri arasındaki illiyet bağı kavramı ile bu ilişki anlatılmaya çalışılmaktadır. Orantılılık ilkesi gereği, her verinin işlenmesinde, söz konusu verinin işleme amacı için uygun olup olmadığı ve söz konusu verinin işlenmesinin amacın gerçekleşmesi için gerekip gerekmediği her somut olayda incelenmelidir. (Bu inceleme esnasında yapılması gereken, kişisel verilerin toplanmaya başladığı anın amacı, sonrasında değişen bir amaç söz konusuysa yeni amaç, her iki amaç arasındaki bağlantı, kişisel verilerin toplandığı bağlamda ve veri sahiplerinin ileri safhadaki kullanım konusundaki beklentileri, ne tür verilerin toplandığı ve işlendiği ve bunların işleme sürecinin her safhası için gerekliliği gibi detaylara dikkat edilmesidir). İncelemelerin sonrasında uygunluk tespit edilse dahi, ölçülülüğün sürekliliği ve veri sahiplerinin sorun yaşamamaları için gereken önlemlerin alınması da şarttır (Ayözger, 2016: 126). Bu ilkeye ilişkin tartışmalar devam etmektedir çünkü bir bilginin gerekliliği tartışmaya ve farklı kişilerce farklı şekilde yorumlanmaya açık bir durum haline gelmiştir. Mahkemelerin bu ilkeyi birbirinden farklı yorumladığı da unutulmamalıdır (Kılınç, 2012: 1130).

1.8.7. Sorumluluk İlkesi

İnsanların kendilerine ait hangi verilerin tutulduğu, bunların ne amaçla işlendiği ne kadar süre ile saklandığı gibi soruları sorabilme ve bunların işlenmesi neticesinde zarar görmeleri halinde tazmin edilmesini isteme hakkına sahiptir. İşte bu noktada bir sorumlunun varlığı söz konusudur. Kişinin kişisel verilere ilişkin mahkemeye başvurması halinde karşıda bir sorumlunun var olması gerekmektedir. Ancak bu noktada çeşitli görüşler de söz konusudur. Çekin konuya şu şekilde yaklaşmaktadır: “Öncelikle tazminat hususuna bakıldığında kanunda öngörülen mekanizmanın bir kusur sorumluluğu hali olduğunu kabul etmek bir hayli zor olacaktır. Nitekim kanun koyucu kusur şartını aramamıştır. Kanaatimizce ilgili hükümde öngörülen tazminat yükümlülüğünün bir sebep sorumluluğu niteliği taşıdığını kabul etmek daha isabetli olacaktır. Zira veri sorumlusu, Md.12’de öngörülen şartları yerine getirdiği takdirde ilgili kişiyi hala mesul kılmanın bir anlamı olmayacaktır. Bu sebeple kural olarak zarar meydana geldiğinde veri sorumlusunun Md. 12’de öngörülen yükümlülüklerini yerine getirmediği kabul edilmeli, ancak veri sorumlusunun ilgili hükümde öngörülen bütün koşulları yerine getirdiğini ispat etmesi halinde kendisine kurtuluş imkânı tanınmalıdır” (Çekin, 2016: 637).

Bizim kanaatimizce de tazminat sorumluluğunun bir sebep sorumluluğu olduğunu kabul etmek değerlendirme açısından daha doğru olacaktır. Veri sorumlusu yükümlülüklerine uyduğu takdirde ve bunu ispatladığında tazminat açısından tek sorumlu olmaktan kurtulabilmelidir.

İKİNCİ BÖLÜM

KİŞİSEL VERİ HUKUKU, ULUSLARARASI DÜZENLEMELER VE TÜRK HUKUKUNDAKİ YERİ

2.1. Kişisel Veri Hukukunun Tarihsel Gelişimi

Kişisel veriler, üretilmekte, depolanmakta ve yer yer üçüncü kişiler ile paylaşılmaktadır. Ancak bunların hangi şartlarla gerçekleştirileceğine dair düzenlemelerin yapılmaması, hem bilgi kirliliği, hem yanlışta ve yanlışta hem de kişinin kendisine ilişkin özel bilgilerin açığa çıkması risklerini taşımaktadır. Bu durum toplumsal ve bireysel sorunlar anlamına geleceğinden, kişisel veri hukukuna ihtiyaç duyulmuştur.

Özellikle 1970'li yıllardan itibaren bilgi üretimi ve iletimi hız kazanmıştır ve verilerin nasıl korunacağına ilişkin ulusal ve uluslararası düzenlemelere daha fazla önem verilmeye başlanmıştır. Kişisel verilerin korunmasına ilişkin kurallar ilk toplumlarda bile vardır. Özellikle hekimler, hastalarının gizli kalmasını istedikleri bilgileri saklamak mecburiyetinde olmuşlardır ve bu durum kişisel verilerin gizliliğine ilişkin ilk uygulama örneklerinden biri olarak kabul edilebilir. Ancak yasal düzenlemeler öncelikle OECD, ardından Avrupa Konseyi ve sonrasında ise Birleşmiş Milletler tarafından önerilmiştir.



Şekil 4. OECD, AK ve BM Bünyesinde Kişisel Verilere İlişkin Yapılan Yasal Düzenlemeler

Kaynak: Boz, 2014: 44.

2.1. Genel Olarak

Kişisel verilerin insanlar arasındaki ilişkilerde bir rol oynamasının yanı sıra özellikle bankacılık sektöründe ve dolandırıcılık gibi suç teşkil eden alanlarda kullanılmasına ilişkin olayların artması, konuya ilişkin yasal düzenlemelerin de zorunlu hale gelmesine neden olmuştur. Yasal düzenlemeler, kişisel verilerin nasıl toplanacağı, saklanacağı, bu alandaki sorumluluklar ve üçüncü kişilere hangi koşullarda aktarılması gerektiği gibi bilgi sızmalarına neden olabilecek olasılıkları ortadan kaldırmaya yöneliktir. 1960 ve özellikle 70'lerin sonrasında bilgi toplumu oluşmaya başlamış, toprak, işgücü ve sermaye gibi üretim girdilerinin önemi azalmaya başlamış ve bilgi en önemli kaynak haline gelmiştir. Bilginin sızması, onun sahibini maddi ve manevi zarara sokabilmektedir. Bu riskler, özellikle gelişime açık toplumlarda bilginin korunması konusunda ulusal ve uluslararası düzenlemeleri beraberinde getirmiştir (Aksoy, 2010: 4).

Hem ülkemizde hem de uluslararası alanda, bilginin nasıl güvende tutulacağına ve buna neden ihtiyaç olduğuna dair açıklamaları da içeren yasal düzenlemeler yapılmıştır ve ihtiyaçlar doğrultusunda bu yasalar düzenlenmekte ve geliştirilmektedir.

2.2. Uluslararası Belgelerde Kişisel Verilerin Korunmasına İlişkin Temel Düzenlemeler

Bilginin güvenliği konusunun önem kazanması ve konunun yasal düzenlemeler ile güçlendirilmesinin temelindeki ilk ve en önemli unsur kuşkusuz insan haklarıdır. Her bireyin, kendisine özgü olan bilgileri üretme, saklama ve istediği kişiler ile paylaşma hakkı mevcuttur. İnsan haklarından ve yaşanan teknolojik gelişmelerin doğurduğu sonuçlardan ve bilgi toplumunu oluşturan temellerden yola çıkarak OECD, Avrupa Konseyi ve Birleşmiş Milletler tarafından oluşturulan ve ülkelerin yasal düzenlemelerine rehberlik etme niteliğine sahip yasal düzenlemeler yapılmıştır. Bu başlık altında uluslararası düzenlemeler incelenmektedir.

Uluslararası hukukta kişisel verilerin korunmasına ilişkin olarak yapılan düzenlemeleri şu şekilde özetlemek mümkündür:

Tablo 1. Kişisel Verilerin Korunmasına İlişkin Uluslararası Yasal Düzenlemeler

Tarih	Düzenleme
3 Eylül 1953	İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi
23 Eylül 1980	OECD'nin Özel Yaşamın Korunması ve Kişisel Verilerin Sınır ötesi Akışına İlişkin Rehber İlkeleri
28 Ocak 1981	108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

14 Aralık 1990	BM'nin Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri
25 Ekim 1998	95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi
8 Kasım 2001	181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır aşan Veri Akışına İlişkin Protokol
2016	2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

Kaynak: KVKK, 2017:10.

2.2.1. Temel İnsan Haklarında Düzenlenmesi

Bilindiği üzere insan hakları, yalnızca insan olmaktan kaynaklanan doğal haklardır. Bunlar devredilemez ve dokunulamaz haklardır.

Tüm dünyada yasalar oluşturulurken, küresel düzeyde kabul görmüş olan temel insan hakları baz alınmalıdır. Bu alan incelendiğinde, insan haklarının 3 temel düzeyde toplandığı görülecektir. Bunlar (Ayözger 2016: 40),

i. Birinci kuşak haklar (kişilerin özgürlükleri ve siyasi hakları ile ilişkili haklardır),

ii. İkinci kuşak haklar (sosyal ve ekonomik hak ve özgürlükleri kapsamaktadır),

iii. Üçüncü kuşak haklar (dayanışma haklarıdır) şeklinde sıralanabilir.

Tarihsel süreç incelendiğinde sürekli gelişim gösteren insan hakları kavramı hukuk sistemlerinin ve modern yaşamın temeli olmakla birlikte günümüz dünyasının vazgeçilmez bir olgusu halindedir. İnsan hakları kavramı temel hali ve düzenlenme biçimleriyle birlikte değerlendirildiğinde insan hakları kavramının temelini oluşturan yaklaşımların tezimizle bağdaşan kısmı incelendiğinde; kişisel verilerin korunması hakkının temelini oluşturan ana düşünce daha net anlaşılacak ve ortak değerlendirilmesi daha kolay yapılacaktır. Kişisel veri kavramı ve hakkının gelişimini temel insan haklarına ve insan hakları uygulamalarına dayandırmak yanlış olmayacaktır.

Bireyin kişisel verileri üzerindeki hakları ortadan kaldırıldığında bireyi bir hiç haline getirmek insan onurundan kaynaklı kişinin sahip olduğu öz değeri yok saymaktır ve bu durum insan onuru ile bağdaşmayan insan haklarına aykırı bir durumdur. (Şimşek, 2008 :131.) Dolayısıyla kişisel verilerin işlenmesi konusunda temel alınan nokta insan onuru ve insan haklarıdır. Bu sebeple kişisel verilerin korunması hakkının temeli insan hakları olarak kabul edilmelidir.

2.2.2. Ekonomik İş birliği ve Kalkınma Teşkilatı (OECD)

OECD özellikle 1970 ve sonrasında kişisel verilerin korunmasına verdiği önemi arttırmıştır. 1978 yılında kişisel verilerin güvenliğini izlemek amacı ile OECD içinde kurulan bir grup, ülkeler arasında kişisel veri aktarımı gerçekleştirilirken ne tür faaliyetler yürütülmesi gerektiği ve hangi detaylara önem verilmesi gerektiği konularını araştırmaya başlamıştır. 1980 yılında bu grup tarafından diğer ülkelerin mevzuatları için rehber niteliğinde olan “Gizliliğin ve Sınır Aşan Kişisel Veri Trafikinin Korunmasına Dair Kurallar” yayınlanmış, bu kurallar 2013 yılında “2013 OECD Gizlilik Kuralları” olarak yeniden düzenlenmiştir (Oğuz, 2015: 7-8).

Ekonomik İş birliği ve Kalkınma Teşkilatı, kişisel verilerin korunma hakkı konusunun doğrudan doğruya ele alınması ve buna ilişkin yasalar oluşturulması konusunda ilk adım atan oluşumdur. OECD tarafından hazırlanan Gizliliğin ve Sınır Aşan Kişisel Veri Trafikinin Korunmasına Dair Kurallar rehber niteliğindedir ve hiçbir bağlayıcılığı bulunmamaktadır (Bük, 2015: 55).

OECD tarafından hazırlanan bu kuralların 2. Bölümünde Ulusal Uygulama Temel İlkeleri başlığı altında ülkelerin yasal düzenlemeler yaparken hangi ilkelere bağlı kalınması gerektiğine ilişkin bilgiler yer almaktadır. Bu temel ilkeler sekiz adettir ve şu şekildedir (Boz, 2014: 44-45):

i. Sınırlı Bilgi Toplama:

Ulusal Uygulama Temel İlkeleri Md.7, veri toplamanın sınırlarına ilişkin bilgiler yer almaktadır. Bu ilkeye göre kurumlar ya da kişiler tarafından edinilen bilgilerin belirli sınırlar içinde kalması gerekmektedir. Veri toplama hukuki çerçevede gerçekleşmeli ve veri sahibi konuyla ilgili mutlaka bilgilendirilmelidir. Bilgi toplama esnasında hangi verilerin toplanacağı öncesinde netleştirilmeli, toplama işlemi hukuka uygun ve dürüst biçimde olmalıdır.

ii. Veri Kalitesi:

Veri kalitesi 8. Md. açıklığa kavuşturulmuştur. Verilerin geçerli ve güvenilir olması, kullanılacakları amaca hizmet edecek şekilde toplanması gerekmektedir. Bu noktada amacın ne olduğu, verilerin amaca uygunluğunun güncel olup olmadığı, verilerin kesinliği gibi detayların da kontrol edilmesi gerektiği belirtilmektedir.

iii. Amaca Özgülük:

9. Md. amaca özgülük ilkelerini belirlemektedir. Bu maddeye göre, toplanan verilerin hangi amaçla toplanacağı ve toplanan verilerin amaca hizmet edebilirliği net olarak belirlenmelidir. Veri toplama amacı somut olmalıdır ve yorum yapılabilir biçimde olmamalıdır. Kullanım amacı kimi zaman verinin toplanmasından sonra değişebilmektedir. Böyle durumlarda yeni amaç hakkında veri sahibine bilgi verilmelidir. Kişisel verilerin toplanmasının veri sahibine zarar verme olasılığı mevcutsa, bununla ilgili bilgilendirmenin de

yapılması şarttır. Ayrıca madde, yeni amacın eski amaç ile uyumlu olması gerektiğinin de altını çizmektedir.

iv. Kullanım Sınırlaması:

Kullanım amacı dışında bilgilerin asla kullanılmaması gerekmektedir. Kullanım sınırlamasına ilişkin istisnalar söz konusu olduğu takdirde, veri sahibinin bilgilendirilmesi şarttır.

v. Güvenlik Önlemleri:

Toplanan verilerin saklanması esnasında dikkatli olunmalıdır. Çalınma, değiştirilme ya da amaç dışında kullanıma gibi olasılıklara ilişkin gerekli önlemler alınmalıdır.

vi. Açıklık:

Kişisel verilerin alınması ve sonrasında, bunlarla ilgili tüm gelişmeler için genel bir açıklık ilkesi oluşturulmalıdır. Bireyler, kendi verilerini barındıran kurum ve kuruluşların açıklık ve gizlilik politikalarına ilişkin detaylara kolaylıkla ulaşabilmelidirler.

vii. Bireyin Katılımı:

Kişinin rızası veri depolamanın odak noktasıdır. Bireyin izni olmaksızın verilerin ulaşılabilir olması mümkün olmamalıdır.

viii. Hesap Verebilirlik:

Kişiler yukarıda sayılan tüm maddelere ilişkin her zaman hesap sorma hakkına sahip olmalı, gerekli hallerde verilerini alabilmeli ya da değiştirebilmelidirler.

OECD tarafından konuyla ilişkili olarak yapılan düzenlemeler elbette bunlarla sınırlı değildir. 1985 yılında Sınır Ötesi Veri Akışı Bildirisi, 1992’de Bilgi Sistemlerinin Güvenliği İçin Rehber İlkeler, 1997’de Kriptografi Politikası Rehber İlkeleri ve 1998 yılında ise Küresel Ağlarda Mahremiyetin Korunmasına İlişkin Bakanlar Konseyi Bildirisi yayımlanmıştır (Uygun, 2010: 25).

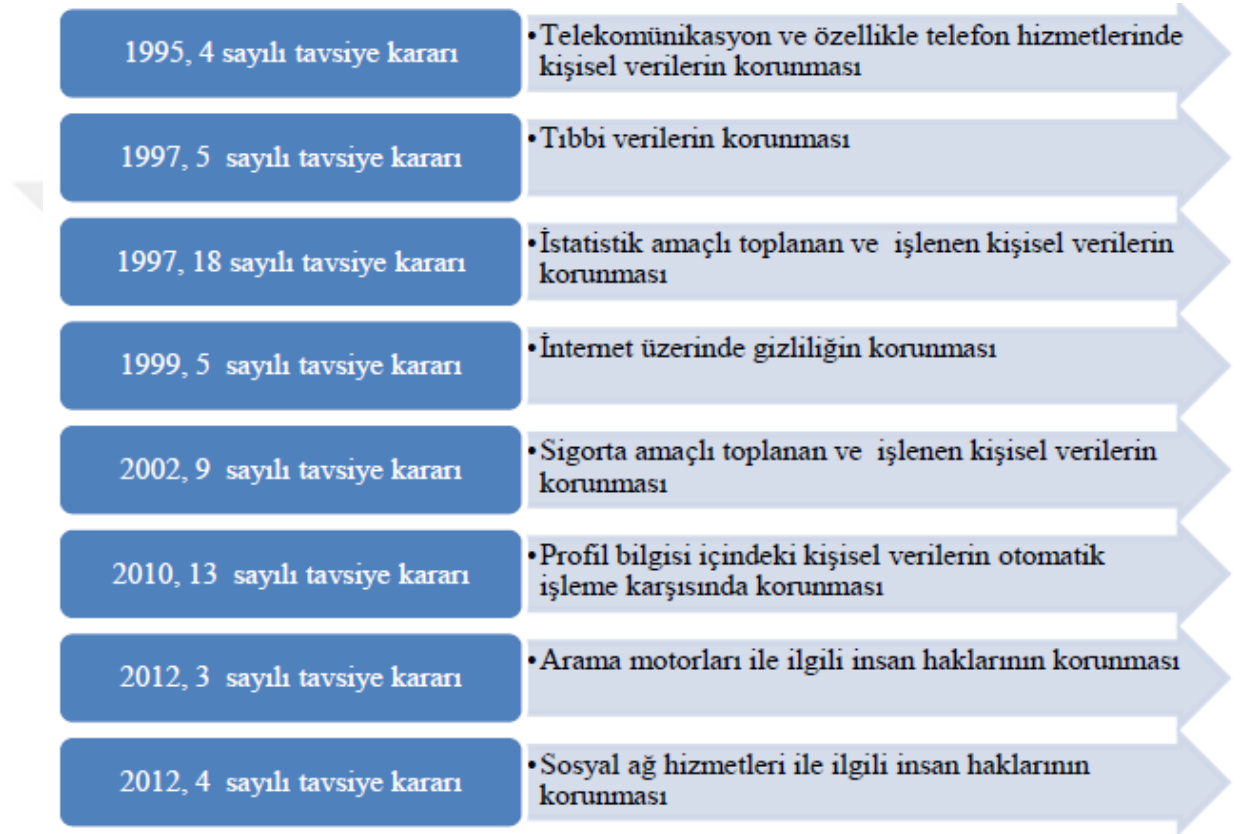
2.2.3. Avrupa Konseyi ve Avrupa Birliđi

1949 yılında 2. Dünya Savaşı sonrasında Avrupa’da yer alan ülkeler arasındaki anlaşmazlıkların yok edilmesi ve ülkeler arasındaki çatışmaların sonlandırılması amacı ile kurulan Avrupa Konseyi, insan hakları temelinde çođulcu demokrasinin yerleřtirilmesi, yasaların oluşturulması ve sosyal sorunlara çözümler bulunmasına hizmet etmektedir. Konsey kararları, üye ülkelerin kendi yasal düzenlemelerini nasıl gerçekleřtireceklerine dair rehberlik etmektedir. 1981 yılında ilk defa kişisel verilerin korunması konusu burada ele alınmış ve 108 Sayılı “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme” kabul edilmiştir (Boz, 2014: 46).

Bu sözleşme temelde “Modern Bilimsel ve Teknolojik Gelişmeler ve İnsan Hakları Hakkında 509 sayılı Tavsiye Kararına” bađlıdır. Ana amaç, üye olan ülkelerin standart bir veri koruma hukuk sistemi oluşturmalarını sağlamaktır. Ayrıca bu sözleşme ile insanların temel hak ve özgürlüklerinin korunma altına alınması da hedeflenmektedir. Avrupa İnsan Hakları Sözleşmesi’nde kişisel verilerin korunmasına ilişkin bađımsız bir konu başlıđı bulunmamaktadır ve 108 Sayılı Sözleşme aslında bu açığı kapatmaktadır. Sözleşmenin 5. maddesi geređince, verilerin tamamı adil ve hukuka uygun şekilde edinilmiş olmalıdır. Ayrıca verilerin özel ve meşru amaçlar ile saklanması, amaç dışında kullanılmasının yasak olduđunun altı çizilmektedir. Gereksiz bilgiler istenmemeli, veri sahibine belirtildiđi şekilde, dođru ve belirlenen tarihe kadar saklanabilecektir. Sözleşmenin 7. maddesi, kişisel verilerin saklanması gerekliliđine ve bu konuda alınması gereken güvenlik önlemlerine dikkat çekmektedir. Bunun yanında 5, 6 ve 8. maddeler verilerin gizliliđi esnasında ortaya çıkabilecek istisnai durumları açıklamaktadırlar. Örneđin, Devletin veya kamunun güvenliđinin veya devletin önemli malî çıkarlarının korunması veya suçun önlenmesi, söz konusu ise veri güvenliđini tehlikeye atmak ya da kişisel verileri gerekli yerler ile paylaşmak mümkündür (Bük, 2015: 56).

2004 yılında, 181 Sayılı “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşmeye Ek Protokol”

imzalanmıştır. Ek Protokol ile amaçlanan kişisel verilerin güvenliğinin artırılmasıdır. Ayrıca bu ek protokol, sözleşmeye taraf olan ülkelerde veri güvenliğinin yasal düzenlemelerini izlemesi için bağımsız bir otorite oluşturulmasına olanak tanımıştır. Tüm bunların yanında yurt dışına veri transferi konusu da ele alınmıştır (Boz, 2014: 51-52).



Şekil 5. AK Bakanlar Komitesi Tavsiye Kararları

Kaynak: Boz, 2014: 54.

Avrupa Konseyi, Bakanlar Komitesi tarafından tavsiye kararları ile veri güvenliğine ilişkin hukuki düzenlemeler artırılmıştır. Bakanlar Komitesi ülkelerin hükümetlerinin temsilcileri ile olduğundan, alınan kararlar demokratik bir ortamda alınmakta ve üye ülkelerin tamamı görüş belirtebilmektedir. Bakanlar Komitesi kararlarını uygulama zorunluluğu bulunmamaktadır ancak Komite uygulamaya ilişkin

üye ülkeleri izleyebilme hakkına da sahiptir. Bu sayede üye ülkelerin kararları nasıl uygulayacağı konusunda özgürlük tanınmış olmaktadır (Boz, 2014: 53).

Avrupa Birliği'nde ise amaç Avrupa ülkeleri arasında barışın sağlanması ve ekonomik bir birliğin oluşturulmasıdır. 2009 yılında imzalanan Lizbon Antlaşması, kişisel verilerin korunmasına ilişkin önemli bir adım olarak görülmelidir. Bu antlaşmada, AB'nin İşleyişine İlişkin Sözleşme (Treaty on the Functioning of the EU) ile AB Antlaşması (Treaty on EU) birleştirilmiş ve verilerin korunmasına ilişkin yeni düzenlemeler yapılmıştır. Yeni yapı, güvenlik konusu Avrupa Birliği'ni oluşturan ülkelerin kanunlarında veri güvenliğine ilişkin konular hakkında değişiklik yapılmasını da zorunlu hale getirmiştir. Antlaşmada, kişisel verilerin korunmasının insani bir hak olduğu da kabul görmüştür. AB'nin kişisel verilere ilişkin düzenlemeleri içeren en önemli metinleri şunlardır; (Kuşkonmaz, 2013: 67-68):

i. Avrupa Birliği Temel Haklar Şartı:

Bu şartın 7. maddesi kişisel verilerin korunması hakkı ile doğrudan ilişkilidir. Madde, “herkes özel ve aile yaşamına, evine ve iletişimine saygı gösterilmesini isteme hakkına sahiptir” demektedir. Buradaki iletişim ibaresi çok önemlidir. Geliştirilebilecek tüm teknolojilere uyum sağlayabilmesi amacı ile eskiden haberleşme olarak düşünülen tüm mekanizmalar bu maddede iletişim adı ile anılmaya başlanmıştır.

AİHS' de kişisel verilerin korunması, ayrı bir hak alanı olarak düzenlenmemiş olduğunun ancak AİHM'nin verdiği kararlarla, kişisel verilerin korunmasında temel ilkelerin büyük bir bölümünü, Sözleşme'nin 8. maddesi kapsamında değerlendirmekte olduğu açıktır (Küzeci, 2014:4).

Şartın 8. maddesi ise “Kişisel Verilerin Korunması” başlığına sahiptir. Bu madde herkesin kendisine ilişkin bilgileri koruma ve saklama konusunda hak sahibi olduğunu düzenlemektedir. Ayrıca, bu bilgilerin kullanılması esnasında kişinin rızasının alınması da zorunlu hale getirilmiştir. Yine aynı maddeye göre

kamu kurumları ile özel sektör kuruluşlarının kişisel verileri toplaması ve saklanması konusunda geçerli bir nedenlerinin olması gerekmektedir.

ii. 95/46/AT Sayılı Kişisel Verilerin Korunması Direktifi:

1995 yılında kabul edilen 95/46/AT Sayılı Kişisel Verilerin Korunması Direktifi AB’de kişisel verilerin korunmasına dair yapılan en önemli hukuki düzenlemelerden biridir. Bu direktifin şartlarına üye ülkelerin tamamının uyması bir zorunluluktur. Çünkü direktif devletin yasal düzenlemeleri içinde kişisel verilerin korunmasına ilişkin yaptırımların olmaması halinde tam bir korunma sağlanamayacağını altını çizmektedir. Direktif, özel hayatın gizliliğine saygı duyulması ve kişisel verilerin yönetiminin bireyin tekelinde olması konularının altını çizmektedir. Ayrıca ülkelerin veri koruma konusunda oluşturdukları politikalar ve veri koruma düzeyleri konusunda alınması gereken önlemler ve uyulması gereken asgari standartları da belirlemektedir (Ayözger, 2016: 80).

iii. 2002/58/EC Sayılı Elektronik Veri Koruma Direktifi:

Bu direktifin amacı, “Üye ülkelerin, elektronik haberleşme sektöründe kişisel bilgilerin işlenmesine ilişkin olarak temel hak ve özgürlüklerin, özellikle de gizlilik hakkının eşit ölçüde korunmasını ve Birlik içinde bu tür veriler ile elektronik haberleşme ekipmanı ve hizmetlerinin serbest bir şekilde dolaşmasını sağlamasını gerektiren hükümleri uyumlaştırmaktır” (Ayözger, 2016: 86).

Bu direktif ile tüzel kişilerin kişisel verileri de güvence altına alınmaktadır. Ayrıca gelişen teknoloji karşısında veri güvenliğine ilişkin ilkelerin yetersiz kalmasının da önüne geçilmesine çalışılmaktadır. İnternet üzerinde çerez ve konum belirleme gibi faaliyetler karşısında kullanıcının uyarılması ve

bilgilendirilmesine ilişkin düzenlemeler de yine bu direktif ile belirlenmektedir (Şahin, 2011: 36).

iv. 2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR):

Bu tüzük gelişen teknoloji ile birlikte yasal düzenlemelerin geliştirilmesi amacına dayanmaktadır. 95/46 sayılı Direktifi ilga edecek olan ve Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu tarafından yapılan tüzük 2016 yılında kabul edilmiş olup, 25 Mayıs 2018 tarihinde 95/46 sayılı Direktifi ilga ederek yürürlüğe girmiştir.

v. 95/46/EC Sayılı Kişisel Verilerin Korunması Direktifi

1995 yılında kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması hakkındaki 95/46/EC sayılı direktif oluşturulmuştur. Direktifin ilk maddesinde Topluluğun demokrasiye verdiği önem ve bu direktif ile kişisel verilerin demokratik ortama yakışır şekilde korunmasının öneminin vurgulanacağı belirtilmiştir. İkinci madde, veri işleme sistemlerinin insana hizmet etmek üzere tasarlanması gerektiğinin altını çizmektedir. Direktif 'in 3. Md. İnde küreselleşmenin bir sonucu olarak uluslararası faaliyetlerin kişisel verilerin dolaşımına zemin hazırladığı belirtilmiş ve bunu korumanın devletlerin görevi olduğunun altı çizilmiştir. 4. Md.; teknolojik gelişmelerin kişisel verilere ilişkin güvenilirliği ortadan kaldırdığını ve insanların bunu şikâyet ettiğini belirtmektedir. Toplulukta yeni haberleşme ağlarının eşgüdümlü uygulanması ve bilimsel ve teknik iş birliğindeki artış, kişisel verilerin sınır ötesi akışını gerektirmekte ve kolaylaştırmaktadır diyen direktif; devletlerin üyeliğin bir şartı olarak kişiyi ve onun haklarını koruması gerektiğini vurgulamaktadır. Korumanın esasları; bir taraftan, başta işlemenin yürütülebileceği koşullar ve denetleme makamına bildirim, teknik güvenlik ve veri kalitesi olmak üzere işlemeden sorumlu diğer kuruluşlar veya kişiler, kamu makamları, işletmeler, temsilciler üzerine yüklenen yükümlülöklere ve diğer

tarafından, bireylere verilen haklara, işlemin konusu olan verilere, işlemin yapıldığını bildirmeye, verileri danışmaya, düzeltme talep etmeye ve hatta bazı koşullarda işlemeye itiraza yansıtılmalıdır diyen direktif; kişisel olan her türlü verinin bu direktifin kapsamı içinde olduğunu da belirtmektedir (www.kişiselveri.com).

2.2.4. Birleşmiş Milletler

İkinci Dünya Savaşı, ülkelerde ortaya çıkan herhangi bir siyasal ya da ekonomik sorunun diğerlerini de kolaylıkla etkileyebileceğini göstermiştir. Bunun dışında özellikle küreselleşmenin ticari faaliyetleri arttırdığı ve ülkelerin bu nedenle hem ticaret hem de dostluk ilişkileri kurmasının her iki tarafa da faydası olacağı görülmüştür. Birleşmiş Milletler, sorunlara ortak çözümler sunmak, ortak kaynak oluşturmak, ülkeler arasında doğabilecek problemlerin çözümünde görev alacak bir merkez oluşturmak, dostluk ilişkileri kurmak, korumak ve onları geliştirmek amacı ile kurulmuştur. BM üyeleri, bu merkezin oluşturduğu kurallara da uymak durumundadırlar. Bu durum eşit standartların oluşturulmasını da desteklemektedir (Aydın, 2014: 28).

“Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler” 1990 tarihinde BM tarafından kabul edilmiştir. Bu belgedeki ilkeleri şu şekilde özetlemek mümkündür.

i. Yasallık ve Dürüstlük:

Kişisel verilerin toplanması esnasında yasal koşullara uygun davranılmalı ve kural dışı biçimde asla veri toplanılmamalıdır. Ayrıca toplanan verilerin toplanma amacı dışında kullanılması kesinlikle yasaktır (Ayözger, 2016: 71).

ii. Doğruluk:

Veri toplama esnasında elde edilenlerin doğru olup olmadığının kontrol edilmesi gerekmektedir. Ayrıca elde edilen veriler eksiksiz ve doğru şekilde

saklanmalıdır. Güncelliğın sađlanması için rutin aralıklar ile verilerin dođru olup olmadıđı da kontrol edilmelidir.

iii. Amacın Belirli ve Haklı Olması:

Kişisel verilerin neden toplanacağı en başında çok açık ve net şekilde belirlenmesi ve konuyla ilgisi olan herkese açıklanması gerekmektedir.

iv. İlgili Kişilere Erişme Hakkı:

Kişisel verilerin sahipleri, bunlara sahip olduklarını kanıtladıktan sonra kendileri ile ilgili verilerin ne amaçlarla kullanıldığını anlayabilmeli ve sorgulayabilmelidir. Verilerin kullanım amaç ve biçimlerine ilişkin bilgi edinirken kişinin aşırı zaman kaybetmesi ya da masrafa girmesi önlenmelidir (Kılınç, 2012: 1111).

v. Ayrımcılıktan Kaçınma:

Kişisel verilerin korunmasına ilişkin hiçbir ayrımcılık söz konusu olamaz. Ayrıca bireylerin ırkı, kökeni, dili, dini gibi detaylara ilişkin bilgiler yasal sınırlara uygun şekilde toplanabilecektir. Bu tür ayrımcılığa neden olabilecek hassas bilgilerin toplanması zorunluluk olmadığı takdirde yasaklanmalıdır (Kılınç, 2012: 1112).

vii. İstisna Koyma Yetkisi:

Görevli makamlara, milli güvenliği, kamu düzenini, halk sağlığını, genel ahlakı korumak veya diğer kişilerin hak ve özgürlüklerine zarar vermemek amacıyla yasallık ve dürüstlük, doğruluk, amacın belirli ve haklı olması, ilgili kişilerin erişme hakkı ilkeleri ile ilgili önlemlerden ayrılma yetkisi tanınabilecektir. Ancak bu yetkinin kapsamı ve sınırlamaları kanunlar ile belirlenmelidir. Ayrımcılıktan kaçınma ilkesine getirilecek istisnanın her durumda temel hak ve özgürlüklere aykırı olmaması çok önemlidir (Kuşkonmaz, 2013: 43).

viii. Güvenlik:

Kişisel verilerin toplanması ve saklanması ile ilişkili ve yetkili kurumların olası tüm riskleri değerlendirmesi ve önlem alması gerekmektedir. Bilgilerin dışarıya sızması doğal afetler, sistem hataları ya da kişilerden kaynaklanabilmektedir ve her olasılık göz önünde tutularak gerekli önlemler alınmalıdır.

ix. Denetim ve Yaptırım:

Kişisel verilerin nasıl toplandığı, korunduğu ya da paylaşıldığına ilişkin faaliyetlerin kontrol edilmesi, konu hakkında detaylı bilgi ve deneyim sahibi ve tarafsız organlar tarafından yapılmalıdır. Kanuna uygun olmayan haller tarafsız şekilde raporlanmalı ve yasalar çerçevesinde yaptırımlar uygulanmalıdır.

x. Sınır Ötesi Veri Transferi:

Kimi durumlarda kişisel verilerin bir ülkeden başka bir ülkeye aktarılması gerekmektedir. Bu tür durumlarda söz konusu ülkelerin mevzuatlarında kişisel veri transferine yönelik izinlerin uyumlu olması gerekliliği mevcuttur. Ayrıca gidecek olan verilerin, varacakları ülkede korunma şartlarının da en az verilerin geldiği ülkedeki standartlarda olması gerekmektedir. Aksi takdirde, kişiye kanunların taahhüt ettiği güvenlik risk altına girecektir (Kılınç, 2012: 1112).

Birleşmiş Milletlerin bu düzenlemelerinin hukuki bağlayıcılığının olmadığı bilgisi de vermek gerekmektedir. Ancak ülkeler arasında iş birlikleri esnasında sorunların oluşmaması için kuralların birbirine benzer olması gerekliliği ve küreselleşme, ülkelerin bu ilkelere uymalarını da zorunlu hale getirmektedir. Bu nedenle ülkeler bu tavsiye ilkelerine uygun biçimde kendi mevzuatlarını oluşturmaktadırlar (Aydın, 2014: 29).

2.3. Ulusal hukukta kişisel verilerin korunması hakkı

Ulusal ya da uluslararası hukukta kişisel verilerin korunması konusuna ihtiyaç duyulmasına neden olan en önemli etken teknolojidir. Teknoloji aracılığıyla, devlet kurumları ve özel kuruluşlar her gün binlerce kişinin bilgilerine ulaşabilir hale gelmişlerdir. Bu ulaşılabilirliğin denetlenmesi ve kurumların dışına çıkmaması için yasal düzenlemeler zorunluluk haline gelmiştir (KVKK, 2017: 8).

Yasal düzenlemeler Türk hukuk sisteminde kendine geç de olsa yer bulmuştur ve şu anda temel alınan yasalar uluslararası standartta kişisel veri korunması sağlanmasını amaçlamaktadır.

Tablo 2. Kişisel Verilerin Korunmasına İlişkin Ulusal Düzenlemeler

Tarih	Düzenleme
12 Ekim 2004	5237 Sayılı Türk Ceza Kanunu
12 Eylül 2010	Kişisel Verilerin Korunması ile ilgili hükmün T.C. Anayasası'na dahil edilmesi
17 Mart 2016	108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin Türk hukukuna dahil edilmesi
7 Nisan 2016	6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 29677 sayılı Resmî Gazete 'de yayımlanarak yürürlüğe girmesi
05 Mayıs 2016	181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır aşan

	Veri Akışına İlişkin Protokolün Türk hukukuna dahil edilmesi
--	--

Kaynak: KVKK, 2017: 11.

2.3.1. Anayasal Düzenleme

1982 Anayasasında kişisel verilerin gizliliğine ilişkin hükümlerin yer almaktadır. Fakat bu anayasada kişisel veriler, “özel hayatın gizliliği” başlığı altında ele alınmıştır ve gelişen teknolojik yapı ve bilgi toplumunun düzeni, modern topluma geçiş sürecinde özel hayat kavramının ve kişisel veri güvenliğinin yeterliliğini de sorgulatmaya başlamıştır. Kişisel verilerin güvenliğine ilişkin daha gelişmiş olan ülkeler de anayasada bu hakların özel hayatın gizliliği temeline değil, özgürlük temeline dayandırıldığı unutulmamalıdır (Çokmutlu, 2014: 119).

2010 yılında yapılan anayasa değişikliğinden önce kişisel verilerin korunması hakkı kelime ve kavram olarak olmasa bile anayasa ve çeşitli kanunlarda korunmuş ve yasal zemine oturtularak değerlendirilmiştir. (Kılınç, 2012: 1131).6698 sayılı özel kanunun çıkmasından önce kişisel verilerin korunması hakkı için öncelikle anayasa daha sonra yaptırım öngören yürürlükteki kanunlar uygulanmıştır ancak özel bir kanunun varlığına ihtiyaç duyulmuştur.

Bu ihtiyaca binaen kişisel verilerin korunması hakkının da içinde bulunduğu anayasa değişikliği niteliğindeki kanun tasarısı meclise sunulmuştur.5982 numaralı 2010 tarihli Kanun için 4. Yasama yılında 88. Birleşimden başlanarak tartışmalar yapılmış, 103. Oturumda tasarı Kanunlaşmıştır. 2/656 Esas Numaralı Kanun Teklifinin Özet Metni şu şekildedir (TBMM Arşiv):

“Anayasa Değişikliği Teklifi ile kadın-erkek eşitliğinin sağlanmasında Devletçe alınacak tedbirlerin eşitlik ilkesine aykırı yorumlanamayacağı ve toplumun bazı kesimlerinin sosyal devlet ilkesi gereği daha iyi korunması ve gözetilmesi

öngörülmekte, kişisel verilerin korunması, bireylerin yurt dışına çıkışlarıyla ilgili sınırlamaların daraltılması, çocuk haklarının anayasal temele kavuşturulması düzenlenmekte, sendikal haklar ve grevle ilgili bazı sınırlamalar kaldırılmakta, memurlara ve diğer kamu görevlilerine toplu sözleşme hakkı tanınmakta, siyasi partilerin kapatılması yeniden düzenlenmekte, bilgi edinme hakkı anayasal dayanağa kavuşturulmakta ve Kamu Denetçiliği Kurumu kurulması öngörülmekte, bir siyasi partinin kapatılmasına sebep olan milletvekilinin milletvekilliğinin düşmesine son verilmekte, Yüksek Askeri Şura kararları ile memur ve diğer kamu görevlilerine verilen uyarma ve kınama cezaları yargı denetimine açılmakta, askeri yargının görev alanı daraltılmakta, Anayasa Mahkemesi ve Hâkimler ve Savcılar Yüksek Kurulu yeniden yapılandırılmakta, Ekonomik ve Sosyal Konseyin kuruluşu anayasal dayanağa kavuşturulmakta ve Anayasanın Geçici 15 inci maddesi yürürlükten kaldırılmaktadır.”

Tam metni yukardaki şekilde olan 2010 anayasa değişikliği paketinde T.C. Anayasasında bazı maddelerin değiştirilmesine yönelik olarak kabul edilen 5982 sayılı kanunda kişisel verilere ilişkin ilk ve tek ifade 2. maddede geçmektedir. Madde, T.C. Anayasası'nın 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” demektedir (5982 sayılı kanun 2. Md.).

Anayasaların kişisel veri konusuna değinmesi ve bu konunun anayasalarda düzenlenmesi, kişisel verilerin güvenliğine ilişkin başlayan tartışmaların çok sonrasında denk gelmektedir. Bu nedenle genellikle anayasalar konuyu yüzeysel olarak ele almakta, ülkeler kişisel veri güvenliği konusunu yasalar ile desteklemektedirler.

2.3.2. Uluslararası Yükümlülükler

Türkiye Avrupa ülkeleri başta olmak üzere, dünya ile çeşitli ilişkiler içindedir ve uluslararası sözleşmelere taraftır. Kişisel verilerin korunmasına ilişkin gerekliliklerin bir kısmı halkın istekleri ve çağın gereklilikleriyken bir kısmı da

uluslararası hukuki düzenlemelere uymak ve ilişkilerini güçlü kılmak amacına hizmet etmektedir. Avrupa Birliđi ve Birleşmiş Milletler 'in rehber niteliğindeki düzenlemeleri ve AB müzakereleri, kanuni düzenlemeler ile kişisel verilerin korunmasını zorunlu hale getirmektedir.

Özellikle “108 Sayılı Sözleşme” adı verilen, Türkiye'nin 28 Ocak 1981 tarihinde imzaladığı ve 30 Ocak 2016 tarihinde onayladığı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi ile Avrupa Birliđi Komisyonu İlerleme Raporları, Katılım Ortaklığı Belgesi ve Türkiye Ulusal Programında Kişisel Verilerin Korunması ulusal alanda kişisel verilerin korunması yönünde acil adımlar atılmasını gerekli kılmıştır (Bük, 2015: 65 ve Turunç, 2016: 1).

i. 108 Sayılı Sözleşme

108 Sayılı Sözleşmeyi imzalayan Türkiye, sözleşme ile birlikte aynı anda iç hukukta buna uygun düzenlemeleri yapacağını ifade etmiştir. Bu sözleşmenin amacına uygun bir yasal düzenleme yapılması gerekmiştir. O halde bu noktada öncelikle sözleşmenin amacını açıklamak yerinde olacaktır. 108 Sayılı Sözleşme'nin amacı, Sözleşmeye taraf ülkelerde uyruđu veya ikametgahı ne olursa olsun gerçek kişilerin kişisel nitelikteki verilerinin otomatik bilgi işleme tabi tutulması karşısında özel yaşam hakkını güvenceye almaktır. Bunun yanı sıra, Türkiye sözleşmeyi imzalarken otomatik olarak işlenmeyen veriler konusunda da güvence sistemi kuracağını beyan etmiştir. Sözleşme ile Türkiye kişisel verilerin;

a. Adil yoldan ve tamamen yasal olarak elde edileceđi ve işleneceđi,

b. Verilerin toplanması esnasında önceden belirlenen amaçlara göre işlem yapılacağı, amaçların açıklanacağı ve verilerin amaç dışında kullanılmayacağı,

c. Amaçların uygun, yerinde ve aşırı olmayacak şekilde düzenleneceđi,

d. Verilerin güncel ve doğru olacağı,

e. Amaçlara hizmet ettiği sürece, veri sahiplerinin kimliğinin anlaşılacağı şekilde ancak süresi bittiğinde verilerin yok edilmek kaydıyla saklanacağı yönünde taahhütte de bulunmuş olmaktadır.

Buna ek olarak iç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel verilerin, otomatik işleme tabi tutulmayacağını, aynı şeyin ceza mahkûmiyetiyle ilgili kişisel veriler için de geçerli olduğu kabul edilmiştir (Turunç, 2016: 1-2).

ii. Avrupa Birliği Komisyonu İlerleme Raporları,

Daha önce de bahsedildiği gibi Türkiye'nin uluslararası ilişkileri, onun yasal düzenlemeler yaparak uyum sağlamasını da gerekli kılmaktadır. Avrupa Birliği Komisyonu İlerleme Raporu, Ulusal Programlar ve Katılım sürecinin bir gerekliliği olarak kişisel verilere ilişkin düzenlemeler yapmak durumundadır. Avrupa Birliği katılım süreci gereği, 1998 yılından sonra AB Komisyonu, ilerlemelerin izlenmesi adına raporlar hazırlamaktadır. Türkiye için bu süreç 2001 yılında başlamıştır. İlerleme raporları Türkiye'nin kişisel verilerin korunması konusunda eksikliklerinin olduğunu göstermiştir. AB, Türkiye'ye, üyeliğin gerçekleşmesi için bu konuda düzenlemeler yapması gerektiğini belirtmiştir.

iii. Türkiye Ulusal Programında Kişisel Verilerin Korunması

Ulusal Programlar da kişisel verilere yönelik düzenlemeleri gündeme getirmektedir. Bu programlar, AB'ne aday ülkelerin hazırladıkları ve Avrupa Birliği Komisyonuna sunularak, Katılım Ortaklığı Belgesinde yer alan ve öncelikle yerine getirilmesi istenilenlerin nasıl yapılacağına dair rapor mahiyetinde belgedir. Ulusal programların amacı AB üyeliğine girebilmek için ülkelerin eksiklerini tamamlamak amacıyla yardımcı olmaktır. Bu programlarda ülkelere mali ve beşerî destek sağlanmaktadır. AB müktesebatının yürütülebilmesi için uyumlulaştırılması lüzumlu yönetsel yapı ve sonuç olarak bütün bu konulara ilişkin kısa ve orta vadeli öncelikli yapılacak işler takvimi belirlenmektedir. Türkiye, Ulusal Programları kabul ederken,

onların kaynaklarının verilme amacına uygun şekilde kullanılacağını da taahhüt etmektedir (Bük, 2015: 66).

2.3.3. Kanuni Düzenlemeler

Türkiye’de kişisel verilerin korunmasına ilişkin düzenlemeler ; konu hakkındaki özel kanun olan 6698 sayılı Kişisel Verileri Koruma Kanunu başta olmak üzere 5237 sayılı Türk Ceza Kanunu,4721 sayılı Türk Medeni Kanunu,4857 sayılı İş kanunu,5490 sayılı Nüfus Hizmetleri Kanunu,213 sayılı Vergi Usul Kanunu,2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu,,5809 sayılı Elektronik Haberleşme Kanunu,5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,6098 sayılı Türk Borçlar Kanunu, Ticaret Kanunu , Ceza Muhakemesi Kanunu kanunlarındaki ilgili maddeler incelenerek ele alınabilir.

2.3.3.1.Genel Olarak

Türkiye, uluslararası ilişkileri ve elbette çağın gerekliliği olarak kişisel verilerin korunmasına ilişkin yasal düzenlemeleri yapmak konusunu birçok kez gündemine getirmiş ancak bu 2016 yılına dek gerçekleştirilememiştir. Bir kanun ile kişisel verilerin güvence altına alınmamış olması, Avrupa’ya ve diğer gelişmiş ülkelere göre Türkiye’nin çok geride kalmasına neden olmuştur. Kanun şimdiye dek ulaşılabildiği olan ve kişileri çeşitli sorunlar ile karşı karşıya bırakan bilgi paylaşımını kısıtlamaya yönelik düzenlemeler içermektedir. Ancak kanunun tasarımı sürecinden itibaren çok fazla eleştiri aldığı da unutulmamalıdır. Bu bölümde, Türkiye Cumhuriyeti mevzuatında kişisel verilerin güvenliğine ilişkin olarak hazırlanmış ve yeniden düzenlenmiş olan kanun ve yönetmeliklerin güncel halleri paylaşılmaktadır.

2.3.2.2. Kişisel Verilerin Korunması Kanun Tasarısı

Kişisel verileri korumayla ilgili gündem ilk defa 1981 yılında Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme ile oluşmuştur (Ayözger, 2016: 109). Kişisel verilerin Türkiye içinde korunmasına yönelik ilk kanun tasarısı hazırlama komisyonu 1995

yılında kurulmuştur. Fakat bu komisyon çalışmalarını tamamlayamamış, bunun üzerine 18.09.2000 tarihinde yeni bir komisyon kurulmuş ve bu komisyon 2003 yılında bir yasa tasarısı hazırlamıştır. 1/576 Esas No.lu Kişisel Verilerin Korunması Kanunu Tasarısı ancak beş yıl sonra, 2008 tarihinde Kanunlar Başkanlığına gelmiştir. 2 Mayıs'ta TBMM Adalet Komisyonuna gelen tasarı, 22 Mayıs'ta ise AB Uyum Komisyonu'ndan çıkmıştır. 2010 yılında yapılan Anayasa değişikliği ve Avrupa Birliği Uyum Komisyonu'nun raporu sonrasında tasarı geçersiz hale gelmiş ve kişisel verilere yönelik bir kanun hazırlanamamıştır (Uncular, 2012: 32).

Kişisel Verilerin Korunması Kanun Tasarısı 2007 ve 2012 yıllarında yenilenmiştir Başbakanlığa gönderilen bu tasarılar, 2014 tarihinde son halini almış ve Türkiye Büyük Millet Meclisi'ne sunulmuştur. 2015 tarihinde AB Uyum Komisyonu'ndan geçmiştir (Ayözger, 2016: 110). Ancak bu tasarının kanunlaştırılması sürecinde Meclis'te tartışmalar olmuş, özellikle iktidar partisinin dışındaki partilerin tamamı tasarıyı eleştirmiştir.

Burada kanun tasarısına ilişkin çeşitli tartışmalardan bahsetmek gerekmektedir. Tasarıya ilişkin ilk itiraz kişisel verilerin işlenmesi hususunda kanunun kişinin iznini gerektirmesi ancak bu ibarelerin Türk Hukuk Sistemi içinde gerçekten yer bulamaması konusunda olmuştur. Örneğin Türk Hukuk sisteminde kişiye ilişkin bilgilerin toplanması ve işlenmesi konusunda kanunlarda açıkça öngörülmesi halinde kişinin rızasının alınması koşulu aranmamaktadır. Ayrıca söz konusu kişi rızasını açıklama konusunda fiili bir imkânsızlık yaşıyorsa, onun rızasını almak zorunda kalınmayacaktır. Yine hukuki sisteme bakıldığında bir kişinin bilgilerinin saklanması bir başka kişinin hayatı veya beden bütünlüğünün korunması için zorunlu olması halinde rızadan bahsedilemeyeceği görülecektir. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması ve son olarak bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması gibi hallerde kişisel verilere ilişkin izin ve rıza zorunluluğu ortadan kalkmaktadır. Kanun tasarısında da bu haller rıza almak konusunda istisnai haller olarak nitelendirilmektedir. Ancak bu hallerin tamamı bir şekilde

yaratılabilecektir. Örneğin bireyin kendi sosyal medya hesabında vermiş olduğu bir bilgi bu bilgiyi alenileştirmiş olduğunu gösterebilecektir. Ancak bu tür bir durumda kişinin bu bilgiyi kendisinin yayınlayıp yayınlamamış olup olmadığı tespit edilemeyecektir. Bunun yanı sıra bir suç ile ilişkili şüphe söz konusu olduğunda bu hal devlete kişisel bilgileri işleme hakkını verebilecektir. Ancak bu, kişinin gerçekten suçlu olduğunu kanıtlamamaktadır. O nedenle kişisel bilgilerde bireyin rızası konusu büyük tartışmaları beraberinde getirmektedir (Çayır, 2013: 5).

Tasariya ilişkin bir diğere eleştirisi de tasarının kişiyi özel sektöre karşı korurken devlete karşı korumadığı ve kişi haklarına eşit düzeyde yaklaşmadığı yönündedir. Tasariya devlet merkezli düşünce hâkim olması ve bireyi özel sektöre karşı korumak için ciddi kısıtlamalar getirilirken kamuya karşı aynı denge söz konusu olmaması eleştirilerin başında gelirken kamuya getirilen geniş istisnaların orantılılık ilkesine göre yeniden düzenlenmesi talep edilmiştir. Tasarıda devletçi bir otorite hâkim” olması en çok eleştirilen noktadır. Bu tasarının birey merkezci değil de devlet merkezci bir yapıda olmasının da kabul edilemez nitelikte olduğu eleştirisi tasarı tartışmalarına damga vurmuştur, devletin bağımsız olmayan herhangi bir yapısının kişisel verileri yayınlatabilmek için çok basit şekilde bahane bulabileceğinin de altını çizilmiştir (Kıraç, 2015).

Kanun tasarısının devletin eline fişleme ve fişlemeye yönelik uzun süre hapiste tutma yetkileri vereceğini ve bu tasarının hem Anayasa’ya hem de AB’nin kurallarına aykırı olduğu görüşünde olan muhalefet grupları 19.01.2015 tarihinde yayınlanmış olan 41/1009 esas No.’lu “Kişisel Verilerin Korunması Kanunu Tasarısı’na şerh koymuştur. T.C. Anayasasının 20.maddesinin 3.fıkrası “(Ek fıkra: 12/9/2010-5982/2 Md.) 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.” Demektedir ancak tasarı buna aykırıdır şeklinde koyulan şerh kayıtlara geçmiştir.

Devlet çalışanı olan ve sır saklama yükümlülüğü bulunan kişilerin kişisel verilere ulaşma konusunda bu kanun ile sınırsız yetkisinin olacağına kanun tasarısının

yorumundan çıkarılabileceğini ,bunun yanı sıra devlete özel bir imtiyaz tanınmasının AB mevzuatına da tamamen aykırı olduğunu belirten muhalefet vekilleri “Tasarı Anayasa ve AB mevzuatına aykırı fiili duruma yasal güvence getiriyor”, “Taslak uyum zorunluluğu içinde olduğu Avrupa Birliği sözleşmeleri ve yönergeleriyle, devletin istihbarat ve zor aygıtlarının dayatmaları arasında bir orta yol seçimine işaret etmektedir” şeklinde meclis kayıtlarına tasarı hakkında görüşlerini not düşürmüştür.

Kişilerin kişisel verilerinin kullanılması konusunda rahatsızlık duymaları halinde şikâyette bulunabilecekleri merciinin hükümet uzantılı bir kuruluş olacağı ve bu durumun eşitliğe de aykırı olduğu, bu yöntemler ile kişisel sırların “devletleştirileceği” eleştirisi de yine tasarıya gelen ve tasarının devletçiliği hususundaki dikkat çekici bir noktadır.

Tasarıyı eleştiren ve şerh koyan vekiller özellikle 2010 yılında referandum ile kabul edilen Anayasa'nın 20.maddesinin kişisel verileri güvence altına almak üzere hazırlandığını ancak konuyla ilişkili çerçeveyi belirleyecek olan kanunun da gerekli olduğunu vurgulamıştır ve insan hakları ile uyumlu bir yasa hazırlanması gerektiğinin, kişisel verilere ilişkin var olan tüm maddelerin açık ve yoruma kapalı biçimde düzenlenmesi gerektiğinin, kişinin kendisine ait verilerin neden istendiği ve bununla ne yapılacağına dair her zaman şeffaf şekilde bilgilendirilmesi gerektiğinin altını çizilmiş ve taraflarca zapta geçirilmiştir. (www.tbmm.gov.tr/tutanak).

TBMM'de tasarıya ilişkin görüşmeler sırasında sözlerine kişisel verilerin korunmasının önemi muhalefet ve iktidar tarafından ortak olarak vurgulanan bir noktadır fakat muhalefet genel olarak milletin menfaatine olan her şeye destek vereceğini ancak bu tasarının kişileri korumayacağı görüşünde birleşmiştir. ([Www.tbmm.gov.tr/tutanak](http://www.tbmm.gov.tr/tutanak))

Kanun tasarının bazı maddelerinin çok kritik olduğuna ve bunların bir karar alınmadan önce yeniden incelenmesi gerektiğine değinen muhalefet milletvekilleri kişisel verilere ilişkin kuralları denetleyecek olan Kurul'un kesinlikle tarafsız ve şeffaf olması gerektiğine dikkat çekmiş ve bunun gerekliliğinin de Avrupa Konseyinin direktif kararlarında net biçimde yazdığını belirtmiştir. Bu tasarının kanunlaşması halinde kurulun bağımsız olmayacağı görüşünü savunulmuş ve bunun nedeni olarak

kurulun 7 üyeden oluşacağını ve 4'ünün Bakanlar Kurulu, 3'ünün ise cumhurbaşkanı tarafından atanacağını gösterilmiştir. Kurulun başkan, başkan yardımcısı ve üyeleri hakkındaki soruşturmaya izin yetkisinin de Başbakan'a bırakılmış olmasının da tarafsızlık ve bağımsızlığa aykırı olduğunu belirten muhalefet; ayrıca bu tasarinın, "özünde dünyayı bir anlamda şirketlerin yöneteceği günlere yönelik olarak yapılmış bir hazırlık" olduğunu belirterek tasarımı sözcüleri aracılığıyla eleştirmiştir (www.tbmm.gov.tr/tutanak).

Tasarının ikinci bölümü ile ilgili tartışmalar da mecliste şu şekilde kayda geçmiştir. Muhalefet ve tasarı karşıtları bu tasarinın kanunlaşması söz konusu olması halinde kişisel verilerin ortada kolaylıkla dolaşabileceğini belirtmiş ve bunun AB'nin değil çağın gerekliliği olarak ciddiye alınması gerektiğini ancak bu hali ile yasalaşması halinde korumadan uzak bir düzenleme olacağını belirtmiştir.

Tasarı tartışmalarında muhalefeti yanlı davranmakla suçlayıp, her tasarıya objektif bakılması gerektiğini belirten iktidar çevresi ve tasarıya muhalefet etmeyen vekiller; Türkiye'nin kişisel verilerin korunmasına ilişkin olarak henüz bir kanunun olmamasının onun uluslararası faaliyetlerde zorluklar yaşamasına neden olduğunu belirtmişler ve artık bir kanun oluşturulmasının bir zorunluluk olduğuna katıldıklarını ortak bir şekilde ifade etmişlerdir. Tasarinın "henüz Adalet Komisyonuna gelmeden, içeriği tam olarak bilinmeden, Komisyonda, Genel Kurulda görüşülmeden "fişleme tasarısı" olarak anılması, bu konuda haberler çıkması esasında bir ön yargıdır" diyerek diğerlerinden farklı bir yaklaşım sergileyen muhalefet vekilleri ve tasarinın uluslararası standartta olduğunu belirten iktidar partisi sözcüleri açıklamaların netleştirilmesi halinde bu güvensizliğin giderileceğini söylemiştir. Muhalefet tasarının esası hakkında hassas veriler gibi çok önemli kavramların yeterince net olmadığı şeklinde ikinci bir şerh daha düşerken; ana muhalefet vekilleri en önemli endişelerinin tasarıda adı geçen kurulun bağımsızlığı olduğunu da sözlerine eklemiştir.

Tasarı hakkında doktrinden bir bakış açısı olarak Şimşek; "*Kişisel Verilerin Korunması Kanun Tasarısı genel olarak bireyin kişisel verilerini korunması hakkının yasal temele bağlanması ve bu bağlamda anayasadaki temel hak ve özgürlüklerle ilişki kurması ve ilgili uluslararası belgelere referans alması bakımından olumludur. Ancak tasarının yasalaşma sürecinde bireyin kişisel verilerinin korunması hakkı bakımından*

getirilen geniş istisnai düzenlemelerin gözden geçirilmesi ve bireyin kişisel verileri üzerindeki haklarını genişletici ve denetim organlarının bağımsızlığını ve işlevselliğini güçlendirici şekilde tamamlanması gerekmektedir. Bu çerçevede bir yasal düzenleme yapılırken, düzenlemenin temel hareket noktası bireyin kişisel verilerinin korunması hakkının güvence altına alınması, kişisel verilerin işlenmesi sırasında temel ilkelerin konulması suretiyle özellikle bireyin özel alanından hukuka aykırı olarak veri elde edilip işlenmesinin önlenmesi ve kamusal organların kişisel veri gereksinimlerinin karşılanmasının hukuksal temellerinin oluşturulması olmalıdır.” diyerek tasarı hakkındaki görüşlerini ifade etmiştir

Bu tartışmalardan ve belirtilen görüşlerden anlaşıldığı üzere, devletin kişisel verilerin işlenmesine ilişkin geniş yetkileri, bu mekanizmayı destekleyen kurulun yönetici ve çalışanları ile kişisel verileri işleme izni olan kamu görevlilerini hükümetin seçecek olması ve devletin yetkileri ile özel sektörün yetkileri arasında uçurumun olması, yasa tasarısının en çok konuşulan konuları olmuştur. İktidar partisi dışında tüm partiler, yasa tasarısının hem Türkiye Cumhuriyeti Anayasası ve diğer mevzuatına hem insan haklarına hem de Avrupa Birliği Mevzuatına aykırı olduğu görüşünde birleşmişlerdir. Ancak tasarı 2016 tarihinde yasalaşmıştır. Bu tartışmalar ışığında, CHP adına partinin Ankara Milletvekili Murat Emir, kanun haline getirilen tasarının iptal edilmesi için Anayasa Mahkemesi'ne başvuru yapmıştır ancak Anayasa Mahkemesi tarafından 28.09.2017 tarihli ve 2017/143 karar numaralı (www.Sinerjihukuk.com) kararda başvuru reddedilmiştir. (T24, 2916).

Kişisel Verilerin Korunması Kanun Tasarısı; 108 sayılı Avrupa Konseyi Sözleşmesi ile 95/46 sayılı AB Direktifinin bir gerekliliği olarak hazırlanmış ve hükümetin belirttiğine göre AB mevzuatı rehber olarak alınmıştır. Amaç AB iç hukuku ile Türkiye Cumhuriyeti mevzuatını uyumlaştırmak olmuştur. Özellikle AB ile Türkiye arasındaki bilgi akışı esnasında sorunlar yaşanması, tasarının oluşturulmasını zorunlu hale getirmektedir. Şimdiye dek hazırlanmış olan tasarıların her biri 108 sayılı Avrupa Konseyi Sözleşmesi ile 95/46 sayılı AB Direktifinden ve OECD'nin 23.09.1980 tarihli “Kişisel Alanın ve Sınıraşan Kişisel Bilgi Trafikinin Korunmasına İlişkin Rehber İlkeler” ışığında hazırlanmıştır (Bük, 2015: 77).

Kişisel Verilerin Korunmasına ilişkin hazırlanan kanun tasarısı incelendiğinde, kişisel verilerin nasıl işleneceğine dair hukuk kurallarını belirlediği görülecektir. Bu tasarıya göre, kişisel verilerin toplanması için bir amaç olması gerekmektedir ve kişisel veriler de bu amaca uygun şekilde toplanmalıdır. Tasarı, kişiye kendisine ilişkin veriler hakkında bilgi edinme hakkını da vermektedir. Tasarı, kişisel verilerin toplanma amacının değişmesi halinde kişiye onları sildirme hakkını da vermektedir. Bu sayede üçüncü kişilerin kişisel verileri ele geçirmesi önlenmiş olacaktır. Tasarı kanunlaşarak kişisel verilerin korunması hakkının özel kanunu haline gelmiş ve Türk mevzuatındaki kişisel verileri koruma seviyesini uluslararası alandaki düzenlemelerle eşdeğer düzeye erdirmiştir.

2.3.3.3. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Bir önceki başlıkta da görüldüğü gibi Kişisel Verilerin Korunması Kanunu, Avrupa Konseyi anlaşmasına uygun olarak yapılmaya çalışılmış, hükümet kişileri korumayı hedeflediğini iddia etmiş fakat buna karşın tasarı çok fazla eleştiri almıştır. Tasarı, kanunlaşmasını takiben 7 Nisan 2016 tarihli Resmî Gazetede yayınlanarak yürürlüğe girmiştir. Kanun adından da anlaşıldığı üzere kişilerin hak ve özgürlüklerini ve özel hayatlarının gizliliğini koruma altına almak amacına hizmet etmektedir. Kanun ayrıca kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uymaları gereken usul ve esasları da çerçeve içine almaktadır (6698 Sayılı Kanun, 1. Md.).

Kanun kişisel verileri işlenen kişilerin ve bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanmaktadır (6698 Sayılı Kanun, 2. Md.). Kanunun 3. Md., kanunda geçen kavramları tanımlamakta, 4. Md. ise kişisel verilerin işlenmesi ile ilgili genel hükümleri açıklamaktadır. Bu maddeye göre kişisel verilerin işlenmesi hukuka uygun olmak zorundadır. Verilerin tamamı doğru ve güncel olmalı, amaçlar önceden belirlenmiş ve açık olmalıdır. Elde edilen veriler amaçlara hizmet edilecek biçimde olmalı, fazlası istenmemelidir. Ayrıca amaçların tamamı mevzuata uygun şekilde olmalı ve amaçların bir süresi belirlenmiş olmalıdır (6698 Sayılı Kanun, 4. Md.). Kişisel veriler kişinin rızası olmadan hiçbir

şekilde işlenememektedir. İşleme yapacak olan gerçek ya da tüzel kişilerin kişisel bilgi sahibinin açık rızasını almaları zorunludur. Ancak şayet kanunlarla açıkça öngörülüyorsa, fiziki imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması halinde, bir sözleşmenin oluşturulması için kişisel verilerin zorunluluğu söz konusuysa, veri sorumlusu hukuki olarak görevini yerine getirebilmek için kişisel verilere ihtiyaç duyuyorsa, kişinin kendi verilerini öncesinde alenileştirmesi halinde açık rıza şartı mevcut değildir. Ayrıca ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması halinde de rıza alma şartı yoktur (6698 Sayılı Kanun, 5. Md.).

İşte en fazla tartışmaya konu olan madde 5 Md.'dir. Sözleşmenin gerçekleşmesi, öncesinde kişinin kendi bilgilerini alenileştirmiş olması gibi maddeler kanun tasarı halindeyken en fazla tartışılan maddeler olmuştur. Kişisel verileri elde etmek için sözleşmenin bir zorunluluğuymuş gibi göstermek, veri sorumlusunun bunu hukuki bir zorunluluk gibi göstermesi, kişinin kendisine ait verileri daha önceden bir süreliğine ya da halen alenileştirmiş olması ve bunu bilinçli ya da bilinçsiz şekilde yapması gibi koşulları duruma göre kolaylıkla değişebilecek ya da yanlış yoruma açık olabilecektir.

Kanunun 6. Md'si, özel nitelikli verilerin hangi şartlarda işlenebileceği açıklanmaktadır. Maddede öncelikle özel nitelikli kişisel verilerin ne olduğu açıklığa kavuşturulmuştur. Bu maddeye göre ırk, etnik köken, siyasi ve/veya felsefi düşünceler, dernek, sendika gibi kurumlara üyelik, cinsel hayat, mahkûmiyet gibi bilgiler özel nitelikli kişisel verilerdir. Madde özel nitelikli kişisel verilerin de kişinin açık rızası olmaması halinde işlenmesinin mümkün olmadığını ancak, sağlık ve cinsel yaşama dair bilgilerin kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceğini belirtmektedir. Ancak bu verilerin işlenmesi esnasında Kurul tarafından belirlenmiş olan güvenlik önlemlerine uyulması şartı aranmaktadır (6698 Sayılı Kanun, 6. Md.).

7. Md., kişisel verilerin silinmesi, yok edilmesi ya da anonim hale getirilmesi halinde ne tür kuralların geçerli olduğunu açık hale getirmektedir. Bu madde,

bilgilerin işlenmesi için gereken şartların ve amaçların ortadan kalkması halinde bu amaçlar doğrultusunda toplanan verilerin silinmesi, yok edilmesi ya da anonim hale getirilmesi gerekmektedir. Bu durum kişisel verilerin sahibinin talebi doğrultusunda da gerçekleşmelidir. Madde silme, yok etme ya da anonim hale getirme konusunda diğer kanunlar dışında kalan bölümler için yönetmeliklere uyulması gerektiğini belirtmektedir (6698 Sayılı Kanun, 7. Md.). Kişisel verilerin aktarılması gerekli olduğunda ise kanunun 8. Md. uyulması gerekmektedir. Bu madde, kişisel verilerin aktarılması için de kişinin açık rızası olması gerektiğini belirtmektedir. Ancak madde, beşinci maddede de belirtilmiş olan haller söz konusu olduğunda kişinin rızasının alınması şartının olmadığını, diğer kanunlarda ilişkili maddelerin de göz ardı edilemeyeceğini söylemektedir (6698 Sayılı Kanun, 8. Md.).

6. ve 8. Md.; 5. Md. ile benzerlik göstermektedir. Kişilerin hassas verilerinin açıklanması ya da paylaşılması konusunda, işlem yapan birimlerin yetkililerinin suiistimaline açık haller söz konusu olabilecektir ve aslında mecliste ve alan yazınında tartışmalara konu olan en önemli etken budur.

9. Md. verilerin aktarılacağı ülkede hangi şartların olması gerektiğini belirlemek adına önemlidir. Buna göre verilerin aktarılacağı ülkelerin yeterli veri koruma sisteminin olması gereklidir. Şayet verilerin yabancı ülkelere aktarılması gerekiyorsa ve bu ülkenin kanunları yeterli korumayı mümkün kılmıyorsa, bu durumda ilgili ülkenin yetkili veri koruma çalışanlarının Türkiye'deki yetkililer ile verilerin korunmasını taahhüt eden yazılı anlaşma yapması gerekmektedir. Ayrıca Kurul izni olmalıdır. Kurul, yeterli korumaya sahip olan ülkeleri belirlemekte ve bunu ilan etmektedirler. Türkiye'nin taraf olduğu sözleşmeler, kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durum, kişisel verilerin aktarılma amacı ve süresi, aktarım yapılacak olan ülkenin mevzuatı, önlemleri ve taahhütleri ülkenin veri aktarmaya uygun olup olmadığının belirlenmesi konusunda en önemli etkenlerdir. Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir. Koruma söz konusu olduğunda, kişinin rızası aranmamaktadır (6698 Sayılı Kanun, 9. Md.).

Kanunun 10. Md., veri sorumlusunun bilgilendirme/aydınlatma gerekliliği konusu hakkındadır. Maddeye göre kişisel verileri işlenecek olan kişiye veri sorumlusu ya da onu temsil eden kişinin kendisini tanıtmayı, veri işleme amacını açıklaması, verilerin aktarılması gerektiğinde bunun hangi şartlarda ve neden yapılabileceği, verilerin toplanma sebebini ve bunun hukuki sınırlarını ve kişisel verilerin sahibinin sahip olduğu hakları açıklama zorunluluğu mevcuttur (6698 Sayılı Kanun, 10. Md.).

11. Md. ise veri sahibinin haklarının neler olduğunu açıklamaktadır. Bu maddeye göre kişisel verilerin sahibinin kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme hakkı mevcuttur. Ayrıca veri sahibi bunların silinmesini talep edebilecektir ve bu durumda 7. Md. hükümleri devreye girecektir. İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme de kişisel veri sahiplerinin hakları arasında yer almaktadır (6698 Sayılı Kanun, 11. Md.)

Kanunun 12. Md., veri güvenliğiyle ilgilidir. Bu madde veri sorumlusunun görev ve yükümlülüklerini açıklar niteliktedir. Maddeye göre veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak durumundadır. Bunu gereken tüm idari ve teknik önlemleri alarak yapmalıdır. Ayrıca veri sorumlusu kendisi adına bir başkasının verileri işlenmesi halinde de sorumlu tutulacaktır. Kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak veri sorumlusunun zorunlulukları arasındadır. Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamayacak ve işleme amacı dışında kullanamayacaklardır. Görevden ayrılışları bile durum değişmeyecektir. İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri

sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirmekle yükümlüdür (6698 Sayılı Kanun, 12. Md.).

13. Md. bakıldığında kanunun uygulanmasıyla ilgili talep ve şikayetlerin nasıl gerçekleştirildiğine açıklık getirdiği görülecektir. Kanun, talep ve şikayetlerin nasıl yapılacağına Kurul'un karar vereceğini belirtirken talepler karşısında cevapların en geç otuz iş günü içinde verilmesi gerektiğinin ve ücretsiz olması gerektiğinin de altını çizmektedir. Talep ve şikâyet işleminin bir maliyetinin olması halinde Kurul bir tarife belirleyecektir ve buna uyulacaktır. Şikayetler ve talepler kişiler tarafından veri sorumlusuna yapılacaktır. Veri sorumlusunun talebi kabul etmemesi halinde bunun gerekçesini kişiye açıklaması da şarttır (6698 Sayılı Kanun, 13. Md.).

14. ve 15. Md. de en fazla tartışma yaşanan maddelerden biridir. Bu madde Kurul'a nasıl şikâyette bulunulacağını ve bu hususta neler olabileceğini açıklamaktadır. Kişi, veri sorumlusuna başvurduktan sonra probleminin çözülememesi halinde kişisel verileri ile ilgili olarak Kurul'a başvurabilecektir. İlgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve herhâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilecektir. Kişinin veri sorumlusuna yapacağı başvuru yolları tüketilmeden Kurul'a başvurması olanaksızdır. Bu madde ayrıca hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkının da saklı olacağını belirtmektedir (6698 Sayılı Kanun, 14. Md.).

15. Md. göre Kurul şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapacaktır. Ancak Kurul'a şikâyet esnasında, konuyla ilişkili mevzuattaki dilekçe yazma kurallarına uyulması zorunludur. Aksi takdirde Kurul bunun incelemesini yapmayacaktır. Devlet sırrı niteliğindeki bilgi ve belgeler hariç; veri sorumlusu, Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır. Kurul şikâyeti incelemekte ve ilgililerin hepsine bir cevap vermektedir. Cevabın 60 gün içinde verilmemesi, şikâyetin reddedilmesi anlamına gelmektedir. Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ etmekte ve karara uyulması için otuz günlük süre vermektedir. Şayet ihlalin yaygın

olma durumu söz konusu ise Kurul, bu konuda ilke kararı almakta ve bunu yayınlamaktadır. İlke kararının alınması esnasında ihtiyaç halinde kurul ilgili kurum ve kuruluşlar ile görüş alışverişi yapabilecektir. Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verebilecektir (6698 Sayılı Kanun, 15. Md.).

Kanunun 16. Md. veri sorumlularının siciline ilişkin hükümler olduğu görülmektedir. Veri sorumlularının sicilleri Kurul tarafından kamuya açık şekilde tutulmaktadır ve kişisel veri işleyen gerçek ya da tüzel kişilerin işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadırlar. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilecektir (6698 Sayılı Kanun, 16. Md.). Bu nokta da tartışmalara neden olmaktadır. Veri işleme yetkisi bulunan hangi kişilerin sicillerinin kayıt altına alınacağı konusunda yetkilinin Kurul olması ve bu kuralların değiştirilerek bir standardın oluşturulmama endişesi mecliste kanun tasarısı görüşmeleri esnasında ve sonrasında alan yazınında tartışmalara yol açmıştır. Bu madde, veri işleme sorumlularının hangi niteliklere göre seçileceği konusunda bir eşitliğin var olmasının önüne geçebilecektir.

Kurul, veri sorumlularının kayıtları esnasında onların kimlik ve adres bilgileri, veri işleme amaçlarını, veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamaları, bu verilerin aktarılması söz konusu ise nereye olacağı, yabancı ülkeye aktarım söz konusu olursa bunun hangisi olduğu gibi bilgileri istemektedir. Ayrıca Kurul veri güvenliği için alınan önlemleri de incelemektedir. (6698 Sayılı Kanun, 16. Md.).

Kanuna göre veri işlemeye ilişkin bir suç söz konusu olduğunda Türk Ceza Kanunu'nun 135 ile 140.Md. arasındaki hükümler uygulanacaktır. Ayrıca, 6698 sayılı Kanunun 7. Md. hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138. Md. göre cezai yaptırımlar ile karşılaşacaklardır (6698 Sayılı Kanun, 17. Md.).

Kanunun 10. Md. Deki kişisel bilgiler ile ilgili aydınlatma/ bilgi verme hükümleri yerine getirmeyenler 5.000 Türk Lirası ile 100.000 Türk Lirası aralığında idari para cezasına mahkûm edileceklerdir. Şayet 12. Md. De yer alan veri güvenliğine ilişkin hükümler yerine getirilmediyse, 15.000 Türk lirasından 1.000.000 Türk lirasına kadar ceza kesilecektir. 15.Md. de yer alan Kurul kararlarına uyulmasına ilişkin hükümlerin yerine getirilmemesi söz konusu olduğunda, 25.000 Türk lirasından 1.000.000 Türk lirasına; 16.Md. yer alan hükümlerin yerine getirilmemesi halinde ise 20.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verilecektir. Bu cezalar veri sorumlularına verilecektir. Bu maddelerde sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılacaktır (6698 Sayılı Kanun, 18. Md.).

19. Md. de tartışmalara neden olmuştur. Bu madde Kişisel Verileri Koruma Kurumu'nun Başbakanlığa bağlı olduğunu, merkezinin Ankara'da olduğunu ve Kurum, Kurul ve Başkanlıktan oluştuğunu belirtmektedir. Yine aynı maddeye göre, Kurum'un karar organı Kurul'dur (6698 Sayılı Kanun, 19. Md.). Mecliste, Kurum'un başbakanlık bünyesinde olmaması gerektiği aksi takdirde bunun "yanlı" karar vermeye sebep olabileceği konusunda tartışmalar yapılmıştır.

20. Md. Kişisel Verileri Koruma Kurumu'nun görevlerini açıklamaktadır. Buna göre Kurum'un görevleri;

a) Görev alanı itibarıyla, uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak.

b) İhtiyaç duyulması hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak.

c) Kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda uluslararası kuruluşlarla iş birliği yapmak, toplantılara katılmak.

ç) Yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna ve Başbakanlığa sunmak.

d) Kanunlarla verilen diğer görevleri yerine getirmek şeklindedir (6698 Sayılı Kanun, 20. Md.).

Bir sonraki madde Kişisel Verileri Koruma Kurulu'nun yapması gereken uygulamaları açıklamaktadır. Kurul, mevzuatla kendisine verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirmelidir. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunma hakkı mevcut değildir (6698 Sayılı Kanun, 21 Md.). Ayrıca Kurul'un 9 üyeden oluşacağı da bu maddede açıklanmıştır. Bunların beş üyesi Türkiye Büyük Millet Meclisi, iki üyesi Cumhurbaşkanı, iki üyesi Bakanlar Kurulu tarafından seçilecektir denmektedir. Meclis çoğunluğu ve Cumhurbaşkanı'nın aynı görüşte olması halinde Kurul üyelerinin taraflı olabileceği ve bu durumun tarafsızlığı bozabileceği riskine karşı da mecliste tartışmalar yapılmıştır. Kurulun görev ve yetkileri şu şekildedir:

a) Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak.

b) Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak.

c) Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak.

ç) Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek.

d) Veri Sorumluları Sicilinin tutulmasını sağlamak.

e) Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak.

f) Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak.

g) Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak.

ğ) Bu Kanunda öngörülen idari yaptırımlara karar vermek.

h) Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat tasarıları hakkında görüş bildirmek. (6698 sayılı Kanun,22. Md.)

Kurul'un hangi günlerde toplanacağı ve toplantı gündemlerinde hangi konuların yer alacağı Kurul Başkanı tarafından belirlenmektedir. Bir toplantının gerçekleşebilmesi için Başkan'la birlikte 6 üyenin olması zorunludur ve kararlar salt çoğunluğa göre alınmalıdır. Kurul üyelerinin çekimser kalacak şekilde oy kullanma hakları mevcut değildir. Kurul üyeleri; kendilerini, üçüncü dereceye kadar kan ve ikinci dereceye kadar kayın hısımlarını, evlatlıklarını ve aralarındaki evlilik bağı kalkmış olsa bile eşlerini ilgilendiren konularla ilgili toplantı ve oylamaya katılamayacaklardır. Üyelerin çalışmaları esnasında öğrendikleri bilgileri başkalarına açıklamaları yasaktır. Toplantılarda yapılan görüşmeler hakkında tutanak hazırlanmalıdır. Kararların oy gerekçeleri tutanakta yazılmalıdır. Kararın kamuoyuna duyurulması da Kurul'un kararıdır. Aksi kararlaştırılmadıkça, Kurul toplantılarındaki görüşmeler gizlidir. (6698 Sayılı Kanun, 23. Md.)

2.3.3.4. Diğer Kanunlarda Kişisel Verilerin Korunması Hakkı

Türkiye Cumhuriyeti'nde doğrudan ya da dolaylı olarak kişisel verilerin korunmasına ilişkin kuralların yer aldığı çeşitli kanunlar mevcuttur. Bunları şu şekilde sıralamak ve özetlemek mümkündür:

i. 5237 Sayılı Türk Ceza Kanunu

Türk Ceza Kanunu'nun 134 vd. maddelerinde kişisel verilerin korunması ile özel hayatın gizliliğine ilişkin hükümler bulunmaktadır. 134 Md., bireylerin özel hayatının gizliliğini ihlal edilmesi halinde bunun 1 ile 3 yıl arasında hapis cezası ile sonuçlanacak bir suç olduğuna işaret etmektedir. Aynı madde, gizlilik ihlalinin kişinin bilgisi dışında ses ve/ya görüntüler eşliğinde yapılması durumunda cezanın arttırılacağına da altını çizmektedir. Şayet bu ses ve görüntüler ifşa edilirse, hapis cezasının beş yıla kadar çıkarılabileceği de yine burada açıkça belirtilmektedir (5237 sayılı Kanun 134.Md.).

TCK 135.Md., kişisel verilerin hukuka aykırı biçimde kayıt altına alınması durumunda alınacak cezalara açıklık getirmektedir. Madde, kişisel verilerin hukuki kuralla aykırı biçimde kaydeden kişilerin 1-3 yıl arasında hapis cezası ile karşılaşacağını belirtmektedir. Aynı madde, ırk, sendikal kayıt, etnik köken, sağlık bilgisi gibi hassas veri sınıfında olan bilgilerin kaydedilmesi halinde de aynı şartlar altında ceza verileceğini açıkça ifade etmektedir (5237 sayılı Kanun 135.Md).

TCK 136.Md. de yine kişisel verilere ilişkin bir maddedir. Bu madde, kişisel verilerin hukuki kurallar dışında paylaşılması halinde paylaşan sorumluya iki yıldan dört yıla kadar hapis cezası verileceğini; bu sorumlunun kamu görevlisi olması halinde ise

“a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, işlenmesi halinde, verilecek ceza yarı oranında” arttırılacağını yazmaktadır (5237 sayılı Kanun 136.Md).

TCK 138. Md. de yine konu ile ilgilidir. Bu maddede hukuki uygunluk çerçevesinde toplansa ve saklansa dahi, kişisel verilerin kullanılmasına izin verilen süre sonrasında silmeyen kişilere verilecek cezaları açıklamaktadır. Bu maddeye göre bu suçu işleyenler bir yıldan iki yıla kadar hapis cezası ile cezalandırılacaktır (5237 sayılı Kanun 138.Md).

Fakat kanun tüm bu cezaların verilmesini 139. Md.de şikâyete bağlamaktadır. Bu maddeden kişi, kendisine ait verilerin hukuka aykırı biçimde toplandığı, saklandığı ya da yok edilmediğini düşünerek şikâyette bulunmadığı takdirde, sorumluların cezalandırılmayacağını anlamak mümkündür.

ii. 4721 Sayılı Türk Medeni Kanun'u

Kişisel verilerin güvenliğine ilişkin yapılan yasal düzenlemelerin temeli aslında kişilik hakkının özelleştirilmesi ile oluşturulmuştur (Aksoy, 2010: 80). 4721 sayılı Türk Medeni Kanunu'nda kişilik haklarını ve kişiliği koruyan haklar çerçevesinde kişisel verilerin güvenliği de ele alınmaktadır. Kanunun 24. Md. şu şekildedir:

“Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır” (4721 Sayılı Kanun, 24. Md).

Buradan hareketle, kişinin kendisi ile ilgili yanlış ya da hukuka aykırı şekilde kişisel bilgilerinin kaydedildiğini ya da kullanıldığını fark etmesi halinde yasal işlem başlatabileceğini söylemek yanlış olmayacaktır. Medeni Kanun, kişisel verilerin işlenmesini kişilik hakkı kapsamında ele almaktadır (Çokmutlu, 2014: 126).

Yine kanunun 25. Md. bakıldığında, bireyin kişilik haklarına hukuka aykırı bir şekilde saldırı yapılması halinde ne tür davalar açabileceğini açıkladığı görülecektir: “Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir. Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir. Davacının, maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır. Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça

devredilemez; miras bırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez. Davacı, kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yeri mahkemesinde dava açabilir” (4721 Sayılı Kanun, 25. Md).

iii. 4857 Sayılı İş Kanunu

Bilindiği üzere işe alım esnasında insanlar kişisel bilgilerini paylaşmak durumunda kalmaktadırlar. İş Kanunu, konuya ilişkin kapsamlı bir düzenlemeye sahip olmasa da kişisel verilerin korunması konusunda çeşitli düzenlemelere sahiptir demek yanlış olmayacaktır.

Kanunun 75. Md., işçi özlük dosyası başlığını taşımaktadır. Bu maddeye göre, işveren tüm çalışanları için özlük dosyası düzenlemek durumundadır. Bu dosyada, işçinin kimlik bilgileri ile işçiye ait çeşitli kayıtlar bulundurulmalı ve işveren bu bilgileri gerekli hallede talep eden kurumlara göstermelidir. Ancak aynı madde, işvereni bu bilgileri doğru saklamak konusunda da sorumlu tutmaktadır. İşveren edindiği bilgilerin tamamını hukuka uygun olarak toplamalı ve saklamalıdır. Ayrıca işveren gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamak yetkisine de sahiptir (4857 Sayılı Kanun, 75. Md).

iv. 5490 Sayılı Nüfus Hizmetleri Kanunu

“Kişinin doğumundan ölümüne kadar kişisel ve medeni durumuna, uyrukluğuna ve bunlarda meydana gelebilecek değişikliklere ait doğal ve hukuki olayların belirlenip saptanması, bu amaçla düzenlenmiş kütüklere yazılması, elektronik ortamda ulusal adres veri tabanının oluşturulması, nüfus kayıtları ile adres bilgilerinin ilişkilendirilmesini sağlamak” (5490 Sayılı Kanun, 1. Md) amacını taşıyan bu kanun aslında devletin bilgi edinme, kişiyi koruma, sosyal devlet olma, suçu önleme ve benzeri amaçlarına hizmet ettiğinin bir göstergesi olarak kabul edilmelidir.

Fakat buna rağmen, nüfusa ilişkin bilgilerin toplanması da çeşitli kurallara tabidir. Kanunun 7. Md. hangi kişisel bilgilerin aile kütüklerinde yer alması gerektiğinin sınırları net biçimde açıklanmaktadır. Buna göre, Türkiye Cumhuriyeti kimlik numarası, bireyin kayıtlı bulunduğu il, ilçe, köy veya mahalle adı ile cilt, aile ve birey sıra numarası, kişinin adı ve soyadı, cinsiyeti, baba ve ana adı ile soyadları, evli kadınların önceki soyadları, doğum yeri ile gün, ay ve yıl olarak doğum tarihi ve kütüğe kayıt tarihi, evlenme, boşanma, soy bağının kurulması veya reddi, ölüm, vatandaşlığın kazanılması veya kaybedilmesi gibi kişisel durumda meydana gelen değişiklik veya yetkili makamlarca yapılan düzeltmeler gibi bilgiler kaydedilmeli ve saklanmalıdır. Ayrıca bireyin dini, medeni hali ile yaşadığı yerin adresi de kaydedilmektedir (5490 Sayılı Kanun, 7. Md).

Fakat elbette bu kayıtların korunması ve bilginin başkalarının eline geçmemesi gerekmektedir. 9. Md. buna ilişkin kuralları açıklamaktadır. Madde açıkça nüfus kayıtlarının gizli olduğunu belirtmektedir. Maddeye göre nüfus bilgilerine sorumlu memur ile denetlemeye yetkili kişiler dışında birinin ulaşması yasaktır. Ancak ilgili madde mahkemeleri gerekli hallerde bu bilgilere ulaşmaya da yetkili kılmıştır ((5490 Sayılı Kanun, 9. Md).

v. 213 Sayılı Vergi Usul Kanunu

Vergi Usul Kanunu, Maliye Bakanlığının vergi yükümlüleri hakkında bilgi toplama ve saklama yetkisine ilişkin kuralları da barındırmaktadır. 148. Md. bu hükümleri açıklamaktadır. Maddeye bakıldığında, “kamu idare ve müesseseleri, mükellefler veya mükelleflerle muamelede bulunan diğer gerçek ve tüzel kişilerin”, Maliye Bakanlığı’nın istemesi halinde bilgi vermeye zorunlu olduklarını belirtmektedir (213 Sayılı Kanun, 148.Md).

Aynı kanunun 152. Md., edinilen bilgilerin güvenli biçimde saklanması gerektiğinin altını çizmektedir (213 Sayılı Kanun, 152. Md). Fakat bu madde,

saklanma esnasında hangi önlemlerin alınması gerektiğine açıklık getirmemekte, bu konudaki politika ve uygulamaları Maliye Bakanlığı'na bırakmaktadır.

vi. 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanunu

Millî İstihbarat Teşkilatı'nın kişisel verileri toplama konusunda çeşitli yetkileri mevcuttur ve kurumun kurulması, işleyişi, görev ve faaliyetlerine ilişkin detaylar 2937 Sayılı Kanun ile çerçevelenmektedir. MİT'in bu kanuna göre sınırsız bilgi toplama yetkisi mevcuttur ve bu bilgilerin içinde kişisel verilerin de olabileceği unutulmamalıdır. MİT, dış güvenlik, terörle mücadele ve millî güvenliğe ilişkin konularda Bakanlar Kurulunca verilen görevleri yerine getirmekle görevlidir. Bu görevler kanunlar ile açıklanabilmektedir. Ancak Bakanlar Kurulu'nun MİT'e ne tür görevler vereceği konusunda bir açıklama ve sınırlamanın olmadığı da dikkat çekmektedir. Görevler, terör, uluslararası suçlar, siber suçlar ve benzer nedenler ile ilişkili olabilecek ve bu görevler sebebi ile MİT kişisel verileri toplamaya gerek duyabilecektir (Çokmutlu, 2014: 135).

vii. 5809 Sayılı Elektronik Haberleşme Kanunu

2008 yılında kabul edilen ve yürürlüğe giren 5809 sayılı Elektronik Haberleşme Kanunu elektronik ortamda rekabetin sağlanması, tüketicilerin korunması gibi amaçlara sahiptir. Fakat bunun yanı sıra kişisel verilerin korunmasına ilişkin hükümleri de mevcuttur. 12. Md. kişisel verilerin korunması konusunda işletmecileri sorumlu tutmaktadır (5809 Sayılı Kanun, 12. Md).

Bu kanunun 55. Md. abonelerin iletişim, kimlik ve/ya cihaz bilgilerinin dağıtılması ve değiştirilmesi konularında da kurum iznini gerekli olduğunu belirtmektedir. 56. Md. kişi ve kurumların kimlik bilgilerini içeren elektronik cihazların kopyalanamayacağını, çoğaltılamayacağını, dağıtılamayacağını ve değiştirilemeyeceğini belirtmektedir (5809 Sayılı Kanun, 55 ve 56. Md).

viii. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

2007 tarihinde yürürlüğe giren 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un amacı, "içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir" (5651 Sayılı Kanun, 1. Md).

Kanunun 9. Md. gereğince, özel hayatın gizliliği nedeni ile içerik engellemeler yapmak mümkündür. "İçeriğin Yayından Çıkarılması ve Erişimin Engellenmesi" başlığına sahip 9.Md. gerçek ve tüzel kişilerin, elektronik ortamlarda kişisel bilgilerinin yayınlanması halinde bunların içeriklerinin gizlenmesini isteyebileceğini belirtmektedir. Benzer şekilde bu kişiler mahkemeye giderek bu bilgiye erişimin engellenmesini isteme hakkına da sahiptirler (5651 Sayılı Kanun, 9. Md).

ix. 6098 sayılı Türk Borçlar Kanunu

Türk Borçlar Kanunu'nda kişisel verilerin korunması konusu Türk Medeni Kanun'daki gibi ele alınmaktadır. Kanun'un 49. Md. haksız bir fiil ile bir başkasına zarar verenleri, bu zararı gidermek ile sorumlu tutmaktadır. Buradan hareketle, kişisel verilerin kullanılması sonrasında bireye zarar verilmesi halinde kullanan kişinin sorumluluk sahibi olacağını söylemek yanlış olmayacaktır (Çokmutlu, 2014: 127).

x. Ticaret Kanunu

İşletmeler arasında sürekli olarak rekabet mevcuttur ve bu rekabet nedeni ile kimi zaman haksız kazanç elde etmek isteyen işletmeler, müşterilerinin kişisel verilerini kullanabilmektedirler. Ticaret Kanunu bunu yasaklamaktadır. Bununla birlikte bir tüzel kişi kendisine ait kişisel bilgilerin kullanılmasını da yine bu kanun ile sağlamaktadır. Örneğin izinsiz şekilde kar ve prestij elde etmek gibi sebeplerle bir

şirket başka bir şirketin logosunu ya da adını kullanabilmektedir. Türk Ticaret Kanunu'nun 56. Md. ve sonrasındaki hükümler kişisel verilerin kullanılması söz konusu olduğunda tazminat isteme hakkını kişiye vermektedir (Ayözger, 2016: 98).

xi. Ceza Muhakemesi Kanunu

Suçluların tespit edilmesi esnasında kişiye özel bilgiler toplanabilmektedir. 5271 sayılı Ceza Muhakemesi Kanunu'nun 75. Md. ve sonrası, şüpheli ya da sanıkların veya diğer kişilerin fiziksel muayenelerinin, vücutlarından alınan örneklerin, nüfus bilgilerinin ya da şüpheli, mağdur ve suç mahallindeki kişilerin tespit edilmesine yönelik yapılan biyolojik ve moleküler incelemelerin sonuçlarının alınmasına ilişkin kuralları belirlemektedir. Suçların tespit edilmesine yönelik işlemlerde, kişilere özgü bilgilere ulaşılmak durumunda kalınabilmektedir. Cumhuriyet savcısı gerekli gördüğü hallerde kişilerin parmak izi, kimlik bilgileri, soy ağacı, adresi, fotoğraf, vücudundaki özelliklere ilişkin bilgilerin toplanmasını isteme yetkisine sahiptir. Fakat 80.Md., bu bilgilerin tamamının kişisel veri niteliğinde olduğunu ve bunların toplanmasının suçun tespit edilmesi dışında hiçbir sebeple kullanılmayacağını açıkça belirtmektedir (5271 sayılı Kanun, 75.76.78 ve 80. Md.).

CMK'nın kişisel veriler ile ilgili bir diğer maddesi de 134. Md.'dir. Bu madde, bilgisayar ortamlarında var olan kişisel bilgiler ile ilgilidir. Bu madde suçun tespit edilebilmesi için kişilerin bilgisayar ortamındaki hareket ve bilgilerinin izlenebileceğini, bunlardan delil elde edilebileceğini belirtmektedir. Ancak bunun yapılabilmesi için Cumhuriyet savcısının kararı gerekmektedir. Toplanan bilgiler, suç tespiti ve mahkeme delili dışında kullanılmayacaktır (5271 sayılı Kanun, 134. Md.).

xii. Bilgi Edinme Kanunu

24.10.2003 tarihinde Resmî Gazete 'de yayımlanarak yürürlüğe giren bu kanun bilgiyi, "kurum ve kuruluşların sahip oldukları kayıtlarda yer alan her türlü veri" şeklinde tanımlamaktadır. Bilgi edinme bu kayıtlara ulaşabilme imkânı anlamına

gelmektedir. Ancak bilgi edinme konusunda bu kanun tarafından kurallara uyulması gerekmektedir. Bilgi edinme hakkının kişisel verilere ulaşmak için kullanılması olasılığının olduğu unutulmamalıdır. Fakat bu kanun sayesinde kişi aynı şekilde kendisine ilişkin kayıtları öğrenme hakkına da sahip olmaktadır. Böylelikle kurum ve kuruluşların kişilere yaklaşımlarında objektif olmaları hedeflenmektedir (Ayözger, 2016: 104).

Bilgi Edinme Kanunu'nun 21.Md. kişisel verilerin güvenliğine ilişkin ifadeleri içermektedir. Maddeye göre “1) Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. (2) Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir” (4982 sayılı Kanun 21. Md.).

2.3.4. Yönetmelikler

i. Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği (THKY)

Bilgi Teknolojileri ve İletişim Kurumu tarafından 28 Ekim 2017 de yayımlanan bu Yönetmeliğin amacı elektronik haberleşme sektöründe tüketici hak ve menfaatlerini korumaya yönelik usul ve esasları belirlemektir (THKY, 1. Md). 5809 sayılı Elektronik Haberleşme Kanununa dayanılarak hazırlanmış olan bu yönetmeliğin 5. Md. elektronik haberleşme hizmetlerinden yararlanan tüketicilerin sahip olduğu asgari hakları açıklamaktadır. Buna göre, elektronik haberleşme alanında abone olan kişilerin kişisel verilerinin kamuya açık rehberlerde yer alıp almamasını talep etme hakkı mevcuttur. Ayrıca aboneler rehberlere ayırım gözetmeksizin kaydolma ya da olmama hakkına da sahiplerdir (THKY, 5. Md).

Söz konusu yönetmeliğin 6. Md. şeffaflık ve bilgilendirmeye ilişkin hükümleri açıklamaktadır. Burada kişisel verilere atıf yapılmasa da, işletmecilerin

sundukları hizmetlere ilişkin erişim ve bu hizmetlerin kullanımı ile ilgili olarak asgari aşağıdaki bilgiler olmak üzere, özellikle hizmetler arasında seçim yapılırken ve abonelik sözleşmesi kurulurken tüketicilerin karar vermelerinde etkili olabilecek hususlar ile dürüstlük kuralı gereğince bilgilendirilmelerinin gerekli olduğu her durumda talep olmaksızın tüketicileri bilgilendirmekle ve bu bilgilere kolayca ulaşılabilmesini sağlamakla yükümlü olması kişisel veriler konusunu da etkilemektedir (THKY, 6. Md).

7.Md., abonelik sözleşmeleri hazırlanırken ve imzalanırken hangi kurallara uyulması gerektiğini açıklamaktadır. Bu maddeye göre abonelik sözleşmesi yapılırken rehber hizmetleri için, aboneden bu rehberlerde kişisel verilerinin yer alıp almayacağına ilişkin tercihleri alınmaktadır (THKY, 7. Md). Buna göre kişiler diledikleri takdirde kişisel verilerini paylaşmama hakkına sahiptir.

ii. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik (EHSKVİY)

2012 tarihinde yayınlanan bu yönetmeliğin amacı elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması için elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenlemektir. Ancak bu noktada haberleşmenin içeriğine ilişkin verilerin saklanması bu yönetmeliğin kapsamının dışında olduğunu da belirtmek gerekmektedir (EHSKVİY, 1.Md).

Yönetmeliğin 4. Md. kişisel verilerin hukuka uygun ve dürüstlük kurallarına göre, kişinin rızasını alarak, elde edilme amacıyla bağlantılı şekilde, güncel ve doğru olması gibi gereklilikleri açıklamaktadır. Bu maddeye göre verilerin yurt dışına aktarılması yasaktır. Kişisel verilerin işlenmesi kapsamında abone tarafından işletmeciye verilen rıza, sadece alınan hizmete özgü olmak koşuluyla, kişisel verilerin işletmeci tarafından yetkilendirilen taraflar marifetiyle işlenebilmesini de kapsamalıdır. Madde, işletmeci tarafından yetkilendirilen taraflarca bu Yönetmelik hükümlerinin ihlal edilmesi de dâhil olmak üzere kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda

kullanılmasının temininden işletmeci sorumludur demektedir (EHSKVİY, 4. Md).

5. Md. göre işletmecilerin kişisel verilerin işlenmesi esnasında hangi güvenlik politikaları kullanacaklarını belirlemeleri gerekmektedir. Bu verilerin güvenliği için teknik ve idari tedbirlerin alınması da işletmecilerin sorumluluğundadır. İşletmeciler teknolojik gelişmeleri de takip ederek güvenlik tedbirlerini almak durumundadırlar (EHSKVİY, 5. Md).

İşletmeci, şebekenin ve kişisel verilerin güvenliğini ihlal eden belirli bir risk olması durumunda bu risk hakkında Kurumu ve Kurum tarafından gerekli görülmesi halinde abonelerini/kullanıcılarını etkin ve hızlı bir şekilde bilgilendirmekle yükümlüdür. Şayet risk işletmecinin sorumluluk alanı dışındaysa, söz konusu riskin kapsamı, giderilme yöntemleri ve yaklaşık maliyeti hakkında abonelerin/kullanıcıların etkin ve hızlı bir şekilde bilgilendirilmesi sağlanmalıdır. İşletmeci, kişisel veri ihlali olması durumunda söz konusu ihlalin niteliği ve sonuçları hakkında abonelere/kullanıcılara yapılacak bilgilendirmenin detayları ve ihlalin giderilmesi için alınan tedbirlere ilişkin olarak Kurumu da bilgilendirmek zorundadır. Bütün bilgilendirmeler ücretsiz olarak yapılmalıdır. Ayrıca ihlalin yenilenmemesi için bunun nedenleri, bulunan çözüm metodolojileri gibi bilgiler kayıt altına alınmalıdır (EHSKVİY, 6. Md).

7.Md.haberleşmenin gizliliğine ilişkin hükümleri ele almıştır. Kişilerin haberleşme trafiklerinin gizlilikleri esastır. Konuyla ilgili hazırlanmış olan mevzuatın ya da yargı kararlarının haricinde kişinin elektronik haberleşmeleri esnasında yaptığı görüşmelerin izlenmesi/dinlenmesi yasaktır. Bu dinleme ve izleme için haberleşmeyi gerçekleştiren tüm tarafların açık rızası olmalıdır. Elektronik haberleşme şebekeleri, haberleşmenin iletimini gerçekleştirmek dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili kullanıcıların/abonelerin verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve rızalarının alınması kaydıyla kullanılabilir (EHSKVİY, 7. Md).

8.Md., işletmecilere sundukları hizmetin dışında kalan verileri işlemeyi kesinlikle yasaklamaktadır. Trafik verisi, ilgili mevzuat hükümlerine uygun olarak, trafiğin yönetimi, ara bağlantı, faturalama, yolsuzluk tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile ara bağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanabilecektir (EHSKVİY, 8. Md).

11.Md.son yıllardaki en önemli konulardan birine açıklık getirmektedir. Konum verilerine ilişkin düzenlemelere yer verilen bu maddeye göre katma değerli elektronik haberleşme hizmetleri sunmak amacıyla ihtiyaç duyulan ve trafik verisi niteliğinde olmayan konum verileri, anonim hale getirilerek veya ilgili abonelerin/kullanıcıların işlenecek konum verileri, işleme amacı ve süresi hakkında bilgilendirilmelerinden sonra rızalarının alınması kaydıyla, alınan rızaya uygun olarak sadece katma değerli elektronik haberleşme hizmetlerinin gerektirdiği ölçü ve sürede işlenebilir. İşletmeciler trafik verisi niteliğinde olmayan konum verilerinin işlenmesinde abone/kullanıcılara geçici olarak bu verilerin işlenmesini reddetme imkânı sağlar. Kişilerin konum bilgilerini kısa mesaj, e-posta gibi basit şekillerde verdikleri rızaları her zaman ücretsiz biçimde geri alma hakları mevcuttur. Ancak adli sebepler, afet ve acil durum gibi haller konum bilgisini kullanma konusunda kişinin rızasının alınması haline istisna getirmektedir (EHSKVİY, 11. Md).

14. Md., elektronik haberleşme işletmelerinin hangi süreler ile veri saklayabileceklerini çerçeve içine almaktadır. Şayet haberleşme devam ediyorsa, buna ilişkin veriler bir yıl süre ile haberleşme devam etmiyorsa, abonelik sonlanmışsa ise üç ay süre ile saklanabilecektir. Fakat kişisel verilerle ilgili bir dava ya da süreç devam ediyorsa, bu süreç sonuçlanana dek veriler saklanmaya devam etmelidir. Ayrıca kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları dört yıl süre ile saklanmalıdır (EHSKVİY, 14. Md).

2.4. Kişisel Verileri Koruma Kurum ve Kurulu

Kişisel verilerin korunmasına ilişkin düzenleyici ve denetleyici bir kurum olan KVKK, 6698 sayılı kanunun kabul edilmesinin ardından kurulmuştur. Meclis görüşmelerinde kurumun bağımsızlığına ilişkin endişe ve tartışmalar olmasına karşın kurumun kendi web sitesinde yer alan bilgilere göre kurum Avrupa Konseyinin 108 sayılı S özleşmesi ve Avrupa Birliğinin 95/46/EC sayılı Direktifine uygun şekilde bağımsızdır. Kurum bağımsızlık konusunu “Kurumun, Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getireceği ve kullanacağı, görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişinin Kuruma emir ve talimat veremeyeceği hüküm altına alınmaktadır. Bu hüküm, Kurumun görevini bağımsız bir şekilde yerine getirebilmesi bakımından önem arz etmektedir” şeklinde açıklamaktadır (KVKK, 2017).

Kişisel Verileri Koruma Kurumu'nun karar organı kurul 'dur. Bu kurulun faaliyetleri 9 üye tarafından gerçekleştirilmektedir. Bu üyelerin beş tanesi TBMM, iki üyesi Cumhurbaşkanı, iki üyesi de bakanlar kurulu tarafından seçilmektedir. TBMM beş Kurul üyesini şu şekilde belirler: Seçim için, siyasi parti gruplarının üye sayısı oranında belirlenecek üye sayısının ikişer katı aday gösterilir ve Kurul üyeleri bu adaylar arasından her siyasi parti grubuna düşen üye sayısı esas alınmak suretiyle Türkiye Büyük Millet Meclisi Genel Kurulunca seçilmektedir (KVKK, 2017). İşte zaten kurumun karar organı kurulun tarafsızlığına ilişkin çıkan tartışmaların en temel noktalarından biri de bu seçilme şartları olmuştur.

Fakat bu noktada siyasi partilerde adaylar arasından kimin seçileceğine dair fikir yürütme ve kime oy kullanılacağına dair bir görüşme yapılamayacağı da unutulmamalıdır. Fakat üyelerin belirlenmesinin ardından 10 gün sonra oylama yapılacaktır ve bu durum resmi bir kararlaştırma olmasa bile aday belirlemek için yeterli bir süre olarak görülebilecektir.

Burada aday olabilecek kişilerin taşınması gereken şartları da incelemek gerekmektedir (KVKK, 2017):

- i. Kurumda görev alınacak konulara ilişkin bilgi ve deneyimlerinin olması şarttır.
- ii. Kurumda çalışabilmek için devlet memuru olma konusunda bir engellerinin bulunmaması gerekmektedir.
- iii. Üye ve adayların bir siyasi parti üyelikleri bulunmamalıdır.
- iv. En az 4 yıllık üniversite diplomalarının olması gerekmektedir.
- v. Kamu kurum ve kuruluşlarında, uluslararası kuruluşlarda, sivil toplum kuruluşlarında veya kamu kurumu niteliğindeki meslek kuruluşlarında ya da özel sektörde toplamda en az on yıl çalışmış olmaları gerekmektedir.

2.4.1. Kurul'un Çalışma Esasları

Kişisel Verilerin Koruması Kanunu'nun 23. Md., Kurul'un çalışma esaslarına ilişkin düzenlemeleri içermektedir. Buna göre kurulun hangi günler toplanacağını ve toplantıların gündemlerini başkan belirlemektedir. Ancak gerekli görülen durumlarda belirlenmiş günlerin dışında, kurul üyeleri başkan tarafından olağanüstü toplantıya çağırılabilir. Burada kurulun bir toplantı yapabilmesi için başkan da dahil olmak üzere en az altı kişinin toplanmış olması şartını; ayrıca alınacak kararlarda kurul üyelerinin çekimser karar kullanamayacağını da belirtmek gerekmektedir.

Kurul üyeleri; kendilerini, üçüncü dereceye kadar kan ve ikinci dereceye kadar kayın hısımlarını, evlatlıklarını ve aralarındaki evlilik bağı kalkmış olsa bile eşlerini ilgilendiren konularla ilgili toplantı ve oylamaya katılamayacaklardır. Ayrıca hiçbir kurul üyesi öğrendiği bilgiyi başkaları ile paylaşamayacaktır. Hiçbir koşulda kurul üyelerinin öğrendikleri bilgileri kendi çıkarları için kullanmaları da kabul edilemez. Tüm görüşmelerin tutanağa yansıtılması gerekliliği de yine çalışma esasları arasında yer almaktadır. Kurulların toplantıları gizli tutulmalıdır ancak bunun aksi yönünde karar verilerek kamuoyuna duyurular yapılabilecektir (KVKK, 2017).

2.4.2. Kurul'un Görevleri

Kişisel Verileri Koruma Kurulu'nun kanun ile belirlenmiş olan başlıca görevlerini şu şekilde listelemek mümkündür (KVKK, 2017):

- i. Kurul özel nitelikli kişisel verilerin korunması için gerekli ve yeterli önlemlerin alınmasını sağlamaktadır.
- ii. Verilerin aktarılması söz konusu ise ve aktarım yapılacak olan ülkelerin veri güvenliğinin yeterli düzeyde olmaması halinde kurul aktarım için ilgili ülkeden yazılı güvenlik teminatı almakta ve ancak bu şekilde aktarımı onaylamaktadır.
- iii. Kurul hangi ülkelerin kişisel veri korunması konusunda yeterli düzeyde olduğunu araştırmakta ve tespit etmektedir.
- iv. Gerek görmesi halinde, veri sorumluları tarafından kendisine yapılan, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından ele geçirildiğine ilişkin bildirimleri ilan etmektedir.
- v. Kurul, veri sorumlularına yapılan başvuruların reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi gibi durumlar söz konusu olduğunda şikâyetlere ilişkin araştırmaları yapmaktadır.
- vi. Şikâyet üzerine veya resen harekete geçmek suretiyle tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine de yine kurul karar vermektedir.
- vii. Şayet kişisel verilerin korunması ve işlenmesine ilişkin yaygın sorunlar mevcut ise, kurul ilke kararlar alabilmektedir.
- viii. Telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar vermek de yine kurumun yetkileri arasındadır.
- ix. Kurul başkanlığı veri sorumlusunun sicilinin takibini yapabilmektedir.

x. Veri Sorumluları Siciline kayıt konusunda gerekli görülmesi halinde kurul tarafından istisnalar getirilebilmektedir.

xi. Kurulun kişisel verilerin korunmasına ilişkin öngörülen yükümlülükleri ihlal eden memurlar hakkında disiplin soruşturması yapılması için ilgili kurumlara bildirim yapma yetkisi de mevcuttur.

xii. Kurulun belki de en önemli görevlerinden biri kişisel verilerin insanların temel hak ve özgürlüklerini kısıtlamayacak şekilde işlenmesini sağlamaktır.

xiii. Kurumun işleyişine, veri güvenliği ile ilgili yükümlülükleri belirlemeye ve veri sorumlusu ile temsilcisinin görev yetki ve sorumluluklarına ilişkin düzenleyici işlemler de kurulun yetki ve sorumluluk alanı içindedir.

xiv. Kurumun işleyişine, veri güvenliği ile ilgili yükümlülükleri belirlemeye ve veri sorumlusu ile temsilcisinin görev yetki ve sorumluluklarına ilişkin düzenleyici işlemleri yapmanın yanı sıra kurul kurumun stratejik planına uygun kararlar alınması ve kurumun ihtiyaçları konusundaki alım satım işlemlerinin onaylanmasını, yıllık ve diğer rutin raporların kontrol ve onaylanmasını da gerçekleştirmektedir.

2.4.3. Kurum Tarihçesi, Başkan ve Üyeleri

Mart 2016 tarihinde Kişisel Verilerin Korunmasına ilişkin kanunun mecliste kabul edilmesinin ardından, 6698 sayılı Kişisel Verilerin Korunması Kanununun 21.Md. hükümlerine göre Kişisel Verileri Koruma Kurulunda boş bulunan 3 üyelik için Türkiye Büyük Millet Meclisi Genel Kurulunun 5 Ekim 2016 tarihli 3. birleşiminde yapılan seçim sonucunda aşağıda adı ve soyadı yazılı isimler, seçilmişlerdir. Bu isimler, Cabir Bilirgen, Cengiz Paşaoğlu ve Turan Arık'tır. Ancak kurulun eksik üyeleri olduğundan; Bakanlar Kurulu kararı ile iki kişinin daha ataması yapılmış; Murat Karakaya ve Hasan Aydın eksik üyeler için olan koltuklara seçilmişlerdir. Kanunun 21. Md. gereği, Cumhurbaşkanlığı tarafından iki kişi daha seçilmiştir ve bunlar Faruk Bilir ve Şaban Baba olmuştur. Bu atamaların ardından, 4 Ocak 2017'de Türkiye Büyük Millet Meclisi Genel Kurulunun 4 Ocak 2017 tarihli 50.

Birleşiminde son 3 üyelik koltuğu için seçim yapılmış ve buralarda İhsan Ezel Büyüksekban ve Vedat Yıldız görevlendirilmişlerdir. Yemin edilmesinin ardından üyeler arasındaki oylama ile Faruk Bilir 1.Başkan, Cabir Bilirgen ise 2. Başkan olmuşlardır (KVKK, 2018).

2.5. 5237 Sayılı Türk Ceza Kanunu'na Göre Kişisel Verilerin Korunmasına İlişkin Suç Tipleri

Hukukun uygulanabilmesi için, kurallara uymayanlar için çeşitli uygulamaların yapılması gerekmektedir. Kişisel verilerin korunması, işlenmesi ve paylaşılması konusunda en önemli konulardan biri teknolojinin hızla gelişmesi ve internet ortamında bilgi sızma riskinin artmasıdır. TCK'nın kişisel verilerin korunması ve korunmaması halinde uygulanacak yaptırımlara ilişkin maddeleri henüz siber suçlar kapsamında kişisel verilerin güvenliğini koruyabilmek konusunda yetersizdir. TCK'de düzenlenen kişisel verilerin korunmasına yönelik hükümler eksik norm niteliğinde olup özellikle hukuka aykırılığın hangi hallerde oluştuğuna ilişkin olarak başvurulabilecek olan kişisel verilerin korunmasına ilişkin düzenlemenin yapılması gerekmektedir (Bük, 2015: 84). Bu noktada, günümüz şartlarına uygun olan TCK maddelerini incelemek gerekmektedir.

Ancak bunun öncesinde kişisel veriler hakkında işlenen suçların ne olduğunun doğru kavranabilmesi için TCK'da açıklanmış olan "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünün kısaca incelenmesi gereklidir. TCK'nın 9. Bölümü, Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar olarak adlandırılmıştır ve bölüm 132. Md. ile başlamaktadır. 132. Md. haberleşmenin gizliliğini vurgulamaktadır. 133. Md. kişiler arasındaki konuşmaların dinlenmesi ve kayda alınmasını suç olarak kabul etmektedir. 134. Md. ise "özel hayatın gizliliğini ihlal" suçuna ayrılmıştır. 135. Md. Kişisel verilerin hangi şartlarda kaydedileceğini ve şartlara uyulmaması hallerini; 136. Md. verilerin hukuka aykırı biçimde edinilmesi ya da dağıtılmasını işlemektedir. 138. Md., verilerin yok edilmemesi halinde gerçekleşecek yaptırımları, 139.Md. ise şikâyet durumunu irdelemektedir (TBMM, 2004).

2.5.1. Kişisel Verilerin Kaydedilmesi Suçu (Md. 135)

Bu çalışmanın önceki bölümlerinde TCK'da kişisel verilere ilişkin maddeler kısaca açıklanmıştır. Ancak bu noktada bunların daha detaylı hale getirilmesi hem yeni kanun ve TCK hem de AB ve Türkiye arasındaki mevzuatın uyumluluğu hakkında fikir edinilmesi açısından önemlidir.

135. Md. iki fıkrada düzenlenmiştir ve birinci fıkra, kişisel verilerin hukuka aykırı kaydedilmesini açıklamaktadır. Hukuka aykırı bir şekilde kişisel verileri kaydeden sorumlulara 6 ay- 3 yıl aralığında hapis cezası verileceği açıklanmaktadır. İkinci fıkrada ise bireylerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kişilerin de birinci fıkradaki gibi işlem göreceğini açıkça belirtmektedir (TCK 135. Md).

Bu verilerin izinsiz şekilde kayıt altına alınması aslında kişinin haklarına saldırıdır. Özellikle teknolojinin gelişmesi, insanların kişisel verilerine ilişkin sorulara alışması ve sorgulamadan yanıtlamasına neden olmuştur. Bugün hastanelerden sigorta kurumlarına ve hatta konut sitelerinde bile kişisel verilere ilişkin sorular yöneltilmekte, kolaylıkla elde edilmektedir. İşte bu nedenle kuruluşların kişilerin verilerini alması ve işlemesi konusunda yasal düzenlemeler şart hale gelmiştir. Çünkü bu kurumlar, kişisel verileri elde etmeden işleyemeyeceklerdir. Kamusal ve özel faaliyetlerin sürdürülebilmesi açısından kişisel verilere ihtiyaç vardır. Ancak yasal düzenlemelerin yanı sıra, kişilerin, verilerini koruma konusunda ısrarcı ve dikkatli olmaları önem taşımaktadır.

2.5.2. Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu (Md.136)

136. Md. bakıldığında, kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi eylemleri halinde ne tür cezai yaptırımların söz konusu olacağı açıklanmaktadır. Madde net bir şekilde kişisel verileri hukuka

aykırı şekilde başkasına veren, bunları yayan ya da ele geçirenlerin hapis cezası ile cezalandırılacağı yazılıdır. Ancak 137. Md. nitelikli hallerden de söz edilmektedir 137 Md., 135 ve 136. Md. tanımlanan suçlara atıf yapmakta ve suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle oluşması halinde ceza yaptırımının arttırılacağını açıkça belirtmektedir (TCK 136 ve 137. Md).

2.5.3. Verilerin Yok Edilmemesi Suçu (Md.138)

Kişisel verilerin hukuka uygun biçimde yok edilmesi, onların toplanması ve işlenmesi kadar önemli bir konudur. Yok etme gerçekleşmediği takdirde, eski ve yanlış verilerin kalabileceği gibi kişinin verileri istenmeyen yerlere de ulaşabilecektir. TCK'nin 138. Md.de bu öneme vurgu yapmakta ve “kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediğinde altı aydan bir yıla kadar hapis cezası verilir” demektedir (TCK, 138. Md). Yasa koyucu bu suça ilişkin düzenlemeyle amaç olarak, kişisel verilerin her ne kadar hukuka uygun olarak kaydedilse dahi sürekli olarak kayıtlı kalmalarının, örneğin bilişim sistemi içerisinde bulunmasının ve böylece her zaman ulaşılabilir olmasının önüne geçilmesi hedeflenirken, aynı zamanda verileri sistemden silmeyerek bu konudaki görevlerini ihmal edenlere yaptırım öngörülmektedir (Bük, 2015: 88).

2.6. Kişisel Verilerin Korunmasına İlişkin Anayasa Mahkemesi Kararları

Kişisel verilerin korunmasına ilişkin kuşkusuz en popüler iptal davası, Türkiye Büyük Millet Meclisi üyeleri Engin Altay, Levent Gök, Özgür Özel ile birlikte 124 milletvekilinin açtığı iptal davasıdır. 2016 tarihinde açılan bu davada, İptal davasının konusu, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4, 5,6, 7, 8, 9, 13, 15, 16, 24,28 ve 30 numaralı maddelerinde iptali istenen durumlardır. Bu istem Anayasa mahkemesi tarafından reddedilmiştir.

Bu noktada bir diğ er bireysel başvuru ve kararı incelenecektir.2014/1970 numaralı başvuruda, O.K. İsimli kiři, Başvuru, üçüncü bir kiři (K.M.) tarafından rıza olmaksızın kayda alınan ses ve görüntünün ceza soruşturmasında delil olarak sunulması üzerine řikâyette bulunmuş ve dava açılmıştır. Kiři kişisel verileri ve özel hayatına saygı duyulmadığı gerekçesi ile hukuki yollara başvurmuştur. İddianamenin başvurucuya 10/5/2013 tarihinde tebliğ edilmesinden sonra başvuru, Ankara Cumhuriyet Başsavcılığına başvurarak "kiřiler arasındaki konuşmaların dinlenilmesi ve kayda alınması" suçunun işlendiğini ve K.M.nin cezalandırılması gerektiğini belirtmiştir. řikâyet üzerine başlatılan soruşturma kapsamında 13/5/2013 tarihinde başvurucunun ifadesi Cumhuriyet savcısı tarafından alınmış, iddia ve řikayetler yinelemiştir. Şüpheli K.M. verdiği ifadesinde durumdan ve bilgilerden haberdar olduğunu ancak suçlamaları kabul etmediğini belirtmiştir. Ankara Cumhuriyet Başsavcılığı 16/9/2013 tarihli kararıyla "kiřiler arasındaki aleni olmayan konuşmaları kayıt etme" suçu kapsamında kovuşturmaya yer olmadığına dair karar vermiştir. Ancak mahkemenin kararına itiraz edip temyize başvurulduktan sonra, AYM, Özel hayata saygı hakkının ihlal edildiğine ili kin iddianın açıkça dayanaktan yoksun olması nedeniyle kabul edilemez olduğuna karar verilmiştir (AYM Kararlar Bilgi Bankası).

Bir başka dava da 2015/32 esas, 2015/102 karar numarası ile görülen AYM davasıdır. Bu davada, Sanık hakkında kişisel verileri hukuka aykırı olarak ele geçirme ve yayma suçundan açılan kamu davasında, itiraz konusu kuralın Anayasa'ya aykırı olduğu kanısına varan Mahkeme, iptali için başvuru gerçekleştirilmiştir. Batman 2. Asliye Ceza Mahkemesi, řikayetçinin, sanık tarafından bilgilerinin izinsiz alınıp kullanıldığına dair řikâyeti üzerine inceleme yapmış ve Kanun'un itiraz konusu 136. Md. göre bir sorun olmadığı kanaatine varmıştır. Kanun maddesi, "Kiřisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kiři, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır" demektedir. Bunun üzerine karara itiraz eden řikayetçi AYM'ye başvurmuş, incelemeler başlatılmıştır.

2. Başvuru kararı ve ekleri, itiraz konusu kanun hükmü, dayanılan ve ilgili görülen Anayasa kuralları ve bunların gerekçeleri ile diğ er yasama belgeleri okunup incelenmiş, kanunda yer alan "kiřisel veri" kavramının teknolojik gelişmelere bağı olarak çok farklı şekillerde ortaya çıkabileceğ inden bu kapsama giren tüm verilerin

kanun koyucu tarafından önceden öngörülebilmesi ve tek tek sayılabılmesinin mümkün olmadığı belirtilmiştir. İtirazın kabul edilmesi halinde AYM'nin 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun, 21.2.2014 tarihli ve 6526 sayılı Kanun'un 4. Md. değiştirilen 136. Md. (1) numaralı fıkrasının Anayasa'ya aykırı olması ve iptali söz konusu olacaktır. Ancak, inceleme sonrasında mahkeme aykırılık olmadığını ve itirazın reddedilmesi gerektiğini söylemiştir (kararlaryeni.anayasa.gov.tr).



SONUÇ

Kişisel verilerin gizliliğinin korunması konusu, çok hassas bir konudur çünkü en sınırları belirsiz alandır. Kişinin kim olduğunun belirlenmesinden farklı olarak onun onurunu ve özel yaşamını sergileyecek her türlü bilgi kişisel veri sayılmaktadır. Bu durum toplumdan topluma hangi verilerin kişisel veri sınıfında ele alınacağını değiştirdiği gibi, kanunların da yorumlanmasında farklılıkların ortaya çıkması olasılığını beraberinde getirmektedir. Kişisel verilerin gizliliğinin korunması, düşünce özgürlüğü ve bilgi alma hakkı gibi diğer temel hakları hem koruyan ve destekleyen hem de onlarla kimi zaman çelişen bir haktır ve yasa koyucuların bu ayrımı en doğru yapacak şekilde düzenlemeleri yapması gerekmektedir. Örneğin basının kişisel verileri gizleme ile düşünce ve ifade özgürlüğü arasında sıkışmaması, ya da kamuya mal olmuş kişilerin, düşünce ve ifade özgürlüğü nedeni ile unutulma hakkını kullanamaması söz konusu olabilmektedir.

Bugün kişisel veriler her yeredir ve modern insanı temel alan tüm sistemlerin işlemeye devam edebilmesi için insanların verilerinin toplanması ve işlenmesi şarttır. Bir hastanede hastalara aynı testlerin yeniden yapılarak zaman ve kaynak kaybedilmemesi, teşhisin doğru konulması ya da tedavi planına eksiksiz uyulabilmesi için kişisel verilerin saklanması lazımdır. Bunun dışında bir sigorta şirketinin kaza yapmayan kişilere indirimli hizmet sunabilmesi, eğitimde çocukların aile bilgilerinin, maddi durumlarının bilinmesi, doğru yerlere yardım ulaştırılması gibi pek çok nedenden dolayı kişisel veriler alınmakta ve işlenmektedir. Ancak kişisel verilerin satılması, reklam amaçlı kullanılması da söz konusu olabilmektedir. Buna örnek olarak web sitelerindeki çerez adı verilen yazılımları işaret etmek mümkündür. Yazılımlar kişinin yaşı, geliri, eğitim durumu gibi bilgileri alıp web siteleri arasında bilgi akışı sağlayabilmekte, buna göre reklamlar doğru kitlelere verilebilmektedir. Ancak bu durum kişinin bilgisinin haberi olmadan ve kontrolsüzce sızması anlamına da gelmektedir.

Kişisel veriler, günlük yaşamda teknolojinin de etkisi ile sürekli kullanılan bilgiler haline gelmiştir. Bugün kişiler yaptıkları hemen her faaliyette kişisel verilerini kullanmak ya da bunların işlenmesine izin vermek durumunda kalmaktadırlar. Ancak kişisel verilerin bu kadar sık kullanılması ve özellikle kolay paylaşılır hale gelmesi çeşitli sorunları da beraberinde getirmektedir. Kişisel verilerin gerçek kişiler için anonim hale gelmesi, bireyin sosyal yaşamını etkileyebileceği gibi dolandırılması ya da izlenebilmesini de mümkün hale getirmektedir. Tüzel kişilerin kişisel verilerinin kullanılması, ticari zorluklara, rekabet ortamında dezavantaja, yatırımcı ve ortaklar ile problemler yaşanmasına neden olabilmektedir. Kişisel veriler, kişinin kolaylıkla tespit edilmesine neden olabilen her türlü veriyi içerdiğinden kişisel veri kavramı sebebiyle yaşanacak avantaj ve dezavantajların skalası da oldukça geniştir.

Bu çalışmada, kişisel verilerin ne olduğu, saklanması artan önemi, uluslararası mevzuatta kişisel verilerin nasıl korunduğu ve Türkiye’de çok yeni olan kişisel verilerin işlenmesine ilişkin mevzuat ve bununla ilgili tartışmalar araştırılmıştır. Kişisel verilerin ne olduğunun halk tarafından bilinmesi, hemen her yerde kendilerine sorulan ve kişisel verileri kapsayan sorular karşısında bilinçlenmeleri ve neden bu bilgilerin istendiğinin anlaşılması, gerekli hallerde ise yok edilmesini talep edebilmeleri açısından oldukça önemlidir. Gelecek dönemlerde kişinin kişisel verileri nedeni ile sorunlar yaşamaması, yasaların yanında kişilerin bilincine de bağlı bir durumdur.

Dönemin iktidar partisi tarafından hazırlanan yasa tasarısının 108 sayılı Avrupa Konseyi Sözleşmesi ile 95/46 sayılı AB Direktifinin bir gerekliliği olarak hazırlanmış olduğunu ve tüm maddeleri için AB mevzuatının rehber olarak alındığını belirtilmiştir. Ana muhalefet partisi milletvekilleri kanun haline gelen yasayı iptal için anayasa mahkemesine taşımıştır ve iptal istemi reddedilmiştir. Bugün hala ilgili yasa Türkiye Cumhuriyeti Mevzuat Sisteminde yer almaktadır. Bugün Türkiye’de Kişisel verilerin korunmasına ilişkin kurallar, 6698 sayılı Kişisel Verilerin Korunması Kanunu’na göre düzenlenmektedir.

Sadece ulusal düzeyde değil uluslararası düzeyde de kişiler verilerin korunması zorunluluğu sonucunu doğmasından ötürü Birleşmiş Milletler, OECD, Avrupa Konseyi gibi uluslararası kuruluşlar kişisel verilerin korunmasına yönelik uluslararası düzeyde

kurallar belirlemişlerdir. Birleşmiş Milletler Rehber İlkeleri ile OECD Rehber İlkeleri, hukuki açıdan bağlayıcılığı olmayan düzenlemeler olmalarına karşın, kişisel veriler korunması alanında birçok ulusal ve uluslararası düzenlemenin yapılmasına sağlamıştır.

Çalışmamızda detaylandırdığımız üzere kişisel verilerin korunması üzerine çalışma ve yasal düzenlemeler uzun yıllardır Batılı hukuk sistemlerinin gündemindedir ve bu konu; çeşitli şekillerde düzenlenen ve güvence altına alınan önemli bir alanı oluşturmaktadır. Türkiye’de AK Veri Koruma Sözleşmesi çok zaman önce imzalanmasına karşın bu konuda kapsayıcı bir düzenleme yapılması çağdaş hukuk düzenleriyle kıyaslandığında oldukça geç olmuştur.

Kanımızca ülkemizde kişisel verilerin korunmasını sağlayacak, bu konuda temel ilkeleri ve denetim usulünü belirleyecek bir yasal düzenlemenin ve kişisel verileri koruma kanununun kapsamının daha da genişletilip, kişisel verilerin korunması konusuna verilen önemin çağdaş devletlere seviyesine çıkarılması mühim bir gerekliliktir.

Türkiye, 1981 yılında 108 Sayılı Avrupa Konseyi Sözleşmesi’ni imzalanmış olmasına karşın, bir süre sözleşmede zorunlu olarak belirtilen kişisel verilerin korunması alanını düzenleyen özel bir kanun çıkarmamıştır. Bu sebeple sözleşmeyi imzalayıp onaylamayan tek ülke olan Türkiye 95/46/AT sayılı Avrupa Birliği Yönergesine göre Avrupa ülkelerinin kişisel verileri eşdeğer koruma bulunmayan ülkelere aktarmamaları nedeniyle bu konuda sorun oluşturan bir alanda durmuş ve insan haklarına saygılı, demokratik bir hukuk devleti olma yolunda ilerlemesi açısından kişisel verilerin korunması alanında özel bir düzenleme yapılması bir zorunluluk halini aldığını net bir şekilde görmüştür. Nihayet 24 Mart 2016 tarihinde Kişisel Verilerin Korunması Kanunu Türkiye Büyük Millet Meclisi tarafından kabul edilerek yürürlüğe girdiğinde bu konudaki büyük bir hukuki boşluk doldurulmuştur. Kanun kişisel verilerin korunması hakkını düzenleyen önemli bir yasal düzenleme olmasına karşın bu konuda çağdaş düzenin gerekliliklerini sıkı takip etmek ve yasal düzenlemelerle bu kişisel verilerin korunması hakkının gelişme sürecini düzenlemek gerekmektedir.



KAYNAKÇA

AB Veri Koruma Çalışması, Article 29 Data Protection Working Party, EU,
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Akgül, Aydın. (2016). Kişisel Verilerin Korunması, Beta Basım Yayın

Aksoy, Hüseyin Can. (2010). Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi

Aydın, Sedat Erdem. (2014). AİHM içtihatları bağlamında kişisel verilerin kaydedilmesi suçu. İstanbul Üniversitesi / Sosyal Bilimler Enstitüsü / Kamu Hukuku Anabilim Dalı. Yüksek Lisans Tezi.

Ayözger, A. Çiğdem. (2016). Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, Doktora Tezi

Boğaziçi Üniversitesi Sosyal Politika Forumu. (2010). “Türkiye’de Eşitsizlikler: Kalıcı Eşitsizliklere Genel Bir Bakış,”http://www.spf.boun.edu.tr/img/1439796553_turkiyede_esitsizlikler_spf.pdf

Boz, Ahmet. (2014). Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri, T.C. Polis Akademisi, Güvenlik Bilimleri Enstitüsü, Güvenlik Stratejileri ve Yönetimi Anabilim Dalı, Yüksek Lisans Tezi

Bozkurt, Paşa. (2013). Denetim Kavramı ve Denetim Anlayışındaki Gelişmeler, Kamu İç Denetçilerinin Performansının Belirlenmesine Etkisi Açısından Dış Değerlendirme, Türkiye ve Ortadoğu Amme İdaresi Enstitüsü Kamu Yönetimi Yüksek Lisans Programı (İ.Ö.) Dönem Projesi

- Bük, Alaatin. (2015). Elektronik ortamda saklanan kişisel verilerin elde edilmesi/değiřtirilmesi suretiyle iřlenen suçların Ceza Hukuku aısından deęerlendirilmesi. Polis Akademisi Bařkanlıęı, Gvenlik Bilimleri Enstits, Gvenlik Stratejileri ve Ynetimi Anabilim Dalı. Doktora Tezi
- Clarke, Roger. (2000). Beyond the OECD Guidelines: Privacy Protection for the 21st Century, Rwww.rogerclarke.com/DV/PP21C.html
- ComputerWorld. (2016). Kiřisel Verilerin Korunması Neden nemli?, <http://www.computerworld.com.tr/haberler/kisisel-verilerin-korunmasi-neden-onemli/>
- avuřoęlu, Hakan. (2016). Kiřisel Verilerin Korunması Kanunu Tasarısı Mnasebetiyle, AKP adına TBMM Genel Kurul Konuřması, https://www.tbmm.gov.tr/develop/owa/genel_kurul.cl_getir?pEid=46497
- ekin, Mesut Serdar. (2016). Tehlike Sorumluluęu (6098 sayılı Trk Borlar Kanunu Madde 71 erevesinde). On iki levha yayıncılık.
- elik, Yeřim. 2017. “zel Hayatın Gizlilięinin Yansıması Olarak Kiřisel Verilerin Korunması ve Bu Baęlamda Unutulma Hakkı,” TAAD, Yıl:8, Sayı:32. (391-410)
- okmutlu, Metin. (2014). Trk Ceza Hukukunda Kiřisel Verilerin Korunması, T.C. Kocaeli niversitesi Sosyal Bilimler Enstits Kamu Hukuku Anabilim Dalı, Yksek Lisans Tezi
- Demirel, Demokaan. (2015). Yasal erevede Bilgi Edinme Hakkı: Kanada ve Trkiye rneęi, Bartın niversitesi İ.İ.B.F. Dergisi, Cilt: 6, Sayı: 11. (45- 161).
- Dinki, Fatih. (2014). Kiřisel Verilerin Korunmasında Uluslararası Dzenlemeler ve Trkiye rneęi, T.C. On dokuz Mayıs niversitesi, Sosyal Bilimler Enstits, Kamu Hukuku Anabilim Dalı, Yksek Lisans Tezi

Ertan, Özgökçe Bedia. (2016). Kişisel Verilerin Korunması Kanunu Tasarısı Münasebetiyle HDP adına TBMM Genel Kurul Konuşması, https://www.tbmm.gov.tr/develop/owa/genel_kurul.cl_getir?pEid=44479

Henkoğlu, Türkey. (2015). Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi, T.C. Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Bilgi ve Belge Yönetimi Anabilim Dalı, Doktora Tezi

İmam Taşçier (2016), Kişisel Verilerin Korunması Kanunu Tasarısı Münasebetiyle, HDP adına TBMM Genel Kurul Konuşması, https://www.tbmm.gov.tr/develop/owa/genel_kurul.cl_getir?pEid=46432

İmre, Zahit. (1974). “Şahsiyet Haklarından Şahsın Özel Hayatının ve Gizliliklerin Korunmasına İlişkin Meseleler,” İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: 39, Sayı:1 – 4. (147-168)

Karabulut, Ramazan. (2014). Kişisel Verilerin Korunması ve Kolluk Hizmetleri, Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi

Kaya, Cemil. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İÜHFMD Dergisi, Cilt: LXIX, Sayı: 1-2. (317-334)

Ketizmen, Muammer ve Ülküderner, Çağlar. (2007). E-Devlet Uygulamalarında Kişisel Verilerin Korun (ma)ması, XII. “Türkiye’de İnternet” Konferansı 8-10 Kasım 2007,

Kılınç, Doğan. (2012). “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması,” AÜHFMD, Cilt: 61, Sayı: 3. (1089-1169)

Kıraç, Şehriban. (2015). Kişisel Veriler AKP’ye Emanet, 20.01.2015 Tarihli Cumhuriyet Gazetesi Haberi,

http://www.cumhuriyet.com.tr/haber/ekonomi/191029/Kisisel_veriler_AKP_ye_emanet.html

Korkmaz, Ali. (2014). İnsan Hakları Bağlamında Özel Hayatın Gizliliği Ve Korunması, KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi 16 (Özel Sayı I). (99-103)

Korkmaz, İbrahim. (2016). “Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme,” TBB Dergisi, Cilt: 124. (81-152).

Kudat, Aydın. (2014). “Hak ve Hukuk Kavramları Üzerinde Bir Değerlendirme,” Adam Akademi Dergisi, Cilt: 4, Sayı: 2. (87-106).

Kuşkonmaz, Mendos, Elif. (2013). Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, T.C. İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi

Küpelı, Ceren. (2016). Şiddet Mağduru Kadınların Unutulma Hakkı, MÜHF – HAD, Cilt: 22, Sayı: 1. (229-238).

Kürkçü, Ertuğrul. (2015). “Kişisel Verilerin Korunması Yasa Tasarısı” kişisel sırları “devletleştiriyor”, <http://www.ertugrulkurkcu.org/tbmm-de-ertugrul-kurkcu/kisisel-veriler-tasarisiyla-kisisel-sirlar-devletlestiriliyor/>

Küzeci, Elif. (2014). “Anayasal Bir Hak: Kişisel Verilerin Korunması”, İdarecinin Sesi Dergisi, Ekim-Kasım-Aralık Sayısı. (11-16).

KVKK- Kişisel Verileri Koruma Kurumu. (2017). Kişisel Verilerin Korunması Kanunu ve Uygulaması, <http://www.kvkk.gov.tr/yayinlar/KIŞISEL%20VERİLERİN%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf>

KVKK, (2017), <https://www.kvkk.gov.tr/yayinlar/ANAYASAL%20BİR%20HAK%20OLARAK%20KIŞISEL%20VERİLERİN%20KORUNMASINI%20İSTEME%20HAKKI.pdf>

KVKK, (2018),
<https://www.kvkk.gov.tr/yayinlar/KIŞİSEL%20VERİLERİ%20KORUMA%20KURULU'NUN%20YAPISI%20VE%20GÖREVLERİ.pdf>

Mehmet Gökdağ, (2016), Kişisel Verilerin Korunması Kanunu Tasarısı Münasebetiyle, CHP adına TBMM Genel Kurul Konuşması,
https://www.tbmm.gov.tr/develop/owa/genel_kurul.cl_getir?pEid=46496

Nalbantoğlu, Lerzan; Özkaya, Asilhan. (2016).
<https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/legal/KisiselVeriler.pdf>

Necati Yılmaz, (2016), Kişisel Verilerin Korunması Kanunu Tasarısı Münasebetiyle, CHP adına TBMM Genel Kurul Konuşması,
https://www.tbmm.gov.tr/develop/owa/genel_kurul.cl_getir?pEid=46572

Oğuz, Habip. (2015). “Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum,” Çağ Üniversitesi Elektronik Ticaret Hukuku Sempozyumu

Ok, İsmail. (2016). Kişisel Verilerin Korunması Kanunu Tasarısı Münasebetiyle MHP adına TBMM Genel Kurul Konuşması,
https://www.tbmm.gov.tr/develop/owa/genel_kurul.cl_getir?pEid=46570

Ömer Süha Aldan, (2016), Kişisel Verilerin Korunması Kanunu Tasarısı Münasebetiyle, CHP adına TBMM Genel Kurul Konuşması,
https://www.tbmm.gov.tr/develop/owa/genel_kurul.cl_getir?pEid=46518

Özbilgin, İ. Gökhan. (2011). Bilgi Teknolojilerinde Gelişmeler, Bilgi Güvenliği ve Bilişim Hukuku (Aracı Kurumlar Açısından), https://www.tspb.org.tr/wp-content/uploads/2015/06/ETM_seminer_bilgi_teknolojileri_21012011.pdf

Savcı, Bahri. (1980). Yaşam Hakkı. Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, Yayın No. 449.

Schwartz, Paul M. (2004). Property, Privacy, and Personal Data, Berkeley Law
Berkeley Law Scholarship Repository,
<https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3150&context=facpubs>

Solove, J. Daniel. (2004). The Digital Person: Technology and Privacy in the
Information Age, New York University Press.

Sönmez, Barbaros. (2016). Gözetim Toplumunun Günümüz Tüketim Dinamikleri
Bağlamında Yorumlanması, Selçuk İletişim Dergisi, Cilt: 9, Sayı 2, (262-284).

Şanbaş, Pınar. (2013). Bilgi teknolojileri dış kaynak alımında (Outsourcing) kişisel
verilerin korunması ve gizlilik sözleşmeleri. İstanbul Bilgi Üniversitesi, Sosyal
Bilimler Enstitüsü, Hukuk Anabilim Dalı. Yüksek Lisans Tezi.

Şahin, Osman. (2011). Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi,
Saklanması ve Gizliliğin Korunması, Bilgi Teknolojileri ve İletişim Kurumu,
Bilişim Uzmanlığı Tezi.

Şimşek, Oğuz. (2008). Anayasa Hukukunda Kişisel Verilerin Korunması , Beta
Yayıncılık.

T24, 03.05.2016 Tarihli Haber, <http://t24.com.tr/haber/chp-kisisel-verilerin-korunmasi-yasasinin-iptali-icin-aymye-basvuracak,343567>

TBMM Genel Kurul Tutanakları,
https://www.tbmm.gov.tr/develop/owa/tutanak_g_sd.birlesim_baslangic?P4=20633&P5=B&page1=2&page2=2

TBMM Kanun Teklifi Metni,
https://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_no=82348

Temiz, Özgür. (2014). “Türk Hukukunda Bir Temel Hak Olarak Sağlık Hakkı,”
Ankara Üniversitesi SBF Dergisi, Cilt 69, No. 1. (165 – 188).

- Turunç Hukuk. (2016). Kişisel Verilerin Korunması Hakkında Kanun. [http://www.turunc.av.tr/publications/alertmemos/Kisisel-Verilerin-Korunmasi-Hakkinda-Kanun-\(TURUNC-08-Nisan-2016\).pdf](http://www.turunc.av.tr/publications/alertmemos/Kisisel-Verilerin-Korunmasi-Hakkinda-Kanun-(TURUNC-08-Nisan-2016).pdf)
- Uncular, Selen. (2012). İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, T.C. Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, Yüksek Lisans Tezi
- Uygun, Murat. (2010). Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi ışığında kişisel verilerin korunması. Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı. Avrupa Birliği Hukuku Bilim Dalı. Yüksek Lisans Tezi.
- Vural, Yılmaz ve Sağıroğlu, Şeref. (2010). “Veri tabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri,” Politeknik Dergisi, Cilt: 13, Sayı:2, (71-81)
- Yılmaz, Malik. (2009). “Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi,” Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi, Cilt: 49, Sayı: 1. (95-118)
- Yüksel, Saadet. (2012). Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale. Beta Yayınları
- Zeynel Emre, (2016), Kişisel Verilerin Korunması Kanunu Tasarısı Münasebetiyle, CHP adına TBMM Genel Kurul Konuşması, https://www.tbmm.gov.tr/develop/owa/genel_kurul.cl_getir?pEid=44484
- Zins, Chaim. (2014). What is the Meaning of “Data”, “Information” and “Knowledge”?, <https://pdfs.semanticscholar.org/d04c/f02cf43bfb27245e2ec8b3c0b0f48837da.pdf>

ÖZGEÇMİŞ

Kişisel Bilgiler:

Adı Soyadı : Nur Halet Avcıoğlu

Doğum Yeri ve Tarihi : Konya -22/03/1992

Eğitim Durumu:

Lisans Öğrenimi :Kto Karatay Üniversitesi Hukuk Fakültesi

Yüksek Lisans Öğrenimi :Kamu Hukuku (Tezli)

Bildiği Yabancı diller : İngilizce

İş Deneyimi:

Staj : Tanrıkulu Hukuk Bürosu (1 yıl)

Çalıştığı Kurumlar : Ergün& Avcıoğlu Hukuk ve Danışmanlık

İletişim :

E-posta Adresi :avcioglunur@gmail.com

Tarih :23/07/2018