



**KİŞİSEL VERİLERİN KORUNMASI VE
6698 SAYILI KANUN**

Kerim KILIÇ

**Yüksek Lisans Tezi
Kamu Hukuku Anabilim Dalı
Yrd. Doç. Dr. Özgür TEMİZ
2016
Her Hakkı Saklıdır**

T.C
ATATÜRK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

Kerim KILIÇ

KİŞİSEL VERİLERİN KORUNMASI VE 6698 SAYILI KANUN

YÜKSEK LİSANS TEZİ

TEZ YÖNETİCİSİ
Yrd. Doç. Dr. Özgür TEMİZ

ERZURUM - 2016



T.C.
ATATÜRK ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ



TEZ BEYAN FORMU

05.08.2016

SOSYAL BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

BİLDİRİM

Atatürk Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğine göre hazırlamış olduğum "Kızılca... Karırm... Karırm... ve 6698 Sayılı Kanun..." adlı tezin/raporun tamamen kendi çalışmam olduğunu ve her alıntıya kaynak gösterdiğimi taahhüt eder, tezimin/raporumun kağıt ve elektronik kopyalarının Atatürk Üniversitesi Sosyal Bilimler Enstitüsü arşivlerinde aşağıda belirttiğim koşullarda saklanmasına izin verdiğimi onaylarım:

Lisansüstü Eğitim-Öğretim yönetmeliğinin ilgili maddeleri uyarınca gereğinin yapılmasını arz ederim.

☐ Tezimin/Raporumun tamamı her yerden erişime açılabilir.

☐ Tezim/Raporum sadece Atatürk Üniversitesi yerleşkelerinden erişime açılabilir.

☒ Tezimin/Raporumun 3 yıl süreyle erişime açılmasını istemiyorum. Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin/raporumun tamamı her yerden erişime açılabilir.

05.08.2016

[Tarih ve İmza]

[Öğrencinin Adı Soyadı]

Kerim KILIÇ



T.C.
ATATÜRK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



TEZ KABUL TUTANAĞI

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Yrd. Doç. Dr. Özgür TEMİZ danışmanlığında, Kerim KILIÇ tarafından hazırlanan bu çalışma 05/08/2016 tarihinde aşağıdaki jüri tarafından, KAMU HUKUKU Anabilim Dalı'nda Yüksek Lisans Tezi olarak kabul edilmiştir.

Başkan : Doç. Dr. Bülent ALGAN

İmza:

Jüri Üyesi : Yrd. Doç. Dr. Cem ŞENOL

İmza:

Jüri Üyesi : Yrd. Doç. Dr. Özgür TEMİZ

İmza:

Yukarıdaki imzalar adı geçen öğretim üyelerine aittir. / /

Prof. Dr. Mustafa YILDIRIM

Enstitü Müdürü

F-85/00/22.02.2012

İÇİNDEKİLER

ÖZET.....	V
ABSTRACT	VI
KISALTMALAR DİZİNİ	VII
GİRİŞ	1

BİRİNCİ BÖLÜM

KİŞİSEL VERİLER ve KİŞİSEL VERİLERİN İŞLENMESİ

1.1. KİŞİSEL VERİLER	3
1.1.1. Tanım ve Kapsam.....	3
1.1.2. Kişisel Veri Çeşitleri	7
1.1.2.1. Genel Olarak.....	7
1.1.2.2. Hassas Veriler.....	8
1.1.2.3. Hassas Olmayan Veriler	10
1.2. KİŞİSEL VERİLERİN İŞLENMESİ.....	10
1.2.1. Genel Olarak.....	10
1.2.1.1. Verilerin Toplanması.....	12
1.2.1.2. Verilerin Kaydedilmesi.....	12
1.2.1.3. Verilerin Değiştirilmesi	13
1.2.1.4. Verilerin Aktarılması	13
1.2.1.5. Verilerin Kullanılmasının Engellenmesi	14
1.2.1.6. Verilerin Kullanılması	16
1.2.1.7. Verilerin Silinmesi.....	16
1.2.2. Hassas Verilerin İşlenmesi	18
1.2.3. Hassas Verilerin İşlenebileceği (İstisnai) Durumlar	18
1.2.3.1. İlgilinin Rızası ile Hassas Verilerin İşlenmesi	19
1.2.3.2. İş Kanunları Hükümlerine Göre Hassas Verilerin İşlenmesi	20
1.2.3.3. Hayati Menfaatlerin Korunması Amacıyla Hassas Verilerin İşlenmesi.....	21
1.2.3.4. Kamuya Yararlı Kurum ve Kuruluşlarca Hassas Verilerin İşlenmesi.....	22
1.2.3.5. İlgili Kişi Tarafından Kamuya Açıklanan Hassas Verilerin İşlenmesi	22
1.2.3.6. Yargılama Faaliyetleri Nedeni ile Hassas Verilerin İşlenmesi.....	23
1.2.3.7. Tıbbi Gerekliklik Açısından Hassas Verilerin İşlenmesi	24

1.2.3.8. Kamu Yararı Nedeniyle Hassas Verilerin İşlenmesi	24
1.2.3.9. Suçlar, Hükümler ve Güvenlik Tedbirlerine İlişkin Hassas Verilerin İşlenmesi	26
1.2.4. Hassas Olmayan Verilerin İşlenmesi	26
1.2.4.1. Genel olarak.....	26
1.2.4.2. Kişisel Verilerin İşlenmesine Dair İlkeler	27
1.2.4.2.1. Hukuka ve Dürüstlük Kuralına Uygun İşlenmesi İlkesi	27
1.2.4.2.2. Amaca Uygun İşlenmesi İlkesi	28
1.2.4.2.3. Doğruluk İlkesi	29
1.2.4.2.4. Gerekli Olan Süreden Daha Uzun Tutulamaması İlkesi.....	30
1.2.4.3. Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri	31
1.2.4.3.1. Rıza	32
1.2.4.3.2. Sözleşmenin İfası ve Sözleşme Öncesi Önlem Alınması	33
1.2.4.3.3. Kanuni Yükümlülüklerin Yerine Getirilmesi	33
1.2.4.3.4. İlgili Kişinin Hayati Menfaatlerinin Korunması.....	34
1.2.4.3.5. Kamu Yararı veya Kamu Görevinin Yerine Getirilmesi	34
1.2.4.3.6. Haklı Çıkarların Korunması.....	35
1.2.4.3.7. Herkesçe Bilinen Verilerin İşlenmesi	36
1.2.4.3.8. Verilerin Anonim Hale Getirilerek İşlenmesi.....	37

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN SAKLANMASI, GÜVENLİĞİ ve KORUNMASI

2.1. KİŞİSEL VERİLERİN SAKLANMASI ve VERİLERİN GÜVENLİĞİ	39
2.1.1. Kişisel Verilerin Saklanması	39
2.1.1.1. Kişisel Verilerin Saklanma Süresi	40
2.1.1.2. Kişisel Verilerin Daha Sonra İşlenme İhtimali ile Saklanıp Saklanamayacağı Meselesi	41
2.1.2. Kişisel Verilerin Güvenliği	43
2.2. KİŞİSEL VERİLERİN KORUNMASI.....	47
2.2.1. Tarihsel Gelişim ve Verilerin Korunması İhtiyacı	47
2.2.2. Kişisel Verilerin Korunması Alanındaki Uluslararası Düzenlemeler	49

2.2.2.1. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Bünyesindeki Durum.....	49
2.2.2.2. Avrupa Konseyi Bünyesindeki Durum.....	51
2.2.2.3. Birleşmiş Milletler Bünyesindeki Durum.....	53
2.2.2.4. Avrupa Birliği Bünyesindeki Durum	54
2.2.3. Türk Hukukunda Kişisel Verilerin Korunması	58
2.2.3.1. 6698 sayılı KVKK'dan Önceki Durum	58
2.2.3.1.1. 1982 Anayasası	59
2.2.3.1.2. 5237 sayılı Türk Ceza Kanunu	69
2.2.3.1.3. 5271 sayılı Ceza Muhakemesi Kanunu.....	72
2.2.3.2. 6698 sayılı Kişisel Verilerin Korunması Kanunu.....	73
2.2.3.2.1. Kişisel Verilerin Kanun Yoluyla Korunmasına Duyulan İhtiyaç	73
2.2.3.2.1.1. Kişisel Verilerin Esasını Oluşturan Hususların Bağımsız Bir Kanun ile Düzenlenmesi Açısından	74
2.2.3.2.1.2. Uluslararası Üyeliklerin Gereklerinin Yerine Getirilmesi Açısından.....	74
2.2.3.2.2. 6698 sayılı Kişisel Verilerin Korunması Kanun Hükümleri.....	77
2.2.3.2.2.1. Kanun'un Sistematiik Görünümü.....	77
2.2.3.2.2.2. Kanun Hükümleri.....	77

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİ SAHİBİNİN AYDINLATILMASI VE HAKLARI

3.1. AYDINLATMA YÜKÜMLÜLÜĞÜ	89
3.1.1. Aydınlatma Yükümlülüğünün Önemi	90
3.1.2. Aydınlatma Yükümlülüğünün Gerekliliği.....	91
3.1.3. Kavramsal Tartışma	93
3.1.4. Aydınlatma Yükümlülüğünün Yerine Getirilmesi	95
3.2. KİŞİSEL VERİ SAHİBİNİN 6698 SAYILI KANUN KAPSAMINDA YER ALAN HAKLARI	96
3.2.1. Bilgi Edinme Hakkı.....	96
3.2.2. Verilerin Düzeltilmesini, Silinmesini ve Yok Edilmesini İsteme Hakkı	98
3.2.3. İtiraz Hakkı.....	100

3.2.4. Zararın Giderilmesi Hakkı.....	102
3.2.4.1. Kanuni Düzenleme	102
3.2.4.2. Genel Hükümlere Göre Zararın Giderilmesi	102
3.2.4.2.1. 6098 sayılı Borçlar Kanunu'na Göre Zararın Giderilmesi.....	103
3.2.4.2.1.1. Maddi Tazminat Davası	103
3.2.4.2.1.2. Manevi Tazminat Davası	104
3.2.4.2.2. Tam Yargı Davası ile Zararın Giderilmesi.....	105
3.3. KİŞİSEL VERİ SAHİBİNİN DİĞER HAKLARI	106
3.3.1. Unutulma Hakkı	106
3.3.2. 4982 sayılı Bilgi Edinme Hakkı Kanunu Kapsamında Bilgi Edinme Hakkı ..	110
3.3.2.1. Genel Olarak Bilgi Edinme Hakkı.....	110
3.3.2.2. Kişisel Verilerin Korunması İle İlişkisi.....	112
SONUÇ.....	114
KAYNAKÇA	117
ÖZGEÇMİŞ.....	122

ÖZET**YÜKSEK LİSANS TEZİ****KİŞİSEL VERİLERİN KORUNMASI VE 6698 SAYILI KANUN****Kerim KILIÇ****Danışman: Yrd. Doç. Dr. Özgür TEMİZ****2016, 122 Sayfa****Jüri: Doç. Dr. Bülent ALGAN****Yrd. Doç. Dr. Cem ŞENOL****Yrd. Doç. Dr. Özgür TEMİZ**

Son dönemlerde, bireylerin özgürlük alanları ile ters orantılı şekilde gelişen ve ilerleyen teknoloji sayesinde, birey ve bireyin sahip olduğu temel hak ve özgürlüklere dair tehdit ve tehlikeler de artmaya devam etmektedir. Bireye yönelmiş olan ve tezimizin konusunu oluşturan bu tehlikelerden birisi olarak kişisel verilerin korunması ve bu bağlamda kişisel verilerin ihlali şüphesiz ki teknoloji, küreselleşme, sanal âlem gibi olgularla bağlantılıdır. Zira kişisel verilerin, özellikle bilişim sistemleri aracılığı ile sınır tanımaksızın hareket edebilmesi, bu verilerin sanal dünyada kayıt altına alınarak elden ele dolaşabilmesi, birey açısından çok büyük riskleri de beraberinde getirmiştir. Bu tehditlere ve tehlikelere karşı bireyin korunması için yasal zeminlerin sağlam şekilde oluşturulması bireyi ve de kişi temel hak ve özgürlüklerinin korunması için oldukça önemlidir.

Avrupa Birliği'ne katılım ve uyum sürecinde Türkiye, sahip olması gereken yasal düzenlemelerden birisi olarak Kişisel Verilerin Korunması Kanunu'nu daha çok yeni kabul etmiş ve bu alanda önemli bir eksikliği gidermiş görünmektedir. Anayasada yer alan hükümlerin yasal düzenleme ile genişletilerek bu alana ait kavram ve ilkelerin belirlenmesi, karşılaşılabilecek olan ihtilafların giderilmesinde çözüm odaklı olunmasında önemli yer tutacaktır.

Bu bağlamda çalışmamızın birinci bölümünde, kişisel verilerin korunması alanında kullanılmakta olan temel kavramlar ve kişisel verilerin işlenmesinde geçerli olan ilkeler üzerinde durulmuştur.

İkinci bölümde ise kişisel verilerin saklanması, güvenliği ve korunması hususları açıklanmaya çalışılmıştır. Bu amaçla kişisel verilerin korunması alanının gelişimi, uluslararası ve ulusal düzeyde bu alanda yaşanan gelişmeler ve yapılan düzenlemeler, hukuki boyutta ele alınmıştır.

Son olarak üçüncü bölümde de, kişisel verileri, devlet ya da üçüncü kişilerin elinde bulunmak suretiyle sürekli olarak bir tehlike, tehdit ve hak ihlali gibi durumlarla karşı karşıya kalan veri sahibinin sahip olduğu ve olması gereken haklar incelenmeye çalışılmıştır.

Anahtar Kelimeler: Kişisel Veri, Veri Koruma, Veri İşleme, İlgili, İlgilinin Hakları, Verilerin Güvenliği

ABSTRACT**MASTER THESIS****PROTECTION OF PERSONAL DATA AND CODE NUMBERED 6698****Kerim KILIÇ****Advisor: Assist. Prof. Dr. Özgür TEMİZ****2016, Page: 122****Jury: Assoc. Prof. Dr. Bülent ALGAN****Assist. Prof. Dr. Cem ŞENOL****Assist. Prof. Dr. Özgür TEMİZ**

Recently, by means of technology which improves and advances inversely proportional to individuals' area of freedom, threats and dangers about individuals and fundamental rights and freedoms of individuals continue to rise. Personal data protection and, in this regard, violation of personal data as one of these threats that is related to individual and that constitutes the subject of this thesis are undoubtedly connected with some facts such as technology, globalization, and cyber world. For this reason, movement of personal data particularly through information systems without boundaries, recording of these data in the cyber world and changing hands many times leads to great risks for individuals. It is very important to form a solid legal basis to protect individuals against these threats and hazards with regards to protecting individuals and fundamental rights and freedoms.

In the process of participation and integration to the European Union, Turkey has very recently enacted the Law of Personal Data Protection (Privacy Act) as one of the legal regulations that it should have, and seems to fill an important gap in this field. Determination of the concepts and principles belonging to this field by enlarging through a legal regulation of constitutional provisions will take an important place to be solution oriented in eliminating the conflicts to be faced.

In this regard, in the first part of the study, basic concepts used in the field of personal data protection and the principles that are valid in processing of personal data are discoursed.

In the second part, it is tried to be explained the issues of storage, security and protection of personal data. For this purpose, the improvement of personal data protection, the developments and arrangements in this field at national and international scale are discussed at legal dimension.

Lastly, in the third part, the rights that a data owner, who is continuously faced with cases such as danger, threat and violation of rights by means of that the owner's data is in the hands of third parties, has and should have are tried to be analyzed.

Key Words: Personal Data, Data Protection, Data Processing, Relative Person, Rights Of Relative Person, Data Security

KISALTMALAR DİZİNİ

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AK	: Avrupa Konseyi
AÜHFD	: Ankara Üniversitesi Hukuk Fakültesi Dergisi
AYMK	: Anayasa Mahkemesi Kararı
b.	: bent
BDSG	: Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz)
BEHK	: Bilgi Edinme Hakkı Kanunu
Bkz.	: Bakınız
C.	: Cilt
CMK	: Ceza Muhakemesi Kanunu
DDK	: Devlet Denetleme Kurumu
DMK	: Devlet Memurları Kanunu
DSG	: İsviçre Veri Koruma Kanunu (Bundesgesetz über den Datenschutz)
E.	: Esas
Ed.	: Editör
EÜHFD	: Erzincan Üniversitesi Hukuk Fakültesi Dergisi
E.T.	: Erişim Tarihi
f.	: fıkra
İYUK	: İdari Yargılama Usul Kanunu
K.T.	: Karar Tarihi
KVKK	: Kişisel Verilerin Korunması Kanunu
KVKKT	: Kişisel Verilerin Korunması Kanunu Tasarısı
m.	: madde
OECD	: Ekonomik Kalkınma ve İşbirliği Örgütü
R.G.	: Resmi Gazete
S.	: Sayı
s.	: sayfa
TBB	: Türkiye Barolar Birliği

TBK	: Türk Borçlar Kanunu
TBMM	: Türkiye Büyük Millet Meclisi
T.C.	: Türkiye Cumhuriyeti
TMK	: Türk Medeni Kanunu
TTK	: Türk Ticaret Kanunu
vb.	: ve bunun gibi
vd.	: ve devamı
ZGB	: İsviçre Medeni Kanunu (Zivilgesetzbuch)



GİRİŞ

Bilim ve teknoloji alanındaki baş döndürücü ilerleme ile birlikte, istenilen ya da ihtiyaç duyulan bilgiye ulaşma günümüzde zor olmayan bir durum haline gelmiştir. Şüphesiz ki yaşanan hızlı gelişmeler ve bilgiye bu denli hızlı ulaşma, insan hayatını kolaylaştırması bakımından olumlu bir gelişme olarak görülebilir. Bu olumlu durumun gerçekleşebilmesi, bireye ait bilgilerin yetkili kişiler elinde, usulüne uygun olarak tutuluyor olmasına bağlıdır. Gerçekten de bilgi toplumunun meydana çıkması ile birlikte özellikle devletin, kamu hizmetlerini hızlı, kolay ve güvenilir bir biçimde yerine getirmesi için bireylere ait doğru bilgilere ulaşması elzemdir. Eğitim, sağlık, nüfus hizmetleri, vergilendirme, kamu güvenliği gibi alanlarda devlet, bireylere ait kişisel verilere fazlasıyla ihtiyaç duymaktadır. Fakat bu amaçla edinilen bilgilerin depolanması, kaydedilmesi, işlenmesi gibi faaliyetler, hem bu verileri elinde bulunduran devlet hem de veri sahipleri açısından birtakım riskleri de bünyesinde barındırmaktadır. Şöyle ki bu verilerin güvenliğinin sağlanamaması veya yetkisiz kişilerin eline geçmesi ya da gereği dışında kullanılması halinde ilgili kişiler açısından, başta özel hayatın gizliliği ve korunması ile kişisel verilerin korunması hakları olmak üzere birtakım anayasal hakların tehlike altında olmasına ve de özgürlüklerin ihlallerine yol açabilecektir. Devlet açısından ise elde bulundurulan kişisel verilerin güvenliğinin sağlanması ve yetkisiz ellere geçme tehlikesi, riskli durumlardır. Bu durum da bilim ve teknoloji alanında yaşanan hızlı gelişmelerin olumsuz yanı olarak görülebilir.

Bireyin kişisel verilerinin korunması iki farklı anlamda değerlendirilebilir. İlk olarak doğrudan kişisel verilerin kendisinin korunması, diğer bir ifadeyle veri güvenliğinin sağlanmasıdır. Bu durumda kişisel verileri yetkili olarak elinde bulunduranların, bu verilere yetkisiz şekilde ulaşmak isteyenlere engel olarak verilerin güvenliğinin sağlanması bireyler açısından hayati öneme sahiptir. İkinci ve esas olarak ise kişisel verilerin korunması ile bireyin kişi temel hak ve özgürlüklerinin korunmasının sağlanması amaçlanmaktadır. Bu nedenle de kişisel verilerin toplanması, kaydedilmesi, işlenmesi, transferi gibi işlemlerde usul ve esasların hukuki düzenlemelerle güvence altına alınmak suretiyle bireyin korunmasının gerçekleştirilmesinin sağlanması gerekmektedir.

Temel hak ve özgürlüklerin, yaşanan gelişmeler sonucunda ihlal edilebilirliğinin kolaylaşmasının, aynı zamanda bu temel hak ve özgürlüklerin önemini de arttırdığı aşikârdır. Bu çerçevede ilgililerin, kişisel verilerinin korunması kapsamında sahip oldukları haklarının neler olduklarının, hakların kapsamlarının ve bu hakların nasıl kullanılacağına bilinmesi, gerçek anlamda veri korumanın gerçekleşmesi ya da kâğıt üstünde kalmaması için önem arz etmektedir.



BİRİNCİ BÖLÜM

KİŞİSEL VERİLER ve KİŞİSEL VERİLERİN İŞLENMESİ

1.1. KİŞİSEL VERİLER

Kişisel veri kavramı, nitelik olarak bir bilgi olmakla birlikte, kavramın son dönemlerde önemli bir şekilde gündeme gelmesi, özellikle de kişi hak ve özgürlüklerinin korunması bağlamında önem arz etmesi nedenleri ile içeriğinin ve sınırlarının belirlenmesi hem kişi hak ve özgürlüklerinin korunması hem de bu anlamda ortaya çıkacak ihtilafların giderilmesi açısından bir gereklilik olarak karşımıza çıkmaktadır.

1.1.1. Tanım ve Kapsam

Kişisel verilere dair hem doktrinde hem de mevzuatta yapılmış tanımlara rastlamak mümkündür. OECD'nin 1980 tarihli ilkelerin 1/b¹, 108 sayılı Avrupa Konseyi Sözleşmesi 2/a² ve 95/46/AT sayılı (29 Eylül 2003 tarihli Konsey ve Avrupa Parlamentosunun 1882/2003 sayılı yönetmeliği ile değişik) AB Konseyi ve Avrupa Parlamentosu Direktifi 2/a³ maddeleri kişisel verilere dair bu alanda yapılmış ilk tanımlamalardır. OECD'nin 1980'de yaptığı tanım “ *kişisel veri, belirli veya belirlenebilir bir kişiye ait herhangi bilgi anlamına gelir (ilgili kişi.)*” Avrupa Konseyi Sözleşmesi'nde kişisel nitelikteki veriler “*kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade eder (ilgili kişi).* 95/46/AT sayılı Direktifte de kişisel veri “*fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye (veri öznesi) ilişkin herhangi bir bilgiyi kastedecektir.*” şeklinde tanımlanmıştır. Ülkemizde 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)

¹ OECD Rehber İlkeler için bkz, Erişim Tarihi: 05.01.2014
<http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>.

² Avrupa Konseyi 108 nolu Sözleşmenin tam metni için bkz. Erişim Tarihi: 05.01.2014,
http://www.avrupakonseyi.org.tr/antlasma/aas_108_p.htm.

³ 95/46/AT sayılı Direktif için bkz. Erişim Tarihi: 05.01.20
http://www.i-hop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf.

m. 3/ d⁴ ‘ de “*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.*”, Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik m. 3⁵ ‘ te “ *Kişisel bilgiler, veriler: Tanımlanmış veya doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgiyi ifade eder.*” olmak üzere kişisel veri tanımlarına yer verilmiştir. İsviçre Veri Koruma Kanunu (Bundesgesetz über den Datenschutz / DSG) üçüncü maddesinin (a) bendinde kişisel veriler “ *Belirli ya da belirlenebilir bir kişiye ilişkin olan tüm bilgiler*” olarak tanımlanmıştır. Bu kavram Federal Alman Veri Koruma Kanunu (Bundesdatenschutzgesetz / BDSG) üçüncü paragrafının birinci fıkrasında ise “ *Belirli ya da belirlenebilir bir gerçek kişinin (ilgilinin) şahsi ya da nesnel ilişkileri hakkındaki münferit bilgiler*” şeklinde tanımlanmıştır.

Yukarıda yapılan açıklamalar doğrultusunda kişisel veriler, kimliği belirli bir gerçek kişiye ait olan ya da bir gerçek kişinin belirlenmesine yardımcı olan her türlü bilgiler şeklinde tanımlanabilir. Bu anlamda kişinin fiziksel özellikleri, parmak izi, resmi, görüntü kaydı, öğrenim durumu, kimlik bilgileri, etnik kökeni, mesleği, dini inancı, banka hesap bilgileri, kullandığı bilgisayarın IP adresi⁶ gibi durumlar kişisel veri olarak nitelendirilebilir.

Ulusal ve uluslararası mevzuatta yapılan tanımlar bir birine benzer niteliktedirler. 22.04.2008 tarihli Kişisel Verilerin Korunması Kanun Tasarısı (KVKKKT), kişi yönünden tüzel kişilere ait verileri de koruma kapsamına dâhil etmiş olmasından dolayı, uluslararası düzenlemelere göre daha geniş kapsamlı nitelikteydi. Ancak 26.12.2014 tarihli KVKKKT ve 6698 sayılı KVKK, tüzel kişi ibaresine kişisel veri tanımında yer vermeyerek uluslararası düzenlemelerdeki tanımlarla örtüşür bir tanıma dönmüştür. OECD Rehber İlkeler, 108 nolu Avrupa Sözleşmesi, 95/46/AT sayılı Direktif ve Federal Alman Veri Koruma Kanunu (BDSG) ilgili maddelerinde açıkça *gerçek kişi* kavramı

⁴ <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2016/04/20160407.htm&main=http://www.resmigazete.gov.tr/eskiler/2016/04/20160407.htm>, Erişim Tarihi: 09.01.2016.

⁵ http://www.tk.gov.tr/mevzuat/yonetmelikler/dosyalar/Kisisel_Bil_Yon_06_02_04.pdf, Erişim Tarihi: 05.01.2014.

⁶ Mustafa Topaloğlu, *Bilişim Hukuku*, Karahan Yayınevi, Adana 2005, 163

kullanılmıştır. Ancak OECD Rehber İlkeler m. 6'da tüzel kişileri koruma kapsamına dâhil etmek açısından üye ülkelere bir serbesti tanımaktadır. Aynı şekilde 95/46/AT sayılı Direktif'te de üye devlerin ulusal düzenlemelerinde tüzel kişileri kapsam dâhilinde düzenlemelerine her hangi bir engel yoktur.

İsviçre Veri Koruma Kanunu'nun (DSG) ikinci maddesinde kanunun uygulama alanı düzenlenmiştir. Buna göre bu kanun hükümlerinin, gerçek ve tüzel kişilerin verilerinin özel kişiler ya da devlet organları tarafından işlenmesi halinde uygulama alanı bulacağı hüküm altına alınmıştır. Bu hükümden anlaşılabileceği üzere İsviçre Veri Koruma Kanunu (DSG) gerçek kişiler yanında tüzel kişileri de kanunun kapsamında koruma altına almıştır. İsviçre Hukuku'nda hukuki anlamda gerçek kişi tüm insanlar olarak kabul edilmiş, her insanî varlık hukuk süjesi olarak tanınmıştır. Böylece her kişi haklara, borçlara ve yeteneklere sahip olmaktadır. İsviçre Medeni Kanunu (ZGB) m. 28 ve devamı maddeleri yanı sıra İsviçre Veri Koruma Kanunu (DSG) ile de bireylerin kişiliği korunmaktadır. Ancak DSG'nin koruması yalnızca yaşayan, hayatta olan kişilere yöneliktir. Yani İsviçre Hukuku ölümden sonra kişiliğin korunmasını tanımamaktadır⁷. İsviçre Hukuku'nda tüzel kişilere ilişkin genel hükümler ZGB m. 52-89 arasında düzenlenmiştir. Tüzel kişiler, gerçek kişilere kıyasla hukuk düzeninin yarattığı sùjelerdir. İsviçre Hukuku'nda tüzel kişiliği olmayan (kolektif şirket, adi komandit şirket gibi) topluluklar dahi veri koruma kanununun korumasında yararlanmakta, ancak adi şirket ve miras topluluğu bu koruma dışında bırakılmıştır⁸. Ancak İsviçre doktrinde şahıs şirketlerinin, adi şirkete göre kanunun koruması kapsamına alınmasının gerekçesinin tam olarak açıklanamadığı ifade edilmiştir. İsviçre kanun anlayışına göre tüzel kişiler, gerçek kişiler gibi haklar, borçlara ve yeteneklere ehildirler. Gerçek kişilerin insan olması sebebiyle sahip olduğu özellikleri istisna olmak üzere tüzel kişilere de uygulanabilen haklar açısından DSG'nin koruması kapsamında yer almaktadır. Ancak tüzel kişilerin bu Kanun kapsamında yer alması İsviçre doktrinde eleştirilmiş ve kanun koyucunun gerçekte tam da ikna edici olmayan nedenlerle tüzel kişilere gerçek kişiler gibi bir koruma sağladığı ileri sür÷lmüştür⁹.

⁷ Usr Maurer, Lambrou Blechta, Simon Kunz, (Editör: Maurer – Lambrou Blechta), *Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz*, 3. Auflage, Helbing Lichtenhahn Verlag, 2014 Basel, Art. 2 DSG, 66, N. 6

⁸ Maurer, Blechta, Kunz, 67, N. 8 (DSG Botschaft s. 438)

⁹ Maurer, Blechta, Kunz, 67, N. 7

Ayrıca 2002/58/AT sayılı Avrupa Parlamentosu ve Konseyi Direktifi'nde¹⁰, elektronik haberleşme sektöründe gerçek kişiler yanında tüzel kişilerin de veri sahibi olabileceği ifade edilmiştir¹¹. Ulusal mevzuatımızda 6698 sayılı KVKK'da yapılan tanıma rağmen Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik'te tüzel kişilere tanımda yer verilmiştir. Bu noktada tüzel kişilerin kapsam dâhilinde değerlendirilip değerlendirilmeyeceği hususuna değinmekte fayda olacağı kanaatindeyiz.

Veri korumaya ilişkin düzenlemelerin temelinde, kişi temel hak ve özgürlüklerinin ihlalinin önlenmesi düşüncesi yer almakta¹², özellikle de kişinin mahremiyetinin korunması ön planda tutulmaktadır. Bu bağlamda kişisel verilerin korunması hakkı ile insanın kişiliği ve özel hayatının korunması amaçlanmaktadır. Ayrıca bu hakkın insan onuru ile bağlantısı noktasında genel kişilik haklarından ayrılacağından gerek kamu hukuku gerekse özel hukuk tüzel kişilerinin verilerin korunması hakkının sahibi olamayacakları sonucuna varmak mümkündür¹³. Dolayısı ile de tüzel kişilerin veri korumaya ilişkin düzenlemelerin kapsamında düzenlenmemeleri doğaları gereğidir. Ancak tüzel kişiler üzerinden gerçek kişilere ulaşma, diğer bir anlatımla kimliği belirli veya belirlenebilir bir gerçek kişiye ait bilgiler edinebilme ihtimali her zaman göz önünde bulundurulmalıdır. Örneğin 6102 sayılı TTK m. 211 gereğince bir kolektif şirket ortağı ancak gerçek kişi olabilir. Yine m. 213 gereğince bir kolektif şirket sözleşmesine, ortakların kişisel veri niteliğini haiz adı, soyadı, yerleşim yeri ve vatandaşlığı gibi ilgili bilgileri yazılmak zorundadır. Dolayısıyla tüzel kişiye ait bu bilgilerden bir gerçek kişiyi belirli veya belirlenebilir kılacak bilgilere ulaşma imkânı söz konusu olacaktır¹⁴. Bu durumda tüzel kişilere ait verilerin de koruma kapsamına dâhil edilmesi yerinde olacağı düşüncesi yersiz olmayacaktır. Doktrinde tüzel kişilere ait verilerin KVKK kanunlaşmadan, kanun kapsamına alınmasının yerinde olmadığını savunan görüşler de vardır. Tüzel kişilerin, kapsam dışında bırakılmasının nedeni

¹⁰ 95/46/AT sayılı Direktif için bkz. Erişim Tarihi: 06.01.2014, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF>.

¹¹ Hüseyin Can Aksoy, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, Çakmak Yayınevi, Ankara 2010, 18

¹² Songül Atak, "Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri", *Bahçeşehir Üniversitesi Kazancı Hakemli Hukuk Dergisi*, sayı 59-60, yıl 2009, 204; Oğuz Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta Yayınevi, İstanbul 2008, 122- 123.

¹³ Şimşek, 123

¹⁴ Nilgün Başalp, *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınevi, Ankara 2004, 35; Şimşek, 123.

olarak, bunların kişisel verilerin korunmasının temel felsefesi ile çelişeceği görüşüdür. Zira kişisel verilerin korunmasında amaç başta özel hayatın gizliliği olmakla birlikte insan haklarının korunmasıdır. Ayrıca tüzel kişilerin kapsama dâhil edilmesi, korunan alanın genişlemesine ve hedeften uzaklaşılmasına neden olabileceği, dolayısıyla da kişisel verilerin korunmasının zayıflaması tehlikesini de beraberinde getireceği ifade edilmiştir¹⁵. Konuya ilişkin olarak Yargıtay verdiği bir kararında¹⁶, şirket bilgilerinin (şirkete ait mali bilgiler ve programlar) kişisel veri olarak değerlendirilemeyeceğine hükmetmiştir. Belirtmek gerekir ki burada asıl tartışılması gereken, tüzel kişiye ait olan verilerin, bu veriler üzerinden bir gerçek kişiye ulaşılabileceği ihtimalinden dolayı mı korunduğu, yoksa gerçekten tüzel kişinin korunması için mi korunduğudur. Diğer yandan hukukumuzda ölüm, gerçek kişiliği sona erdirdiği için kişinin ölümü ile artık ona ait veri korumadan bahsetmek de yersiz olacaktır. Kişi öldükten sonra verilerin açıklanması serbest midir? Ölen kişiye bu hak tanınmamıştır. Onların verileri ancak mesleki sır, sosyal sır, istatistiki veya vergi sırrı ya da diğer özel haklar çerçevesinde korunmuş olabilir. Örneğin Alman Hastane Kanunun 7. m birinci fıkrasına göre kişisel verilerin korunması hastanın ölümü ile birlikte sona ermez¹⁷.

Yukarıda yapılan açıklamalardan kişisel veri olarak nitelendirilecek bu bilgilerden bazıları tek başlarına ait olduğu kişiyi ferden belirleyebilir nitelikteyken, diğer bazıları ise tek başlarına yeterli olmayıp ancak başka bilgiler yardımı ile kişi tayinine yarayan verilerdir. Örneğin parmak izi, kimlik bilgileri gibi veriler ait olduğu kişiyi tek başına belirleyebilirken, mesleki bilgiler, öğrenim durumu gibi veriler ancak yanlarında ilgili kişiyi belirlemeye yardımcı olacak diğer bilgiler ile kime ait olduğu tespit edilebilir.

1.1.2. Kişisel Veri Çeşitleri

1.1.2.1. Genel Olarak

Kişisel verilerin korunmasına yönelik var olan uluslararası düzenlemelerde ve ulusal veri koruma kanunlarında kişisel veriler, nitelik itibarıyla ayrıma tabi tutularak

¹⁵ Bu yönde görüşler için bkz. Elif Küzeci, *Kişisel Verilerin Korunması*, Turhan Kitapevi, Ankara 2010, 364-365

¹⁶ Yargıtay 12. Ceza Dairesi, E. 2013/10672, K. 2013/15772, T.10.06.2013, Kazancı İçtihat Bilgi Bankası, (E.T. 15.05.2015)

¹⁷ Bu yönde verilen kararlar için bkz. Dipnot 13'teki kararlar.

düzenleme altına alınmışlardır. Doktrinde de bu ayırım dikkate alınarak çalışmalar yapılmıştır.

Kişiyi belirlemeye elverişli birçok bilgiye rastlamak mümkündür. Bu bilgiler ilk bakışta nitelik itibari ile birbirine eşit görünümündedir. Diğer bir deyişle bu bilgilerle amaçlanan, bu bilgilerin kimliği belirli veya belirlenebilir bir kişiye ait olması, o kişiyi tespit etmeye yaramasıdır. Ancak kişiyi belirlemeye yönelik bu bilgilerden bir kısmı kişiyi sadece ferden belirlemeye yarayabilirken, diğer bir kısmı ise kişinin bir grup, görüş, inanç vb. mensubiyetine dair belirlemeye yarayabilir. Bu durum, kişi açısından, kişinin toplum nezdinde belirlenmesi olacaktır. Bu anlamda bu tür veriler nitelik itibari ile daha bir önem arz etmektedirler ve bu verilere ulusal ve uluslararası alanda kural koyucular tarafından bir takım endişelerden dolayı ayrıcalık tanınmıştır¹⁸. Bu yönde Avrupa Birliği Veri Koruma Direktifi m. 8/1, 108 nolu Avrupa Sözleşmesi m. 6 ve KVKK m. 6’de bu ayırımı destekleyen düzenlemelere yer verilmiştir.

Yukarıdaki açıklamalar bünyesinde, çalışmada kişisel veriler ikili bir ayırıma tabi tutulacaktır. Ancak kişiler açısından son derece önem arz eden bu verilere dair hukuksal düzenlemelerde terim birliği yoktur¹⁹. Doktrinde kavram sorunu tartışılmış ve yaygın olarak “hassas veri” kavramı kullanılmıştır²⁰. Bu doğrultuda kişisel verileri hassas veriler ve hassas olmayan veriler olmak üzere bu iki başlık altında inceleyeceğiz.

1.1.2.2. Hassas Veriler

Hassas veriler de birer kişisel veri olmakla birlikte ulusal mevzuatta ve uluslararası düzenlemelerde ayrı başlık altında düzenlenmiş, genel anlamdaki kişisel verilerden niteliği itibari ile daha fazla bir korumaya ihtiyaç duyulan verilerdir. Bu tür veriler sosyal ve siyasal boyut açısından endişe uyandırıcı yapıya sahiptirler²¹. Zira bu verilerin başka kişiler tarafından öğrenilmesi, bu tür verilerin nitelikleri gereği, ilgili

¹⁸ Hayrunnisa Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, Seçkin Yayınevi, Ankara 2009, 126

¹⁹ AB Veri Koruma Direktifi m. 8’de “*Verilerin özel işleme kategorileri*”, 108 nolu Avrupa Sözleşmesi m. 6’da “*Özellikli veri kategorileri*”, KVKK md. 6’da “*Özel nitelikli kişisel veriler*”, Federal Alman Veri Koruma Kanunu (Bundesdatenschutzgesetz / BDSG) m. 3/9’da “*kişiyi ilgilendiren verilerin özel türleri*”, İsviçre Veri Koruma Kanunu (Bundesgesetz über den Datenschutz / DSG) m. 3/ c’de “*özel koruma değeri olan kişisel veriler*” ifadeleri kullanılmıştır.

²⁰ Cemil Kaya, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası Prof. Dr. İl Han Özay’a Armağan*, LXIX(1-2), 2011, 317; Özdemir, 126; Atak, 208.

²¹ Özdemir, 126; Kaya, 316

kişinin bir anlamda rencide olmasına, mağduriyetine, yerine göre ayrımcılığa uğramasına neden olabilecek verilerdir²². Bu türden verilerin ayrı bir kategoriye tabi tutulması, diğer bir deyişle bu tür verilerin işlenmesinin ayrı bir maddede düzenlenmesi, bu verilerin daha sıkı bir denetim altında tutulmak istenmesinin bir sonucu olarak da değerlendirilmektedir²³.

Ulusal ve uluslararası hukuki düzenlemelerde hassas verilere dair bir tanım yapılmamış, bunun yerine hangi tür verilerin hassas veri kabul edileceğine dair madde metinlerinde sayım yapılmıştır. Bu düzenlemelerde yer alan sayımlardan yola çıkarak tanım yapılması da mümkündür²⁴. AB 95/46/AT direktifi kapsamında kişinin sağlık durumuna veya cinsel yaşamına, sendika üyeliğine, dini veya felsefi inançlarına, siyasi görüşlerine, ırk veya etnik kökenine dair doğrudan veya dolaylı olarak belirleme yapmaya elverişli her türlü veri hassas veri olarak tanımlanabilir²⁵. 108 nolu Avrupa Sözleşmesi'nde ve KVKK'da, AB 95/46/AT Direktifi' ne ek olarak ceza mahkûmiyetleri hassas veriler kapsamında sayılmıştır. Yine KVKK'da dini inanç yanında kişinin mezhebine dair veriler ve sendika üyeliği, dernek ve vakıf üyeliği, kılık kıyafeti, genetik ve biyometrik verileri de bu türden veriler arasında zikredilmiştir.

Bir önceki paragrafta yapılan açıklamalar kapsamında kişinin;

- Sağlık durumuna,
- Cinsel yaşama,
- Sendika, dernek veya vakıf üyeliğine,
- Dini, felsefi ve diğer inançlara,
- Siyasi görüşlere,
- Irk veya etnik kökene,
- Her türlü mahkûmiyetlere
- Biyometrik ve genetik verilerine

ilişkin veriler hassas verilerin türlerini oluşturmaktadır. Bu türden verilerin işlenmesinin yasak olduğu ulusal ve uluslararası düzenlemelerde belirtilmiştir. İlgili maddelerin devamında da hassas verilerin istisnai olmak üzere hangi hallerde

²² KVKK 6. madde gerekçesi

²³ Küzeci, 230

²⁴ Kaya, 316

²⁵ Benzer yönde tanımlar için bakınız Özdemir, 126; Kaya, 316

işlenebileceği düzenlenmiştir. Burada belirtilmesi gereken, hassas verilerin ayrı bir maddede düzenlenmeleri ile birlikte, hangi hallerde işlenebileceklerinin belirtilmesi ve bu haller haricinde işleme yasağının varlığı²⁶, yasa koyucular tarafından bu tür verilere verilen önemi gösterdiğiidir.

1.1.2.3. Hassas Olmayan Veriler

Genel anlamda kişisel veri olarak kabul edilen, diğer bir deyişle hassas veriler haricinde kalan verilere hassas olmayan veriler denilmektedir. Söz konusu veriler, ilgisine ait özellikleri barındıran veya onu belirleyen ya da belirlemeye yardımcı olan verilerdir. Yine bu veriler hassas veriler gibi Anayasa’da sayılan temel hak ve özgürlüklere ilişkin olmayan, başkaları tarafından bilinmesi durumunda ilgili kişinin mağduriyetine veya herhangi bir ayrımcılığa maruz kalmasını gerektirecek nitelikte veriler değildir. Gerçekten de bir kişinin T.C. kimlik numarası ile herhangi bir siyasi partiye üyeliğinin bilinmesi, bu verileri bilen kişi veya kurumda aynı hissiyatı oluşturmazacaktır.

1.2. KİŞİSEL VERİLERİN İŞLENMESİ

Kişisel verilerin işlenmesi, Kişisel Verilerin Korunması Kanunu (KVKK) m. 3’ de tanımlanmıştır. Bu tanımdan verilerin işlenmesi ifadesi, kapsamında birden fazla eylemi barındıran bir kavram olduğu anlaşılmaktadır. Bu kavramların her biri kişisel veriler üzerinde gerçekleştirilmesi muhtemel eylemler olup veri işleme kavramının da kapsamının ve sınırlarının belirlenmesi açısından önemli bir yere sahiptir.

1.2.1. Genel Olarak

Kişisel verilere dair var olan tüm ulusal ve uluslararası düzenlemelerde, bu verilerin korunması vasıtası ile kişinin temel hak ve özgürlüklerinin korunması amaçlanmaktadır²⁷. Bu amacı destekler yönde 2010 yılında Anayasa’ımızda yapılan değişiklik ile 20. maddeye eklenen son fıkra hükmü kapsamında herkesin kendisi ile ilgili verilerin korunmasını isteme hakkı düzenlenmiştir. Ancak ulusal ve uluslararası

²⁶ Hassas verilerin hangi hallerde işlenebileceği bir sonraki başlıkta incelenecektir.

²⁷ Şimşek, 4

düzenlemelerle koruma altına alınan bu talep hakkının varlığı öncelikle bu hakkın ihlal edilmiş olması önkoşuluna bağlıdır. Bu hakkın ihlali de ancak kişisel verilerin işlenmesi neticesinde mümkün olacaktır²⁸.

Kişisel verilerin işlenmesi, otomatik veya otomatik olmayan yollarla kişisel verilere dair bilgilerin bir takım işlemlerden geçirilmesi olarak tanımlanmaktadır²⁹. Kişisel verilerin işlenmesinde akla ilk gelen verilerin kaydedilmesidir. Ancak işleme kavramı, bünyesinde birçok eylemi barındırmaktadır. Ulusal ve uluslararası düzenlemeler kapsamında yapılan tanımlarda işleme kapsamında hangi faaliyetlerin yer aldığı da örnek kabilinden sayılmıştır. Bu kapsamda toplama, kaydetme, değiştirme, kullanma, aktarma, kullanılmasının engellenmesi, silme gibi faaliyetler ayrı ayrı kişisel verilerin işlenmesi kapsamındaki faaliyetlere birer örnektirler.

Kişisel verilerin işlenmesi ile hassas veriler ve hassas olmayan veriler ayrımı olmaksızın, tüm verileri kapsayan hükümlere hem ulusal hem de uluslararası düzenlemelerde yer verilmiştir. Ancak hassas verilerin işlenmesine yönelik ilgili hukuki metinlerde, bu tür verilerin hem niteliklerinden hem de daha sıkı şekilde korunması ihtiyacından dolayı, ayrıca düzenlemelere de yer verilmiştir. Zira ulusal ve uluslararası hukuki düzenlemelerde hassas veriler ve bu tür verilerin hangi şartlarda işlenebileceği ayrı maddelerde düzenlenmiştir. Bu nedenle hassas veriler ile hassas olmayan verilerin işlenmesi ayrı başlıklar altında incelenecektir.

Verilerin işlenmesi hususuna geçmeden önce, verilerin işlenmesi kapsamında değerlendirilebilecek olan kavramlara kısaca açıklık getirmekte fayda bulunmaktadır. Bu kavramların ne ifade ettiğine dair KVKK, 108 nolu Sözleşme ve 95/46/AT sayılı Direktif'te bir hüküm bulunmamakla birlikte Federal Alman Veri Koruma Kanunu (BDSG)'nda adı geçen kavramların tanımları yapılmış, İsviçre Veri Koruma Kanunu (DSG)'nun üçüncü maddesinde ise verilerin işlenmesi, ilan edilmesi ve toplanması kavramları tanımlanmıştır. Kişisel verilerin işlenmesi kavramının daha iyi

²⁸ Benzer yönde görüş için bkz. Uğur Ersoy, *Bir İnsan Hakkı Olarak Kişisel Verilerin Korunması* (Yayınlanmamış Yüksek Lisans Tezi), Ankara 2009, 17

²⁹ Başalp, 33, 95/46/AT sayılı Avrupa Konseyi Direktifi m.2/b, KVKK m. 3/e, İsviçre Veri Koruma Kanunu (DSG) m. 3/ b. (e)'de kişisel verilerin işlenmesi, kişisel verilerin kullanılan araçlar ya da yöntemlerden bağımsız olarak, özellikle temin edilmesi, saklanması, kullanılması, değiştirilerek işlenmesi, ilan edilmesi (açıklanması), arşivlenmesi ya da verilerin imha edilmesi olarak tanımlanmıştır. Federal Alman Veri Koruma Kanunu (BDSG) m. 3/ b. (4)' te verilerin işlenmesi, kişiye ilişkin verilerin kaydedilmesi, değiştirilmesi, aktarılması, engellenmesi, ve silinmesi şeklinde tanımlanmıştır.

anlaşılabilmesi için, tanım içerisinde yer alan bu kavramlar Federal Alman Veri Koruma Kanunu (BDSG)'ndan esinlenilerek açıklanmaya çalışılmıştır.

1.2.1.1. Verilerin Toplanması

Toplama, ilgililerden kişisel nitelikteki verilerin temin edilmesidir³⁰. Bu verilerin alınması her hangi bir şekilde olabilir. Yani verilerin toplanmasının belli bir usulü yoktur. Örneğin bir kişinin sorması, evrakların talep edilmesi, gözlemlene veya dinlenme yoluyla elde edilmesi mümkündür³¹. Toplama, esasında işleminin ön aşamasıdır. Temin etme kavramının kelime anlamı dikkate alındığında, kişisel verilerin toplayan kişinin hâkimiyet alanına ulaşmış olması zorunluluğu karşımıza çıkar. Çünkü kişisel veriler üzerinde tasarruf yetkisine sahip olunursa ancak o zaman toplayan kişi bu bilgileri işleyebilir³². Bu anlamda hâkimiyet alanının varlığı belirleyici bir rol oynar.

Veriler, verilerin toplanması amacıyla elde edilmelidir. Ancak tesadüfen elde edilmiş bir bilgi de, silinmediyse ve sonradan kendisine toplama amacı yüklendiyse, o zaman veri koruma hukuku kapsamında veri toplanmasından söz edilebilir. Bu yönde ilgilinin kendisine ait verileri vermesi ya da iletmesi şayet toplama amacı yoksa veri koruma hukuku kapsamında verilerin toplanması olarak kabul edilmeyecektir³³.

1.2.1.2. Verilerin Kaydedilmesi

Kaydetmek, kişiye ilişkin verilerin işlenebilmesi amacıyla verilerin, bir veri taşıyıcısı üzerine alınması, kaydedilmesi veya burada muhafaza edilmesidir. Elle yapılan işlemlerde kaydetme, bir kayıt kartına yapılabilir. Hatta kişiye ilişkin bilgilerin bir not defteri üzerine yazılması da kaydetme olarak değerlendirilir. Makine yöntemi ile kaydetmede veri taşıyıcısı olarak akla gelen tüm iletişim araçları dikkate alınır. Bilgi girişinde ara koruma da bir kaydetmedir. Çıkarılan bir DNA'nın vücut hücresinin doku örneklerinin muhafazası da kaydetmedir. Kaydetmenin şartı, kaydetmenin verilerin işlenmesi amacıyla yapılmasıdır. Eğer sorumlu makam işleme amacını

³⁰ Selk, Robert, Datenschutz und Internet, Der Andere Verlag, München 2002 s. 51, Gabor P. Blechta, (Editör: Maurer – Lambrou Blechta), *Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz*, 3. Auflage, Helbing Lichtenhahn Verlag, 2014 Basel, Art. 3/g DSG, 107, N. 78

³¹ Thilo Weihert, Wolfgang Däubler, Thomas Klebe, Peter Wedde, *Bundesdatenschutzgesetz, Kompaktcommentar zum BDSG*, 3. Vollständig neu bearbeitete Auflage, Nördlingen 2010, 126

³² Selk, 51

³³ Weihert, Däubler, Klebe, Wedde, 127

gerçekleştiremediyse ve bu vesile ile elinde bulundurduğu verileri tekrar kullanmak istemiyorsa bu verileri silmek zorundadır³⁴.

1.2.1.3. Verilerin Değiştirilmesi

Verilerin değiştirilmesi, kişiye ilişkin kaydedilmiş verilerin içerik olarak şeklinin değiştirilmesidir (m. 4/2 nr. 2). Değiştirme, kaydedilmiş verinin içeriğinin tamamlanması veya (başka bir veriyle) birleştirilmesi şeklinde ortaya çıkabilir. Bu durum içerik değişikliği de olabilir. Bu bağlamda kaydedilmiş verinin içeriğinin (kısmen) silinmesi artık değiştirme olarak kabul edilmemektedir. İçerik olarak şekillendirilmiş verinin değiştirilmesi, verinin başka bir kullanım bağlamında şekillendirilmesi olarak da görülebilir. Kaydedilen verinin sadece dış şeklinin değiştirilmesi örneğin alan adının değiştirilmesi veya yeni bir güvenlik yazılımının kullanılması bu anlamda değiştirme olarak kabul edilmez. Buna karşın şifreleme veya kodlama içerik olarak değiştirmedir. Değiştirme kavramına işlemenin alt kavramı olarak esaslı maddi ve hukuki anlam yüklenemez (değiştirme kavramına, işlemenin bir alt başlığı olduğu gibi bir anlam yüklenemez). Ama daha ziyade düzeltme, engelleme (bloke etme), (silme), anonimleştirme veya müstear ad haline getirmenin özel bir şeklidir³⁵.

1.2.1.4. Verilerin Aktarılması

Verilerin aktarılması, kişiye ilişkin verilerin iletilmesi veya inceleme amacıyla hazır bulundurulması yoluyla üçüncü kişilere duyurulmasıdır. 1977 tarihli BDSG de verilerin incelenme amacıyla hazır bulundurulması verilerin aktarılması olarak öngörülmüştü. Bunu dengelemek amacıyla aktarma kavramının sınırlandırılması için ve otomatik geri alma yönteminin tehlikeleri nedeniyle 90 tarihli BDSG de özel izin (onay) şartları öngörülmüştür.

Üçüncü kişilere verileri duyurmanın özel bir şekli yoktur. Bu yazılı, sözlü, telefonla verileri aktaran kişinin vücut hareketleri yoluyla veya elektronik medya aracılığı ile gerçekleştirilebilir. Yani telefonda görüşme veya doğrudan görüşme duyurma için yeterlidir. Verilerin aktarılmasında alıcının somut bilinen bir kişi olması

³⁴ Weihert, Däubler, Klebe, Wedde, 127

³⁵ Weihert, Däubler, Klebe, Wedde, 127-128

şart değildir. Duyurunun kamuya ya da belirli kişi grubuna yapılmış olması yeterlidir. Örneğin alkol bağımlılığı veya savurganlık nedeniyle alınan kısıtlama kararının kamuya duyurulması gibi. Verilerin, arama için internete konulması verilerin yayınlaması, aktarılması olarak kabul edilir. Duyurma için bilgilerin ilgilinin belirli durumlarda üçüncü kişilere göstermek amacıyla sunduğu bir veri taşıyıcısı üzerine (örneğin pasaport, kimlik veya chipkart) yazılması yeterlidir. Verilerin ilgilinin bizzat kendisine (veri sahibine) iletilmesi bu anlamda aktarma değildir.

Verileri kaydeden makam içerisinde verilerin iletilmesi ilke olarak verilerin aktarılması olarak kabul edilmez. Alıcı mutlaka üçüncü kişi olmak zorundadır. Ama bu şart verilerin sorumlu makam içerisinde (kullanma) özel hukuki gerekliliklere bağlı olarak aktarılması durumunda aranmaz. Örneğin amaç değişikliği veya mesleki sırlarda olduğu gibi. Örneğin bir kurumun seçilmiş temsilcisi kısmen bağımsız makam olarak öngörülür. Aktarma, üçüncü bir makamda verilerin toplanmasıyla birlikte değerlendirilir³⁶.

1.2.1.5. Verilerin Kullanılmasının Engellenmesi

Verilerin işlenmesinin veya kullanılmasının sınırlandırılması amacıyla uygun işaretler kullanmak suretiyle engelleme, yazılı ve teknik olarak yapılabilir. Engellenmenin, verilerin saklanması, gizlenmesi yoluyla da gerçekleştirilmesi mümkündür. Hukuki anlamda izin verilmeyen, yani hukuka uygun olmayan veri işleme yapılması halinde veya kayıtlarda, tutanaklarda, veri taşıyıcılarında kapama tertibatı kurulması suretiyle de verilerin kullanılmasının engellenmesi sağlanabilir³⁷. Yani elle kaydedilmiş verilerin saklandığı yerlere girişin ya da elektronik ortamda saklanan verilerin bulunduğu cihazlara erişilmesinin engellenmesi yoluyla, hukuki anlamda izin verilemeyen şekillerde verilerin işleme durumlarında, bu verilere ulaşma anlamında kişisel verilerin koruma altına alınması veyahut veri taşıyıcılarında veya tutanaklarda bir kapatma tertibatı olması yoluyla veri kullanımının engellenmesi sağlanabilir. Bunun haricinde veri kullanımının engellenmesi özel bir veri dolabında verilerin saklanması suretiyle de gerçekleştirilebilir. Kaydedilmiş ve işlenmiş verilere ulaşımın engellenmesi teknik surette olabileceği gibi yazılı şekilde de olabilir. Kişisel

³⁶ Weihert, Däubler, Klebe, Wedde, 128-129

³⁷ Weihert, Däubler, Klebe, Wedde, 129

verilerin saklandığı dosyaya ulaşımın şifreli olması da bir engelleme şekli olarak değerlendirilmektedir. Ayrıca kişisel verilerin asıllarına ulaşım engellenmekle birlikte veri aslının kopyasına ulaşım mümkün olabilir³⁸. Belirtmek gerekir ki kişisel verinin aslı olmadan işlem yapılamayacağı durumlarda, diğer bir ifadeyle veri kopyası ile işlem yapmanın mümkün olamayacağı durumlarda veri aslının verilememesi veya veri aslına ulaşılamaması, verilerin kullanılmasının engellenmesi olarak değerlendirilecektir.

Kişisel verilerin kullanılmasının engellenmesi belirli amaçlara yönelik olabilir. Örneğin kişisel verilerin reklam amacıyla veya Pazar veya bir araştırma amacıyla kullanılmasına karşı itiraz halinde verilerin kullanılmasının engellenmesi söz konusu olabilir. Kişisel verilerin güvenliği için veriler başka bir amaç bakımından kısıtlanmışlardır. Yani kişisel verilerin güvenliğine yönelik olarak bu veriler sadece toplanmasında veya işlenmesinde belirlenen amaç³⁹ için kullanılabilirler. Belirlenen bu amaç dışında kişisel verilerin işlenmesi bakımından veri kullanımı engellenmiştir⁴⁰. Direktif m. 6/f. 1- b. (c)'de kişisel verilerin, toplandığı veya işlendiği amaçlara ilişkin olarak yeterli, ilgili ve bu amacı aşamayacağı hüküm altına alınmıştır. Aynı şekilde KVKK'nın Genel İlkeler yan başlıklı m. 4/f. 2- b. (ç) bendinde işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması gerektiği, yani işlenen verilerin belirlenen amaçların gerçekleştirilebilmelerine elverişli olması, amacın gerçekleştirilmesi ile ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılması gerektiği belirtilmiştir⁴¹. Madde metninde yer alan *sınırlı* ifadesi, kişisel verilerin, verilerin işlenmesinde belirtilen amacın dışına çıkılamayacağını açık bir göstergesi olup, bu amaç haricinde mevcut kişisel verilerin kullanımının engellendiği ifade edilmek istenmektedir. Kaldı ki aynı maddenin d bendi gerekçesinde belirtildiği üzere elde bulunan kişisel verilerin, gelecekte işlenme ihtimali gerekçesiyle muhafaza edilemeyeceği, dolayısıyla bu şekilde de kişisel verilerin kullanımının engellenmesi iradesi ortaya konulmuştur⁴².

³⁸ Weihert, Däubler, Klebe, Wedde, 130

³⁹ Kişisel verilerin işlenmesinde amaç unsuru ile ilgili bkz. s. 21, 2.5.2.2. nolu başlık

⁴⁰ Weihert, Däubler, Klebe, Wedde, 130

⁴¹ KVKK m. 4 gerekçesi

⁴² KVKK m. 4 gerekçesi

1.2.1.6. Verilerin Kullanılması

Kişisel verilerin kullanılması, kişiye ilişkin verilerin her türlü kullanımınıdır. Burada kastedilen eğer işlemenin diğer şekilleri söz konusu değilse, kişisel verilerin elde bulundurulması, yakalanması, hapsedilmesidir⁴³.

Pek çok ülkenin veri koruma kanununda kişisel verilerin kullanılması, veri işlemenin bir alt dalı olarak gösterilmiş, veri işlemeden daha farklı, daha ayrık bir durum olarak görülmemiştir. Kullanmada, verilerden bir yararlanma söz konusudur. Örneğin verilerin içten, kayıtlı sistemden çağırılmasında, amaca uygun bilgi alınması durumu söz konusudur⁴⁴.

Diğer bir durum olarak da verilerin, takma ad ile kullanılması da bu kapsamda değerlendirilmektedir. Diğer bir ifadeyle işlenmiş kişisel verilerin takma adlarla veya rumuzlarla kullanılması da bu kapsamda bir kullanma kabul edilmektedir. Bu durum karşısında verilerin kamuya açıklanması ise kullanma kapsamında değerlendirilmeyip, aksine bir veri aktarımı olarak kabul edilmektedir⁴⁵.

1.2.1.7. Verilerin Silinmesi

Verilerin silinmesi, verinin artık her türlü tanınamaz hale getirilmesidir. Diğer bir ifadeyle mevcut kişisel verinin kime ait olduğunun anlaşılamaz olduğu durumlar silme olarak değerlendirilir. Yani veriye bakılarak kime ait olduğunun anlaşılamaması, o veriden veri sahibinin tespit edilememesi silme olarak değerlendirilir⁴⁶.

Diğer taraftan veri taşıyıcısının bozulması, imha edilmesi yoluyla da silme olabilir. Belirtmek gerekir ki önceden kaydedilmiş bir metin varsa, artık bu metnin okunamaz olması gerekir. Elde bulundurulan verilerin artık geçerli olmadığına dair bir açıklama yapılması, kişisel verilerin silinmesi olarak kabul edilmemektedir. Verilerin silinmesi için mutlaka kişisel verilerin tanınamaz hale getirilmesi gerekmektedir. Verilerin üzerlerinin karalanması yoluyla okunması zorlaşmış olsa bile karalama verilerin silinmesi olarak kabul edilmeyecektir. Yani kişisel verilerin yazılı bulunduğu

⁴³ Weihert, Däubler, Klebe, Wedde, 130

⁴⁴ Weihert, Däubler, Klebe, Wedde, 130

⁴⁵ Weihert, Däubler, Klebe, Wedde, 130

⁴⁶ Weihert, Däubler, Klebe, Wedde, 130

metinlerin üzerlerinin karalanması verilerin silinmesi olmayacaktır; ancak verilerin tanınamaz hale getirilmesi silme olarak kabul edilecektir⁴⁷.

Teknik anlamda verilerin yeniden oluşturulmasına ilişkin teknolojik imkânlar bakımından, yani veriler silinmeye çalışıldıktan sonra verilerin yeniden eski hale getirmeye ilişkin teknik ya da teknolojik imkânlar bakımından, tekniğin güncel durumuna göre değerlendirme yapılması gerekmektedir⁴⁸. Şöyle ki; bugün için silme kabul edilen bir durum ilerleyen zamanda silme kabul edilmeyebilir. Örneğin bilgisayar ortamında yer alan bir verinin, geri dönüşüm kutusundan da kalıcı olarak silinmesi durumunda bu bir silme olarak değerlendirilebilir. Ancak kesin olarak silinen bu verinin geri alınmasını sağlayacak bir tekniğin gelişmesi durumunda bu bir silme olmayacaktır. Teknolojinin gelişmesine bağlı olarak bu durumun bir veri silme olup olmadığının yorumlanması ya da değerlendirilmesi gerekmektedir.

6698 sayılı Kanun m. 7'de kişisel verilerin silinmesine ilişkin ayrıca bir düzenleme yer almaktadır. Bu hüküm gereğince işlenme sebebi ortadan kalkmış olan kişisel verilerin silinmesi söz konusu olacaktır. Ancak silinme kavramını açıklayıcı bir düzenleme madde metninde yer almamaktadır. Kanun'un madde gerekçesinde kişisel verilerin silinmesiyle, bu verilerin kayıtlı oldukları yerlerden tekrar kullanılamayacak ve geri getirilemeyecek şekilde imha edilmesinin amaçlandığı açıklaması yapılmıştır. Buna göre verilerin kayıtlı olduğu evrak, CD, disket gibi araçlardan verilerin tekrar geri getirilemeyecek ve kullanılmayacak şekilde silinmesi anlaşılmaktadır⁴⁹. Burada kişisel verilerin silinmesi ifadesiyle benzer olan kişisel verilerin yok edilmesi kavramı arasındaki ince ayrıma dikkat çekmek istemekteyiz. Kişisel verilerin yok edilmesi ifadesi de 6698 sayılı Kanun m.7 hükmü içerisinde düzenlenmiştir. Madde lafzına göre işlenme sebebi ortadan kalkan kişisel verilerin silinmesi veya yok edilmesi gerekmele birlikte yok etme ifadesinden ne anlaşılması gerektiğine dair bir açıklık bulunmamaktadır. Madde gerekçesinde verilerin yok edilmesi ifadesinden, bilgilerin tekrar geri getirilemeyecek ve kullanılmayacak şekilde, verilerin kaydedildiği evrak, dosya, CD, disket gibi veri saklamaya elverişli materyallerin imha edilmesi anlaşılmaktadır⁵⁰.

⁴⁷ Weihert, Däubler, Klebe, Wedde, 130

⁴⁸ Weihert, Däubler, Klebe, Wedde, 130

⁴⁹ KVKK m. 7 gerekçesi

⁵⁰ KVKK m. 7 gerekçesi

Bu iki açıklamanın ilkinden kişisel verilerin saklanması elverişli olduğu materyallere zarar vermemek suretiyle verilerin bu materyallerden tekrar geri getirilemeyecek ve kullanılamayacak şekilde silinmesi anlaşılmaktayken, ikinci açıklamadan kişisel verilerin kaydedildiği materyallerin imha edilmesi suretiyle kişisel verilerin tekrar geri getirilemez ve kullanılamaz hale getirilmesi anlaşılmaktadır.

1.2.2. Hassas Verilerin İşlenmesi

Veri korumaya yönelik ulusal ve uluslararası düzenlemelerde hassas verileri düzenleyen maddelerde açıkça görüldüğü üzere hassas verilerin işlenmesi kural olarak yasaktır. Ancak bu metinlerde izin verildiği durumlarda bu türden verilerin işlenmesi mümkün olabilecektir. Bu bağlamda hassas verilerin işlenmesinin yasak olması kural; işlenmesi ise istisnadır⁵¹. Gerçekten de 95/46/AT sayılı Direktif m. 8/f. 1’de açıkça üye devletlerin bu türden verilere dair veri işleme faaliyetini yasaklayacakları, 108 nolu Avrupa Sözleşmesi m. 6’da üye devletler, iç hukuklarında uygun güvenceler getirmedikçe hassas verilere dair otomatik bilgi işleme yapamayacakları, KVKK md. 6/f. 2’de bu türden verilerin, ilgisinin açık rızasının olmaması durumunda işlenemeyeceği, maddenin üçüncü fıkrasında ise birinci fıkrada sayılan hassas veri türlerinden sağlık ve cinsel hayat dışındaki hassas verilerin, kanunlarda öngörülen durumlarda ilgili kişinin açık rızası olmadan da işlenebileceği hüküm altına alınmıştır.

1.2.3. Hassas Verilerin İşlenebileceği (İstisnai) Durumlar

Yukarıda da belirtildiği üzere, kişisel veriler esas itibari ile işlenmeleri yasak olmakla birlikte, hukuki düzenlemelerinin istisnai olarak izin verdiği durum ve şartlarda mümkün olabilmektedir. Bu noktada nitelik itibariyle ayrıma tabi tutulan kişisel veriler, işlenmeleri açısından da hassas verilerin işlenmesi ve hassas olmayan verilerin işlenmesi ayrımı yapılmak suretiyle ulusal ve uluslararası düzenlemelerde hüküm altına alınmıştır.

⁵¹ Kaya, 321

1.2.3.1. İlgilinin Rızası ile Hassas Verilerin İşlenmesi

Tüm hukuki düzenlemelerde⁵² hassas verilerin istisnai olarak işlenebilmelerini mümkün kılan ilk durum, ilgili kişinin, kendisine ait hassas verinin işlenmesine muvafakat vermesidir. Rıza beyanı, ilgili kişinin kendisine ait olan verilerin geleceğini tayin etme özgürlüğü ve kişinin verileri üzerindeki denetim hakkının önemli bir aracı olması sebebi ile kişisel verilerin işlenmesi açısından en önemli meşruiyet nedenidir⁵³. 95/46/AT sayılı Direktif ilgili maddede ulusal düzenlemelerle rıza beyanına rağmen işlemenin yasak olmasına olanak tanımıştır. 108 sayılı Sözleşme’de ise hassas verilerin işlenebilmesi ulusal mevzuatlarda yeterli güvencelerin varlığı şartına tabi tutulmuştur. Türk Veri Koruma Kanunu’nda da hassas verilerin işlenmesi yasağı, istisnası ile birlikte m. 6/ f. 2’de belirtilmiştir.

Rızayı açıklamaya yetkili kişi, hakkında veri işlenmesi yapılacak olan ilgili kişidir. Hassas verilerin işlenebilmesi için 95/46/AT sayılı Direktif, ilgili kişinin (veri öznesinin) açık rızasının varlığını aramaktadır. Açık rıza beyanı ile şüphesiz ki ilgilinin özgür iradesi ile ve hiçbir etki altında olmadan vereceği beyan ifade edilmektedir. Ayrıca açık rıza beyanının alınabilmesi, ilgili kişinin rıza beyanında bulunacağı konu ile ilgili olarak yeterli derecede bilgilendirilmesi ile mümkündür⁵⁴. Bu anlamda Direktif’e göre zımni rızanın varlığı hassas verilerin işlenmesinde hukuka uygunluk açısından yeterli değildir. Diğer yandan Direktif söz konusu açık rıza beyanı ile ilgili özel şekil şartı aranmadığından beyanın sözlü veya yazılı olması mümkündür. 2008 tarihli Tasarıda rıza beyanı açısından yazılı şekil şartı aranmıştı. 2014 tarihli Tasarı ve 6698 sayılı KVKK’da rızanın yazılı olması şartı kaldırılarak açık rızanın varlığı aranmaktadır. Kanun koyucu, açık rızayı m. 3/ f. 1-b. (a)’da tanımlamıştır. Buna göre açık rıza “*Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızayı,*” şeklinde tanımlanmıştır. Bu tanımda ön plana çıkan ilgilinin rızasının açık olması için bilgilendirilmiş olmasına bağlı olmasıdır. Bu bilgilendirme KVKK m. 10 hükmü

⁵² 108 sayılı Avrupa Konseyi Sözleşmesi m.6, 95/46/AT sayılı AB Direktifi m. 8/f. 2-b. (a), KVKK m. 6/ f. 2

⁵³ Küzeci, 220

⁵⁴ Kaya, 324; Elif Küzeci, Hacettepe Üni. KVK konferans

gereğince, veri sorumlusu tarafından yerine getirilecek olan bir bilgilendirme olacaktır⁵⁵.

Rıza beyanı zaman itibari ile hangi aşamada açıklanacağına dair hukuki düzenlemelerde bir hüküm yer almamaktadır. Burada açık rızanın hassas verinin işlenmesinden önce veya işlenme esnasında var olması gerekeceği kanaatine varılmıştır. Zira hareket tamamlandıktan, yani suç tamam olduktan sonra mağdurun rızası eylemi suç olmaktan çıkarmayacaktır⁵⁶. Aksi durum hassas verilerin istisnai olarak işlenmesiyle de bağdaşmayacaktır.

1.2.3.2. İş Kanunları Hükümlerine Göre Hassas Verilerin İşlenmesi

95/46/AT sayılı Direktif m. 8/f. 2- b. (b) hükmünce yeterli koruma önlemleri sağlanmak kaydıyla ulusal kanunların verdiği yetki ile sınırlı olmak üzere, veriyi işleyecek olan açısından iş kanunları kapsamında yükümlülüklerini ve özel haklarını yerine getirmek amacıyla hassas veriler işlenebilir⁵⁷. Belirtmek gerekir ki bu sebebe dayanarak hassas verilerin işlenebilmesi ancak veriyi işleyecek kişi açısından kanunen kendisine verilmiş bir yükümlülüğün varlığını gerektirir. Diğer yandan ulusal mevzuatlarda hassas verilerin bu madde kapsamında işlenebilmesi ancak yeterli korunmanın da sağlanmasını şartıyla mümkün olabilecektir⁵⁸. 2008 tarihli KVKK'ta benzer düzenleme m.7/ f. 2- b. (c)'de yer almaktaydı. Tasarıda da hassas verilerin rıza olmaksızın işlenebilmesi, işlemeyi yapacak olan veri kütüğü sahibine kanunen yüklenmiş bir yükümlülüğün var olması gerekliliği idi. Diğer bir gereklilik de veri kütüğü sahibinin ilgili kişiye yeterli korumayı sağlamasıydı. Örneğin sağlık konularında Umumi Hıfzısıhha Kanunu ile özel nitelikteki kişisel verilerin işlenebilme olanağı mümkün ise Sağlık Bakanlığı veya ilgili bir başka kuruluş veri işlemlerini gerçekleştirebilecektir⁵⁹. Tasarı'daki bu düzenlemedeki iş kanunları ifadesi ile sadece iş hukukunun anlaşılması gerekir. Tasarının ilgili madde gerekçesindeki örnekten de anlaşılacağı üzere kamu hukuku bünyesindeki çalışmalar da bu kapsamda

⁵⁵ Veri sorumlusunun aydınlatma yükümlülüğü üçüncü bölümde incelenecektir.

⁵⁶ Zeki Hafizoğulları, "Hukuka Uygunluk Nedenleri", Erişim Tarihi: 01.02.2014, <http://www.abchukuk.com/cezahukuku/hukuka-uygunluk.html>.

⁵⁷ Başalp, 44; Kaya, 324

⁵⁸ Kaya, 324-325

⁵⁹ KVKK 7/f. 2- b. (c) madde gerekçesi.

değerlendirilebilecekti⁶⁰. Tasarı'nın bu hükmü, 6698 sayılı KVKK'da değiştirilerek düzenlenmiştir. Buna göre KVKK m. 6/ f. 1'de sayılan hassas verilerden sağlık ve cinsel hayata ilişkin veriler dışında kalan diğer veriler, kanunlarda öngörülen durumlarda, ilgisinin rızası aranmaksızın işlenebilecektir. Yine KVKK m. 6/ f. 4'te, 95/46/AT sayılı Direktif ve Tasarı hükmüne paralel şekilde, Kurul tarafından belirlenecek yeterli önlemlerin alınmış olması, bu verilerin işlenmesi için şart koşulmuştur.

1.2.3.3. Hayati Menfaatlerin Korunması Amacıyla Hassas Verilerin İşlenmesi

95/46/At sayılı Direktif m. 8/f. 2-b. (c) hükmü kapsamında veri öznesinin fiziksel veya yasal olarak rıza açıklamasında bulunamayacağı durumlarda, ilgili kişinin veya diğer bir kişinin hayati menfaatlerini korumak için veri işleme gerçekleştirilebilir. Aynı yönde düzenlemeye 2008 tarihli KVKKT m. 7/f. 2- b. (b)'de de yer verilmişti. Burada hayati menfaatleri korunacak ilgili kişi, yani içinde bulunduğu fiziki veya yasal durum nedeni ile rıza beyanında bulunamayan kişi olabileceği gibi diğer bir kişinin⁶¹ de olabileceği ifade edilmekteydi. Burada belirtilmesi gereken bir husus da ilgili kişinin rıza beyanında bulunamayacak durumda olması, rızanın hiç olmadığı anlamına gelmeyeceğiydi. Çünkü burada farazi olarak rızanın var olduğu kabul edilmekteydi. Bu bağlamda ilgili kişinin fiziki veya yasal durumu elverişli olsaydı dahi hassas verilerin işlenmesine rıza göstermeyeceği anlaşıyor ise rızanın varlığından da söz edilemeyeceği kabul edilmekteydi⁶². 6698 sayılı KKKV'da bu hüküm, m. 6/ f. 3 kapsamında düzenlenmiştir. Bu fıkra hükmüne göre ilgilinin hassas verileri, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi bakımından, ilgililerin rızaları aranmaksızın ve yetkili kurum ve kuruluşların, dördüncü fıkra hükmü gereğince Kurul tarafından belirlenen yeterli önlemlerin alınması şartıyla işlenebileceklerdir.

⁶⁰ Aynı yönde bkz. Kaya, 324.

⁶¹ “Diğer bir kişi” ifadesi ile belli bir kişinin mi yoksa her hangi bir kişinin mi kastedildiği belli değildir. Bu durumda içinde bulunulan durumun şartlarına göre değerlendirme yapılmalıdır. Örneğin bulaşıcı bir hastalık dolayısıyla rıza beyanı olmaksızın hassas veri işlenmesi söz konusu ise burada tehdit tüm topluma karşı olacağından diğer bir kişi ile her hangi bir kişi kastedilmektedir. Bkz. Kaya, 325

⁶² Başalp, 45; Özdemir, 128

1.2.3.4. Kamuya Yararlı Kurum ve Kuruluşlarca Hassas Verilerin İşlenmesi

95/46/AT m. 8/ f. 2- b. (d) ile 2008 tarihli KVKKT m. 7/ f. 2- b. (ç)'de benzer düzenlemelere yer vermiştir. Bu kapsamda dernek, vakıf, sendika gibi kamuya yararlı kurum ve kuruluşlar tarafından hassas verilerin işlenmesi hüküm altına alınmıştır⁶³. Buna göre hassas verilerin, kurum ve kuruluşların meşru faaliyetleri kapsamında, bu kuruluşların üyeleri veya üyelerin faaliyet amaçları ile bağlantılı olarak düzenli şekilde iletişimde bulundukları kişileri⁶⁴ ilgilendirmesi şartıyla ilgili kişinin (veri öznesinin) rızası olmaksızın üçüncü kişilere açıklanmamak üzere işlenmesidir⁶⁵. 6698 sayılı Kanun'da, Tasarı ve Direktif hükmüne birebir karşılık gelecek bir düzenleme yer almamaktadır. Kanun'un lafzından, hassas verilerin işlenmesinin istisna, kural olarak ise işlenememesi olduğu anlaşılmaktadır. Zira 6. maddenin ikinci fıkrasında ilgilisinin açık rızası olmadan işlenemeyeceği hükmü açıktır. Maddenin üçüncü fıkrasında ise hassas verilerin, kanunlarda öngörülen hallerde ilgilisinin açık rızası olmaksızın işlenebileceği düzenlenmiştir. Bu münasebetle kamuya yararlı kurum ve kuruluşlar, ilgili kanun hükümleri gereğince bu anlamda hassa veri işlemesine müsaade etmeleri durumunda hassas verileri işleyebileceklerdir.

1.2.3.5. İlgili Kişi Tarafından Kamuya Açıklanan Hassas Verilerin İşlenmesi

Direktif m. 8/ f. 2- b. (e), 2008 tarihli KVKKT m. 7/ f. 2- b. (d) ve 2014 tarihli KVKKT m. 6/ f. 2- b. (ç) hükümlerine göre ilgilisi tarafından alenen ve herkesin öğrenebileceği şekilde kamuya açıklanan hassas veri ya da veriler açısından korunmaya değer hukuki yarar ortadan kalkacağı için bu hassas veriler de yukarıda zikredilen hallerde olduğu gibi kesin işlem yasağı kapsamında çıkmış olacaktır⁶⁶. Ancak istisnai bu durumda dahi verilerin işlenmesi açısından mutlak bir işleme serbestisi söz konusu değildir. Bu hususta 2008 tarihli Tasarı m. 7 hükmünün gerekçesinde verilerin işlenmesinin temel hak ve özgürlükler ile kişinin özel alanı açısından sınırlandırılması söz konusudur⁶⁷. Diğer yandan kesin işlem yasağı bu hüküm kapsamında ortadan kalksa bile Direktif m. 6 ve 7, Tasarı m. 5 ve 6 kapsamında işlenmesi durumu söz konusu

⁶³ KVKKT 7/f. 2- b. (ç) madde gerekçesi.

⁶⁴ Bu kişilere örnek olarak kurum ya da kuruluşa devamlı bağışta bulunan kimseler verilebilir.

⁶⁵ Kaya, 326-327; Başalp, 45; Özdemir, 129

⁶⁶ KVKHKT 7/2-d madde gerekçesi.

⁶⁷ Başalp, 45, KVKHKT 7/2-d madde gerekçesi.

olacaktır. Diğer bir ifadeyle hassas verinin ilgilisi tarafından kamuya açıklanması ile veri hassas olmaktan çıkmakta ve dolayısı ile kesin işlem yasağı da bu veri için ortadan kalkmakta, ancak genel veri işleme hükümlerine göre verinin işlenmesi durumu söz konusu olmaktadır.

6698 sayılı KVKK kapsamında Direktif'in bu hükmüne açıkça yer verilmemiştir. Ancak hüküm nitelik itibarıyla ele alındığında, ilgilisi tarafından alenen açıklanacak, diğer bir ifadeyle alenileştirilecek olan hassas veriler aslında ilgisinin rızası ile bu hale gerilebileceği açıktır. Dolayısıyla ilgilinin rızası olmadan alenileştirilme söz konusu olmayacağına göre Direktif ve Tasarılar da yer alan bu hükmün, 6698 sayılı Kanun m. 6/ f. 2 kapsamında değerlendirilmesi mümkündür. Zira bu fıkra hükmüne göre ilgisinin rızası olmaksızın hakkında hassas veri işlenmesi mümkün olamayacağı açıktır. İlgilisi tarafından aleni hale getirilmiş olan verilerde, bu alenileştirmenin bizzat ilgili tarafından yapılması, bu eylemde rızanın varlığının bir göstergesi olup bu hale getirilmiş verilerin işlenmesinde bir sakınca bulunmayacaktır.

1.2.3.6. Yargılama Faaliyetleri Nedeni ile Hassas Verilerin İşlenmesi

Hassas verilerin yargılama faaliyetleri veya adli işlemler nedeniyle işlenmesi söz konusu olabilir. Bu durumda da ilgili hassas veri için kesin işlem yasağı ortadan kalkmaktadır. Bu anlamda Direktif m.8/ f. 2- b. (e) ve 2008 ve 2014 tarihli Tasarılar paralel hükümler içermektedirler. Buna göre kanuni hakların tesisi, yerine getirilmesi veya savunulması durumlarında hassas verilerin işlenmesinin zorunlu olması istisnai olarak bu verilerin işlenmesine olanak tanımaktadır⁶⁸. 6698 sayılı Kanun açısından yukarıda da bahsedildiği üzere hassas verilerin işlenmesinde Tasarı ve Direktif hükümlerine nazaran daha genel bir düzenlemeye yer verilmiştir. Bu düzenleme gereği ilgili kanun, hassas verilerin işlenmesine ilgisinin açık rızası olmaksızın izin vermesi halinde, veri sorumlusu da veri işlemesi yapabilecektir.

⁶⁸ KVKK 7/2-e madde gerekçesi.

1.2.3.7. Tıbbi Gereklilik Açısından Hassas Verilerin İşlenmesi

Hassas verilerin istisnai olarak işlenmesine imkân veren hallerden bir diğeri tıbbi gereklilik durumudur. Bu kapsamda tıbbi veriler⁶⁹ ön plana çıkmaktadır. Tıbbi veriler de sağlık durumuna ilişkin veriler olması sebebi ile hassas veriler içerisinde değerlendirileceğinden, kesin işlem yasağı bu türden veriler için de uygulanabilecektir. Ancak Direktif m.8/ f. 3'te tıbbi verilere dair zikredilen kesin işlem yasağına istisnai hüküm düzenlenmiştir. 2008 tarihli Tasarı m.7/ f. 2-b. (f) ve 2014 tarihli Tasarı m. 6/ f. 2- b. (e) hükümleri kapsamında tıbbi verilere dair zikredilen kesin işlem yasağına istisna getirilmişti. Buna göre önleyici tıp (koruyucu hekimlik), sağlık hizmetlerinin yürütülmesi, bakım, tıbbi teşhis veya tedavinin sağlanması açısından hassas verilerin işlenmesi zorunlu ise kesin işlem yasağı uygulanmayacaktır. Direktif kapsamında istisnai bu durumda işleme; ulusal kanun kapsamında veya mesleki gizlilik yükümlülüğü ile ilgili ulusal yetkili kurumlar tarafından veya eşdeğer gizlilik yükümlülüğüne tabi diğer bir kişi tarafından saptanan bir sağlık uzmanı eliyle işlenebileceği düzenlenmiştir. Tasarılarda da benzer yönde düzenlemeye yer vermekle birlikte, hassas tıbbi verilerin kimler tarafından işlenebileceği madde içerisinde tek tek sayılmıştı. Buna göre 1. Sağlık kurumları, 2. Sigorta şirketleri, 3. Sosyal güvenlik kurumları, 4. İşyeri sağlık birimi oluşturmakla yükümlü işverenler, 5. Sağlıkla ilgili okul ve üniversiteler tarafından kanunlara uygun olarak hassas verilerin işlenmesi mümkün olabilecektir.

6698 sayılı KVKK'da ise Direktif'in bu hükmüne karşılık gelecek düzenleme m. 6/ f. 3'te düzenlenmiştir. Buna göre koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri amaçlarıyla yetkili kurum ve kuruluşlar tarafından ilgilinin rızası aranmaksızın hassas veri işlenmesi mümkün olabilecektir.

1.2.3.8. Kamu Yararı Nedeniyle Hassas Verilerin İşlenmesi

Direktif m. 8/ f. 3'te üye devletlere, önemli kamu yararı⁷⁰ açısından gerekli olması durumunda hassas verilerin işlenmesine istisnai hükümler getirme yetkisi tanımıştır.

⁶⁹ Doktrinde tıbbi veriler “ *hastaların her türlü hastalık ve tedavilerine ilişkin kişisel verileridir.* ” şeklinde tanımlanmıştır. Bkz. Özdemir, 130

⁷⁰ Kamu yararı kavramı 1950'li yılların sonunda Fransız hukukunda, idare hukukunun temel kavramı ve uygulama alanı olduğu ileri sürülen bir kavram olarak görülmektedir. Kamu yararı, muğlak ve tanımı

Ancak ilgili Direktif'te önemli kamu menfaatlerinin neler olduğunu tespit eden hükme yer verilmemiştir. Benzer hüküm 2008 tarihli Tasarı'da temel kamu yararının ve yeterli koruma tedbirlerinin bulunması şartıyla Kişisel Verileri Koruma Kurulu tarafından hassas verilerin işlenmesine karar verilebileceği düzenlenmiştir. Tasarı kapsamında da kamu menfaatlerinin neler olabileceğine dair bir düzenlemeye yer verilmemiş, bu belirleme doktrin ve uygulamaya bırakılmıştır. 2014 tarihli Tasarı ve 6698 sayılı Kanun'da, Direktif'in bu hükmü açık şekilde düzenlenmemiştir. Kanun'un, hassas verilerin işlenmesini düzenleyen 6. maddesinin üçüncü fıkrası genel anlamda sağlık ve cinsel hayat dışındaki hassas verilerin belli şartlar altında açık rıza olmaksızın işlenebileceğini belirtmekle birlikte, bunlar haricindeki hassas verilerin, kanunlarda öngörülen hallerde açık rıza aranmaksızın işlenebileceğini düzenlemektedir. Dolayısıyla 6698 sayılı Kanun m. 6/f. 3 hükmü bu kapsamda değerlendirilebilir.

Doktrinde kamu yararı, tüm idari etkinliklerin amacını oluşturan, kamu hizmetlerinin belirlenmesinde de oldukça önemli bir kavram olarak ifade edilmiştir⁷¹. Bu bağlamda Giriş kısmında da belirtildiği üzere devlet, kamu hizmetlerini hızlı, kolay ve güvenilir bir biçimde yerine getirmek için hassas nitelikteki verileri işleyebilme imkânı tanınmıştır. Doktrinde kamu yararının, tüm idari işlemlerin ve kararların değişmez ve genel amacı olduğunun belirtilmesi yanında, bazı idari işlem ve kararlar için kanunlarda daha özel ve somut amaçlar da öngörülmüş olabileceği, bu daha somut ve özel amaçların aslında, temel amaç olan kamu yararının daha da belirginleşmiş bir şekli olduğu belirtilmiştir. Örneğin kolluk işlemlerinin amacı da esas olarak kamu yararının sağlanmasına yöneliktir. Dolayısıyla kamu düzeninin sağlanması ile de kamu yararı gerçekleşmiş olacaktır⁷². Kanun'un 28. maddesi kapsamında belirtilen hallerde Kanun hükümlerinin uygulanmayacağı hüküm altına alınmıştır. Şüphesiz ki bu kapsama hassas olmayan kişisel veriler yanında hassas veriler de dâhil olacaktır. Bu anlamda 28. maddenin birinci fıkrasının (ç) bendi⁷³ içerisinde geçen milli güvenliğin, kamu güvenliğinin, kamu düzeninin sağlanmasına yönelik olarak kamu kurum ve kuruluşları

oldukça güç bir kavramdır. İsmet Giritli, Tayfun Akgüner, Pertev Bilgen, Kahraman Berk, *İdare Hukuku*, Der Yayınları, İstanbul 2012, 60 vd.

⁷¹ Giritli, Akgüner, Bilgen, Berk, 60-61, Metin Günday, *İdare Hukuku*, İmaj Yayınevi, Ankara 2011, 160,

⁷² Günday, 160-161

⁷³ m. 28/f. 1- b. (ç) hükmü: “*Kişisel verilerin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum veya kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarî faaliyetler kapsamında işlenmesi*”

tarafında yürütülecek olan önleyici, koruyucu ve istihbarî faaliyetler kapsamında hassas kişisel verilerin işlenmesi bünyesinde esas itibari ile kamu yararının gerçekleştirilmesi amacı da yer almış olacaktır.

1.2.3.9. Suçlar, Hükümler ve Güvenlik Tedbirlerine İlişkin Hassas Verilerin İşlenmesi

Direktif m. 8/ f. 4 hükmü kapsamında ilgili kişiye ait suç, adli hüküm ve güvenlik tedbirine ilişkin hassas verilerin işlenmesine ancak resmi makamın kontrolü altında olması veya ulusal kanunlar kapsamında yeterli koruma önlemleri sağlanması şartı ile imkân tanınmıştır. Yine benzer düzenlemeye Tasarı m. 7/f. 4'te yer verilmiştir ve ilgili kanunlarda yeterli koruma önlemleri bulunması ve yalnızca yetkili mercilerin kontrolü altında işlenebileceği, ceza mahkûmiyetlerine ilişkin sicilin ise sadece Adalet Bakanlığı'nın kontrolünde tutulabileceği açıkça belirtilmiştir. Bu kapsamda olmak üzere suçların tespiti ve takibi, aynı şekilde suçluların da tespit, takip ve yakalanmaları için kişisel verilerin polis tarafından işlenmesi söz konusu olabilecektir⁷⁴.

1.2.4. Hassas Olmayan Verilerin İşlenmesi

1.2.4.1. Genel olarak

Kişisel veri çeşitleri incelenirken de değinildiği üzere hassas veri olarak belirtilen veriler açısından işlenememe kuralı, işlenme ise istisnaidir. Bu nedenle de hukuki metinlerde ayrı maddeler altında düzenlenmişlerdir. Hassas olmayan verilerin işlenmesi bir anlamda veri korumaya ilişkin düzenlemelerin asıl sebebini teşkil etmektedir. Zira yukarıda 2.3.5 başlığı altında değinildiği üzere hassas veri ilgilisi tarafından kamuya açıklansa dahi bu veri hakkında kişisel veri işlemeye dair genel hükümler uygulama alanı bulmaktadır. Diğer bir anlatımla bir hassas verinin işlenmesi söz konusu olsa bile bu sınırsız işleme olamayacak, veri işlemeye dair genel düzenlemeler çerçevesinde ancak işleme mümkün olabilecektir.

95/46/AT sayılı Direktif Bölüm II'de verilerin işlenmesine dair hükümler düzenlenmiştir. Bu bölümde Veri Kalitesine İlişkin Prensipler ve Veri işlemeyi

⁷⁴ Özdemir, 132

Yasallaştırma Kriterleri yer almaktadır. Benzer hüküm 108 sayılı Avrupa Sözleşmesi m. 5'te Verilerin Niteliği başlığı altında düzenlenmiştir. 6698 sayılı Kanun kapsamında ise, Direktif hükümlerine paralel olmak üzere, İkinci Bölüm altında m. 5'te kişisel verilerin işlenmesine dair hükümlere yer verilmiştir.

1.2.4.2. Kişisel Verilerin İşlenmesine Dair İlkeler⁷⁵

Kişisel verilerin işlenmesinde dikkate alınacak ilkelerin neler olduğuna dair uluslararası temel hukuki metinler olan 95/46/AT sayılı Direktif ve 108 sayılı Avrupa Sözleşmesi ilgili maddelerinde benzer düzenlemeler yer almaktadır. Uluslararası bu düzenlemelere paralel şekilde iç hukukumuzda 6698 sayılı KVKK'da bu ilkeler düzenlenmiştir.

1.2.4.2.1. Hukuka ve Dürüstlük Kuralına Uygun İşlenmesi İlkesi

Bu ilke altında ilgili düzenlemelerin madde metinlerinden de anlaşılacağı üzere kişisel veriler, hukuka uygun ve dürüstlük kuralına uygun olarak işlenmelidir. Bu ilke esas itibari ile genel bir ilke olup, yani diğer ilkeleri de bünyesinde barındırmakla birlikte kişisel verilerin işlenmesi durumunun söz konusu olmasından silinmesine ve hatta yok edilmesine kadar var olması, diğer bir deyişle uyulması gereken ilkedir⁷⁶.

Hukuka uygunluk, genel itibari ile yapılan eylem ya da işlemlerin hukukun koruması altında olması, eylem ya da işlemin hukukun sınırları içerisinde kabul edilmesidir. Yani hukuka uygun görülen bir eylemin var olduğu yerde davranış, en baştan itibaren hukuka uygun kabul edilecek ve bu davranış hiçbir zaman hukuka aykırı da olmayacaktır. Hukuka uygunluk sebepleri, çatışma halindeki iki hukuki menfaatten zarar verenin menfaatinin daha üstün tutulmasıdır⁷⁷. Bu anlamda kişisel verilerin işlenmesinde bu sınırın tespiti önem arz etmektedir. 95/46/AT sayılı Direktif m. 5'de kişisel verilerin işlenmesinin yasal olduğu hallerin üye devletler tarafından belirleneceği ifade edilmiştir. Yasal koşullar ifadesinden burada kanunilik ilkesinin var olduğu kanaatine varılmıştır. Kanun'un İkinci Bölümü, Kişisel Verilerin İşlenmesi başlığı

⁷⁵ Kavram olarak Direktif m. 6 “*Verilerin Kalitesine İlişkin Prensipler*”, 108 sayılı Sözleşme m. 5 “*Verilerin Niteliği*” ve 6698 sayılı KVKK m. 5 “*Kişisel Verilerin İşlenmesine İlişkin İlkeler*” ifadeleri kullanılmıştır.

⁷⁶ Özdemir, 137; Elif Küzeci, *Kişisel Verilerin Korunması*, Turhan Yayınevi, Ankara 2010, 197

⁷⁷ Fikret Eren, *Borçlar Hukuku Genel Hükümler*, Yetkin Yayınları, 14. Baskı, Ankara 2012, 601

altında m. 4/ f. 1’de kanunilik ilkesi düzenlenmiştir. Kişisel verileri işleme yetkisi olanların, ancak ilgili kanunlarda belirtilen durumlarla sınırlı olmak üzere veri işleyebilmesi söz konusu olacağından kanunilik ilkesi ile kişisel verilerin işlenmesinde hukuka uygunluk sınırları da çizilmiş olmaktadır. Kanunilik ilkesinin varlığı kişilerin özel hayatlarının korunması için sınırların belirlenmesi ve veri işlemede keyfi uygulamaların önüne geçmek açısından son derece önemlidir⁷⁸.

Dürüstlük kuralı⁷⁹, somut olarak belirlenmesi oldukça güç bir kavramdır. Her somut olayın özelliğine göre ayrı ayrı değerlendirilmesi gerekir. TMK m. 2’de dürüstlük kuralı genel bir kavram olarak düzenlenmiştir. Hakların kullanılmasında ve borçların yerine getirilmesinde uyulması zorunlu kurallar olarak ifade edilmiştir. Bu bağlamda verilerin işlenmesi açısından veri işleme yetkisine sahip kişiler, işleme eylemini gerçekleştirirken dürüstlük kurallarına uyacaklardır. Madde gerekçesinde veri sorumlusu, meşru bir amaç olmak şartıyla, veri işleme amacını tereddüde yer bırakmayacak şekilde ve açık olarak belirlemek durumundadır ve bu amaç da ilgililer tarafından biliniyor olmalıdır. Bu noktada veri işlemeye yetkili kişilerin belirlenen amaç haricinde veri işlemesi yapması, ilgili kişiyi yeterince bilgilendirmemesi dürüstlük kurallarına aykırılık teşkil edeceği kanaatindeyiz⁸⁰.

1.2.4.2.2. Amaca Uygun İşlenmesi İlkesi

Bu ilkeye göre veri işlemeye yetkili olanlar, ancak hangi amaç için veri işlemede bulunacaklarını açıkça belirlemeleri suretiyle kişisel verileri işlemeleri mümkün olabilecektir. 6698 sayılı Kanun m. 4/ f. 2 – b. (c) madde gerekçesinde de belirtildiği üzere veri işlemeye yetkisi olan kişiler (veri sorumluları), ilgili sicillere kaydolurlarken veri işleme amaçlarını açıkça ve kesin olarak belirtmeleri gerekmektedir. Belirlenen bu amaçlar dışında, başka amaçlarla veri işlemeleri durumunda veri sorumluları, bu fiillerinden dolayı sorumlu tutulabileceklerdir. Bu ilke

⁷⁸ Bkz. 2008 tarihli KVKK m. 4 gerekçesi

⁷⁹ Dürüstlük kuralı anlam olarak, namuslu, dürüst ve mantıklı bir kimseden beklenen davranıştır. Toplumda var olan ahlaki değerlere ve adetlere göre bir davranışın dürüst olup olmadığı tayin edilir. Belirtmek gerekir ki dürüstlük kuralının uygulama alanının büyük bir kısmı özel hukuk içerisinde yer alsa da bu kavram sadece özel hukuk alanında uygulanan bir kavram değildir. Dürüstlük kuralı hukukun her alanında uygulanan bir temel hukuk ilkesidir. Detaylı bilgi için bkz. Kemal Oğuzman, Nami Barlas, *Medeni Hukuk*, 18. Bası, Vedat Kitapçılık, İstanbul 2012, 258 vd.

⁸⁰ Benzer yönde bkz. Özdemir, 138; Küzeci, 197

ile aynı zamanda belirlenen amaçların meşru olmasını da zorunlu kılmaktadır. Amacın meşru olması ile kastedilen, veri sorumlusunun işlediği verilerin yapmış olduğu iş veya sunduğu hizmet ile bağlantılı olması ve bu amaçlar için gereklilik arz etmesi anlamına gelmektedir⁸¹. Ayrıca amacın önceden belirlenmesi veri öznesi için bir güvence mahiyetindedir⁸². Aksi halde bu kişiler sürekli bir tehdit altında kalacaklardır ki bu durum Anayasa m. 17 kapsamında maddi ve manevi kişiliği koruma ve geliştirme hakkını engelleyen bir durum olacaktır. Diğer yandan belirlenmiş bu amaç için işlenmiş bu veriler başka bir amaç için ya da belirsiz bir amaç için yeniden işlenmesi mümkün olmayacaktır. Çünkü veri öznesi, hakkında bir veri işlemesi yapılmasına rıza vermedikçe veri işlemeye yetkili kişiler işleme eylemini gerçekleştiremeyeceklerdir. Aksi halde bir üst başlıkla ilişkili olarak yapılan kişisel veri işleme hukuka aykırı olacaktır. Dolayısı ile amacın değişmesi veya başka bir amaç için verinin işlenebilmesi için veri öznesi ilgili kişinin rızasına ihtiyaç duyulacaktır⁸³.

1.2.4.2.3. Doğruluk İlkesi

Veri koruma kapsamında ilgili kişilerin korunmasının sağlanabilmesi için öncelikli durumlardan biri de verilerin doğru olarak işlenmesidir. Diğer bir ifade ile bir kişisel verinin gerçeğe aykırı olarak işlenmesi ilgili veri sahibi kişi açısından temel hak ve özgürlüklerin ihlali olacaktır⁸⁴. Zira kişisel verilerin korunması ile asıl vurgulanmak istenen de temel hak ve özgürlüklerin korunmasıdır. Bu anlamda verilerin doğru olarak işlenmesi kadar bu verilerin her zaman doğru olarak muhafaza edilebilmesi için güncellenmeleri de gerekmektedir. 95/46/AT sayılı Direktif, 108 sayılı Avrupa Sözleşmesi ve 6698 sayılı Kanun'da verilerin doğru bir şekilde işlenmeleri ve gerektiğinde güncellenebilecekleri ifade edilmiştir. Burada verilerin güncellenmesi önemli bir kavram olarak karşımıza çıkmaktadır. Çünkü belirtmek gerekir ki güncel olmayan bir veri doğru da olmayacaktır⁸⁵. Doğru olmayan verilerin işlenmesi de yukarıda belirtildiği üzere veri korumanın özü olan temel hak ve özgürlüklerin ihlali anlamına gelecektir. Diğer yandan ilgili düzenlemelerde verilerin nasıl

⁸¹ 6698 sayılı KVKK m. 4 gerekçesi

⁸² Şimşek, 85

⁸³ Özdemir, 142

⁸⁴ Küzeci, 208

⁸⁵ Özdemir, 139

güncelleneceğine dair bir hükme yer verilmemiştir. Bir verinin en güncel ve dolayısı ile de doğru halini veri sahibi bilebileceğinden, ilgili kişi hakkındaki işlenmiş verilere dair bir değişiklik olması durumunda, kendisine ait verilerdeki bu değişikliği veri denetçisine bildirmesi suretiyle verilerin güncellenmesi mümkün olabilecektir⁸⁶.

1.2.4.2.4. Gerekli Olan Süreden Daha Uzun Tutulamaması İlkesi

95/46/At sayılı Direktif, 108 sayılı Avrupa Sözleşmesi ve 6698 sayılı Kanun bu ilke ile ilgili olarak benzer düzenlemelere yer vermişlerdir. Buna göre veri işleme yetkisi olanlar, veri sahibini açıkça belirtecek şekilde olmak üzere, veri işleme amacına ulaşmak için gerekli süre kadar muhafaza edebilirler. KVKK madde gerekçesinde de belirtildiği üzere ilgili mevzuatta verilerin saklanması için bir süre öngörülmüşse bu süreye uyulması, böyle bir süre belirlemesi yapılmamışsa veri işleme yetkisi olanlar verileri, ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebileceklerdir. Bir verinin gerekenden daha uzun bir süre saklanmasını gerektirecek bir neden yoksa ya silinecek ya da yok edilecektir. Bu noktada silme ve yok etme işlemleri 6698 sayılı Kanun m. 7/ f. 1 gereğince veri işleyenler tarafından resen veya ilgili kişinin talebi üzerine gerçekleştirilecektir. Aksi halde var olan kişisel verilerin ileride gerekli olması halinde kullanılmak üzere muhafaza edilmesi durumu söz konusu olacaktır⁸⁷. Bu durum ilgili kişi için sürekli bir tehdit anlamına gelecektir ki verilerin korunması anlayışının altında yatan özel hayatın gizliliği ve temel hak ve özgürlüklerin ihlali anlamına gelebilecektir⁸⁸.

Yukarıda belirtilen durumun aksine 95/46/AT sayılı Direktif'in m. 6/ f.1 - b (e) ile verilerin daha uzun süre muhafaza edilmesine olanak tanıyan düzenlemeye yer vermişlerdir. Buna göre tarihsel, istatistiksel veya bilimsel amaçlarla kullanım söz konusu ise verilerin öngörülen gerekli süreden daha uzun bir süre muhafaza edilmesi mümkündür. Aynı düzenlemeye 2008 tarihli Tasarı'da da yer verilmişken, bu hüküm 2014 tarihli Tasarı ve 6698 sayılı Kanun kapsamından çıkarılmıştır. Bu son durumda Direktif'te ve 2008 tarihli Tasarı'da belirtilen tarihi, istatistiki ve bilimsel çalışma amaçları için kişisel verilerin işlenmesi durumunda, verilerin süre bakımından ne denli

⁸⁶ Küzeci, 209

⁸⁷ KVKK 5/1-d madde gerekçesi.

⁸⁸ Küzeci, 210

muhafaza edileceği hususu belirsiz duruma gelmiştir. Bu noktada durumu iki yönlü yaklaşmak mümkün olabilir. Birinci durumda veriler, 6698 sayılı Kanun m. 4/ f. 2 - b. (d) hükmü gereğince belirtilen amaçlar olan tarihi, istatistiki ve bilimsel çalışmalar için gereken süre kadar muhafazası kanuna uygun olacaktır. Diğer bir ifadeyle verilerin saklandığı süre bu amaçların gerçekleştirilmesi için gereken süre kabul edilecektir. İkinci durum ise bu amaçların gerçekleştirilmesinde kullanılacak olan verilerin ilgilisi ile bağlantılarının kopararak, diğer bir deyişle anonim hale getirilerek kullanılması durumudur. Bu durumda verinin ilgisinin tespiti söz konusu olmayacağından kişisel verilerin işlendiği amaç için gerekenden daha uzun süre kişisel verilerin muhafaza edilmesi nedeniyle bir ihlal de ortaya çıkmayacaktır.

1.2.4.3. Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri

Yapılan bir eylem ya da işlemin hukuki sonuç doğurabilmesi için bu eylem ya da işlemin hukukun sınırları içerisinde olması yani hukuka uygun kabul edilmesi gerekir. Diğer bir ifade ile hukukun sonuç bağladığı eylem ya da işlemler ilgisine hak kazandırabilir veya borç altına sokabilirler. Bu anlamda yukarıda bahsedilen kişisel verilerin işlenmesine dair düzenlemelerin yanında kişisel verilerin işlenmesine dair her bir faaliyetin de hukuka uygun olması gerekmektedir. Zira kişisel bir veri her ne kadar belli, meşru bir amaç için toplanmış ve bu amaç için işlenecek olsa da ilgilinin, hakkındaki bu verinin işlenmesine rızasının var olup olmadığı, rızası varsa da bunun kanunun öngördüğü şekilde mi olduğu, kişisel veriyi işleyecek olan açısından veri işleme eylemini hukuka uygun veya aykırı hale getirecektir. Bu noktada hukuka uygunluk sebepleri veri koruması için öncelikli bir öneme sahiptir⁸⁹.

95/46/AT sayılı Direktif m. 7'de hukuka uygunluk sebeplerine yer verilmiştir. Bu sebepler içinde genel hukuka uygunluk halleri yanında özel hukuka uygunluk halleri de düzenlenmiştir. 2008 tarihli Tasarı'da da kişisel verilerin işlenmesinde hukuka uygunluk sebepleri 6. maddede ayrıca düzenlenmişti. 2014 tarihli Tasarı'da ve 6698 sayılı KVKK'da hukuka uygunluk sebeplerine ayrı bir maddede yer verilmemiş, hassas veriler ve hassas olmayan verilerin işlenmesine ilişkin maddeler içerisinde hukuka uygunluk halleri düzenlenmiştir.

⁸⁹ Ersoy, 105

1.2.4.3.1. Rıza

Kişisel verilerin korunmasına yönelik hukuki düzenlemelerde, verilerin işlenebilmesinin ilk şartı olarak rıza düzenlenmiştir⁹⁰. Tüm bu düzenlemelerin ortak paydası veri öznesi hakkında kişisel verilerin işlenmesinin hukuka uygun olabilmesi, veri öznesinin bu işleme dair vereceği rıza ile mümkün olabilmesidir. 6698 sayılı Kanun m. 5/f. 1 hükmünün aksinden veri işlemenin ancak ilgilinin açık rızası ile mümkün olabileceği düzenlenmiş, ikinci fıkrada da yedi bent halinde diğer hukuka uygunluk halleri kaleme alınmıştır. Bu durum bize, hukuka uygunluk sebepleri içinde rıza beyanının ilk ve öncelikli bir konuma sahip olduğunu göstermektedir⁹¹.

95/46/AT sayılı Direktif madde 2/h’de ilgili kişinin rızasının tanımı yapılmıştır. Buna göre ilgili kişinin rızası ile kişinin kendisine ait verilerin işlenmesinin kabulüne dair, ilgilinin bilgilendirilmesi yapıldıktan sonra özgür iradesiyle verdiği rıza kastedilmektedir. Direktif’in 7/a maddesi kapsamında da ilgili kişinin açık, net ve kesin bir biçimde, yani tereddüde yer bırakmayacak şekilde rızasını beyan etmesi gerektiği belirtilmiştir. 6698 sayılı Kanun m. 5 /f. 1’de ise ilgilinin açık rızasının olması gerektiği düzenlenmiştir. Madde kapsamında rızaya ilişkin düzenleme dar kapsamlı görünse de rızanın açık olmasıyla kastedilen tereddüde yer bırakmayacak bir rıza beyanının varlığı arandığı anlaşılmaktadır⁹². Rızanın açık olması arandığı için zımnen verilmiş rıza kabul edilmeyecektir. Diğer yandan ilgili kişi tarafından, hakkında veri işlenmesine objektif olarak rıza gösterme kabul edilebilecek ve karşı taraf açısından da bu şekilde anlaşılabilir, dışa vurulmuş davranışlar geçerli rıza kabul edilebilecektir⁹³.

Rızanın ne şekilde açıklanacağına dair ilgili düzenlemelerde bir hükme yer verilmemiştir. Dolayısıyla rıza açıklamasının yazılı veya sözlü olması mümkündür⁹⁴. Ayrıca rıza açıklamasının ne zaman yapılacağı hususunda da bir düzenleme yoktur. Rıza beyanının veri işleme işlemi başlamadan verilmesi gerekir. Zira ilgili madde metinlerinden de anlaşılacağı üzere rıza olmaksızın yapılacak veri işlemesi hukuka aykırı olacaktır. Bu anlamda ilgili kişinin, hakkındaki veri işleme işlemine daha

⁹⁰ 95/46/AT sayılı Direktif m. 7/1-a, OECD İlkeler m. 7 ve 6698 sayılı KVKK m. 5/f. 1

⁹¹ Murat Uygun, *Avrupa Birliği’nin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması* (Yayınlanmamış Yüksek Lisans Tezi), Ankara 2010, 56 vd.

⁹² KVKK 5. madde gerekçesi.

⁹³ Başalp, 39

⁹⁴ Alman Veri Koruma Kanunu (BDSG) m. 4a’da rıza beyanının yazılı olması gerektiği hüküm altına alınmıştır.

sonradan onay vermesi, bu eylemi hukuka uygun hale getirmeyecektir⁹⁵. 2.3.1. başlığı altında yaptığımız açıklamalarda da belirttiğimiz üzere sonradan verilen rıza hukuka aykırılığı ortadan kaldırmayacaktır. Bu durumda sonradan verilen bu rıza, rızanın verildiği zamandan sonraki veri işleme faaliyetlerine dair gösterilmiş bir rıza olabileceği kabul edilebilir⁹⁶. Son olarak belirtmek gerekir ki ilgilinin verilerinin işlenmesinden önce, veri işlenmesi ve sonuçları hakkında bilgilendirilmesi gerekmektedir. Kişi, bu aydınlatma neticesinde hem ne için rıza beyanında bulunduğunu bilecek hem de verdiği bu beyan sağlıklı bir rıza beyanı olacaktır.

1.2.4.3.2. Sözleşmenin İfası ve Sözleşme Öncesi Önlem Alınması

Bir sözleşmenin yerine getirilebilmesi ya da sözleşmenin kurulmasından önce önlem alınması için taraflara ait kişisel verilerin işlenmesi söz konusu olabilecektir. Bu durumlarda sözleşmeye ilişkin yapılan kişisel verilerin işlenmesine tarafların rızalarının var olduğu kabul edilmekte ve dolayısıyla yapılan veri işleme eylemi de hukuka uygun olmaktadır.

95/46/AT sayılı Direktif m.7/1-b ile 6698 sayılı Kanun m. 5/f. 2 - b. (c) benzer hükümlere yer vermişlerdir. Ancak Kanun’umuzda işlenecek olan verilerin, taraflar arasındaki sözleşmenin kurulması ve yerine getirilmesi ile doğrudan doğruya ilgili olması gerektiği ayrıca belirtilmiştir. Buna göre taraflar arasında ileride bir sözleşme imzalanma ihtimaline binaen taraflara ait veriler işlenemeyecektir. Aksi halde ilgili kişinin verilerin işlenmesine rızasının olmadığı kabul edilecektir ki bu hukuka aykırı bir durum olacaktır.

1.2.4.3.3. Kanuni Yükümlülüklerin Yerine Getirilmesi

6698 sayılı Kanun m. 5/ f. 2- b. (ç) hükmüne göre kişisel verileri işleme hususunda kanunen yükümlü bulunan kişiler, veri işleme faaliyetini ilgili kanunların hükümleri gereğince yapmaları, bu faaliyetlerinin hukuka uygun kabul edilmesinin gereğidir. Bu duruma örnek olarak İş Kanunu m. 75 gösterilebilir. Bu kanun hükmüne göre işverenler, çalıştırdıkları her işçi için bir özlük dosyası tutmak zorundalardır. Bu

⁹⁵ Şimşek, 107

⁹⁶ Şimşek, 107

özlük dosyası içerisinde işçiye ait kimlik bilgisi, adli sicil kaydı, sağlık raporu gibi kişisel veriler yer almaktadır⁹⁷. Benzer şekilde bir şirketin çalışanına maaş ödeyebilmesi için, banka hesap numarası, evli olup olmadığı, bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı, sosyal sigorta numarası gibi verileri işlemesi, bu bent hükmü gereğince istisnai olarak yapılabilecektir⁹⁸.

1.2.4.3.4. İlgili Kişinin Hayati Menfaatlerinin Korunması

Direktif m. 7/d' de veri öznesinin hayati menfaatlerinin korunması açısından gerekli olduğunda kişisel veriler işlenebileceği düzenlenmiştir. Ancak hayati menfaat kavramının ne olduğu veya bu kavramın kapsamına ilişkin her hangi bir düzenlemeye yer verilmemiştir. Benzer düzenlemeye Kanun m. 5/f. 2-b. (b)' de yer verilmiştir ve kanun gerekçesinde, hangi hallerin hükmün lafzında belirtilen durumlar kapsamında değerlendirilebileceği örnek kabilinde ortaya konulmuştur. Buna göre ilgili kişi fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumdaysa veya rızası hukuken geçerli kabul edilemeyecek nitelikte ise, kendisinin veya bir başkasının hayatını veya vücut bütünlüğünü korumak amacıyla kişisel verilerin işlenebilmesi mümkün olabilecektir. Madde lafzında belirtilen durumlara örnek olmak üzere kişinin şuurunun yerinde olmaması veya akıl hastası olması nedeniyle rızasının geçerli olmadığı bir durumda, hayat veya vücut bütünlüğünün korunması amacıyla, tıbbi müdahale yapılması sırasında kişisel verileri işlenebilecektir. Bu kapsamda örneğin kişinin kan gurubu, geçirdiği hastalıklar veya ameliyatlar, kullandığı ilaçlar gibi kişisel verileri işlenebilecektir. Yine hürriyeti elinden alınmış bir kişinin kurtarılması için kendisinin veya başkasının ya da şüphelinin yanında bulundurduğu telefon, kredi kartı, banka kartı ya da diğer teknik bir araç üzerinden yerinin belirlenmesi için kişisel verilerin işlenmesi, açık rıza olmasa da işlenebilecektir⁹⁹.

1.2.4.3.5. Kamu Yararı veya Kamu Görevinin Yerine Getirilmesi

Direktif m. 7/e ile 2008 tarihli KVKK m. 6/f. 3- b. (a) benzer düzenlemeler içermektedirler. Bu hükümlere göre kişisel verileri işleyecek kamu organları, veri

⁹⁷ Başalp, 41

⁹⁸ Bkz. KVKK m. 5/ f. 2- b. (ç) gerekçesi

⁹⁹ Bkz. KVKK m. 5 gerekçesi

işleme hususunda kanunen yetkili olmalıdırlar. Ayrıca verilerin işlenmesi kamu yararı için gerekli ise mümkün olabilecektir¹⁰⁰. İlgili düzenlemelerde bahsi geçen kamu yararı kavramından ne anlaşılması gerektiği belirtilmemiştir. Diğer bir ifadeyle kamu yararı kavramı oldukça geniş kapsamlı bir kavram olup sınırları belirlenmemiştir. Kişisel verilerin işlenmesinde kamu yararı kavramının geniş yorumlanabilmesi ve sınırlarının belirlenmemiş olmasından dolayı, veri işlenmenin yapılamayacağı bir durumun, kamu yararı kavramına dâhil edilerek işlenmesi tehlikesi ile karşılaşma ihtimali bulunmaktadır¹⁰¹. Ancak belirtmek gerekir ki veri hukukunda, kişisel verilerin işlenememesi kural, ilgilinin rızası veya yasal yetkinin varlığı halinde ise verilerin istisnai olarak işlenmesi durumu söz konusudur¹⁰². Burada veriyi işleyecek olan yetkilinin kamu kurumu olması sonucu değiştirmemektedir.

Direktif'in bu hükmüne 6698 sayılı KVKK'da karşılık gelen düzenleme, 5. maddenin ikinci fıkrasının a bendidir. Hükmün lafzından kişisel verilerin, kanunlarda açıkça öngörülmesi halinde açık rıza beyanı olmaksızın işlenebileceği anlaşılmaktadır. Kanun'nun madde metninde, Direktif ve Tasarı'daki düzenlemelerde yer alan "*kamu yararı*" ve "*resmi olarak verilmiş bir görevin yerine getirilmesi amacıyla veri işlenebilmesi*" ifadeleri çıkarılarak sade bir düzenlemeye yer verilmiştir. Buradan, kanunlarda öngörülen hallerde veri işlemesi yapılırken artık kamu menfaatinin gözetilmeyeceği sonucu çıkarılmamalıdır. Zira Kanun'nun bu hükmü kapsamında olmak üzere, kolluk kuvvetleri tarafında bir suç soruşturması sebebiyle şüphelilerin parmak izlerinin alınması, kişilerin ceza mahkûmiyetlerine ilişkin adli sicil kayıtlarındaki verilerin edinilmesi gibi durumlarda¹⁰³, açık rıza olmaksızın yapılacak olan kişisel veri işlemesi şüphesiz ki kamu yararına yönelik bir faaliyet ya da resmi olarak verilmiş bir görevin yerine getirilmesi olarak değerlendirilebilecektir.

1.2.4.3.6. Haklı Çıkarların Korunması

Bu hukuka uygunluk sebebi de hem Direktif m. 7/f hem de 6698 sayılı KVKK m. 5/f. 2- b. (f)'de benzer şekilde düzenlemiştir. Buna göre verileri işlemeye yetki kişilerin haklı çıkarları için ilgili kişiye ait kişisel veriler işlenebilecektir. Ancak verilerin bu

¹⁰⁰ Başalp, 41

¹⁰¹ Ersoy, 106

¹⁰² Şimşek, 107

¹⁰³ Bkz. KVKK m. 5 gerekçesi

şekilde işlenmesi, ilgilinin temel hak ve özgürlüklerine ve aynı zamanda meşru çıkarlarına bir zarar vermemesi şartı ile mümkün olabilecektir. 6698 sayılı Kanun hükmünde, ilgilinin sadece temel hak ve özgürlüklerine aykırı olmaması düzenlenmişken, 2008 tarihli Tasarı'da buna ek olarak veri işleminin ilgilinin meşru çıkarlarına da aykırı olmaması gerektiği hüküm altına alınmıştı. Dikkat edilirse hem verileri işleyen hem de verileri işlenen ilgili kişinin haklı, diğer deyişle meşru çıkarları söz konusudur. Bu noktada hukuki düzenlemelerde verileri işleyenler ile verileri işlenen kişilerin çıkar dengelerinin sağlanması durumu söz konusudur¹⁰⁴. Buna göre de verileri işlemeye yetkili olanların haklı çıkarları, ilgili kişinin verilerinin işlenmesini gerektiriyorsa, yapılacak olan verilerin işlenmesi faaliyeti hukuka uygun olacaktır.

Yukarıdaki açıklamalar altında bir şirket sahibinin, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, işçilerinin terfileri, maaş zamları ya da sosyal haklarını düzenlenmesinde veya işletmenin yeniden yapılandırılması sürecinde görev ve rol dağıtımında esas alınmak üzere işçilerin kişisel verilerini işleyebilecektir. Burada, işletmenin yeniden yapılandırılması ya da ehliyetli ve liyakatli çalışanların terfi almaları, veri sorunlusu statüsündeki şirket sahibinin meşru menfaati kapsamında ileri gelmektedir¹⁰⁵.

1.2.4.3.7. Herkesçe Bilinen Verilerin İşlenmesi

Bu hukuka uygunluk sebebi Direktif'te düzenlenmemiş, 6698 sayılı Kanun m. 5/f. 2-b. (d) hükmünde düzenlenmiştir. Bu hüküm gereğince, kişisel veriler, ilgilisi tarafından alenileştirilmiş ise bu verilerin işlenmesi hukuka uygun olacaktır. Bu kapsamda yer alan veriler artık herkes tarafından bilinebilecek nitelikte veri haline gelmiş olacaktır. Burada belirtmek gerekir ki bu hale gelmiş olan verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir¹⁰⁶. Diğer yandan kişisel verilerin ilgilisi tarafından alenileştirilmesi, veri sahibinin bu verilerin herkes tarafından işlenebilme ihtimalinin de bilincinde olmasından hareketle, bu verilerin işlenmesine dair rızasının var olduğu da düşünülebilir.

¹⁰⁴ Başalp, 41

¹⁰⁵ Bkz. KVKK m. 5 gerekçesi

¹⁰⁶ Bkz. KVKK m. 5 gerekçesi

Madde metninde kişisel verilerin alenileştirilmesinin ne şekilde yapılacağına dair bir açıklık olmamakla birlikte madde gerekçesinden hareketle bu kavramdan, ilgilisinin kendisine ait kişisel verileri kamuoyuna açıklaması anlaşılabilir¹⁰⁷. Zira 2.3.5. numaralı başlık altında yapılan açıklamalara paralel şekilde, ilgili kişi tarafından yapılacak veri açıklaması, ilgilisi tarafından ancak kamuya yönelik olarak yapılan veri açıklaması olacaktır. 2008 tarihli KVKK m.6/f. 3-b. (ç)’de düzenlenen bir diğer durum açık sicillerde yer alan bilgilerdir. Tasarının bu kısmı Kanun hükmüne dâhil edilmemiştir. Bu sicillerin kamuya açık olması neticesinde burada kayıtlı bilgilere herkesin ulaşabilmesi veya bu bilgilerin herkesçe öğrenilmesi halin icabı olup yine burada da korunması gereken hukuki yararın ortadan kalktığı, dolayısıyla böyle bir durumda bu tir sicillerde yer alan kişisel verilerin de açık rıza olmadan işlenebileceği savunulabilir.

1.2.4.3.8. Verilerin Anonim Hale Getirilerek İşlenmesi

Kişisel verilerin anonim hale getirilmek suretiyle işlenmesi, Kanun’da kişisel verilerin işlenmesini düzenleyen madde içerisinde yer almamakla birlikte, kişisel verilerin hukuka uygun olarak işlenmesine imkân veren bir durum olması münasebetiyle bu kısım altında ele alınmıştır.

Kişisel verilerin anonim hale getirilerek işlenmesinden önce anonimleştirme ifadesinden ne anlaşılması gerektiğine değinmekte yarar vardır. Anonimleştirme, kişiye ilişkin verilerin içeriğinin saklı kalması, diğer bir ifadeyle kişisel verilerin, kişiye ilişkin olduğuna dair bir açıklama yapılmaksızın verilerin saklı tutulmasıdır¹⁰⁸. 6698 sayılı Kanun m. 3/f. 1- b.(b)’de de verilerin anonim hale getirilmesi düzenlenmiştir. Buna göre anonim hale getirme, “*Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder.*” şeklinde tanımlanmıştır. Artık anonim hale gelmiş olan bir veri, ait olduğu kişiyi belirlemeye elverişli olamayacaktır. Diğer bir ifadeyle kişi ile veri arasında bağlantı kurulamayacaktır. Zira bu veriler artık kişi bazında kullanılmamaktadır¹⁰⁹. Bu veriler, kişisel veri olarak değil, “anonim veri” olarak

¹⁰⁷ Bkz. KVKK m. 5 gerekçesi

¹⁰⁸ Weihert, Däubler, Klebe, Wedde, 131

¹⁰⁹ Weihert, Däubler, Klebe, Wedde, 131

adlandırılacaklardır ve kişisel veri olma niteliklerini de kaybedeceklerdir¹¹⁰. Bu duruma bağlı olarak veriyi elinde bulunduran tarafından veri paylaşımı durumunda, paylaşılan veriden ilgilisi tespit edilebiliyorsa ya da veri ile bir kişi arasında bağlantı olduğu iddia edilmesi durumunda, kişisel veriyi anonimleştirerek kullanan yetkili makam ya da kişi bu verinin anonimleştirilmiş bir veri olduğunu ispat etmekle yükümlü olacaktır¹¹¹.

Kişisel verinin tanımı dikkate alındığında, veri öznesinin temel hak ve özgürlüklerinin ihlali açısından önem taşıyan kişisel veriler, anonimleştirilmeleri neticesinde kime ait oldukları belli olamayacağından, işlenmeleri durumunda hak ihlali de söz konusu olamayacaktır¹¹².

Anonim hale getirilmiş ya da anonimleştirilmiş olan kişisel veriler, çeşitli amaçlar için işlenebilecektir. Bu amaçlar m.28/f.1-b. (b)' de araştırma, planlama ve istatistik şeklinde açıkça belirtilmiş olmakla birlikte madde hükmü içerisinde sayılanlarla sınırlı değildir. Madde metnindeki "...gibi amaçlarla..." ifadesinden, belirtilen araştırma, planlama ve istatistiki amaçla işlemler yanında başka amaçlara hizmet için de işleme yapılabileceği açıkça anlaşılmaktadır.

Kanun'un bu hükmü gereğince verilerin anonimleştirilerek işlenmesi, kişisel verilerin işlenmesinde hukuka uygunluk sebebi olarak kabul edilebilecek bir durumdur. Madde hükmüne göre kişisel veriler, araştırma, planlama ve istatistik gibi amaçlarla, ancak anonim hale getirilmesi şartıyla işlenebileceklerdir ve m. 28'de belirtilen kişisel verilerin işlenmesi halleri, Kanun kapsamı dışında bırakılmış istisnai durumdur. Diğer ifadeyle Kanun hükümleri, 28. maddede sayılan kişisel veri işleme hallerine uygulanmayacaktır. Bu suretle de elde edilen verilerin ve sonuçların üçüncü kişilere aktarılması ve yayılması mümkün olabilecektir.

¹¹⁰ Ersoy, 17

¹¹¹ Weihert, Däubler, Klebe, Wedde, 131

¹¹² Ersoy, 17

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN SAKLANMASI, GÜVENLİĞİ ve KORUNMASI

2.1. KİŞİSEL VERİLERİN SAKLANMASI ve VERİLERİN GÜVENLİĞİ

2.1.1. Kişisel Verilerin Saklanması

Kişisel verilerin korunması ile amaç, daha önce de sözü edildiği üzere, bireyin temel hak ve özgürlüklerinin korunmasıdır. Bu bağlamda da bireyin özel hayatının gizliliği ön plana çıkmaktadır. Burada özel hayatın gizliliği hususunun iki önemli noktası söz konusudur. Birincisi özel hayatın gizliliğinin arz ettiği önem, ikincisi ise kamusal veya özel faaliyetlerin sürdürülebilmesi için kişisel verilerin işlenmesinin mecburiyetidir. Bu iki durumun bir arada bulunması dolayısıyla özel hayatın gizliliğinin mutlak olarak korunması yönündeki ifadeler her zaman geçerli olamayacaktır. Bu doğrultuda kişisel verilerin işlenmesine dair faaliyetlerin artması durumu verilerin saklanması ve güvenliği sorunlarını da beraberinde getirmektedir¹¹³.

Kişisel verilerin saklanmasından, ilgili kişiye ait kişisel verilerin yetkili kişilerce işlenmiş ya da işlenmek üzere ellerinde bulunan verilerin hukuka aykırı olarak üçüncü kişilerin ellerine geçmemesi veya üçüncü kişilerin yine hukuka aykırı şekilde bu verilere ulaşmaması için muhafaza edilmesi anlaşılmaktadır. Yani kişisel verileri usulünce elinde bulunduranların, bu verilerin gizliliğini sağlamaları gerekmektedir¹¹⁴. Bu anlamda kişisel verilerin saklanması ve gizliliği, veri koruma hukuku açısından son derece önemli ve gerekli bir konudur.

Kişisel verilerin saklanması, bu verilerin özünde ilgilisinin temel hak ve özgürlüklerine ilişkin bilgiler olması, buna bağlı olarak da hukuka aykırı şekilde üçüncü kişilerin bu verilere ulaşmaları, verileri ellerinde bulundurmaları veya yaymaları ihtimalleri karşısında ilgili kişi, sürekli bir tehdit altında bulunabileceğinden dolayı önem arz etmektedir. Diğer yandan bu verilerin en temel haklara yönelik olması nedeniyle bu hakların korunması ve ilgili kişinin bahsedildiği üzere tehditle

¹¹³ Muammer Ketizmen, Çağlar Ülküderner, *E-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması*, Erişim Tarihi: 20.04.2014, <http://inet-tr.org.tr/inetconf12/bildiri/2.pdf>.

¹¹⁴ Muammer Ketizmen, Çağlar Ülküderner, *E-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması*, Erişim Tarihi: 20.04.2014, <http://inet-tr.org.tr/inetconf12/bildiri/2.pdf>.

karşılaşmaması için de verilerin saklanması gereklilik arz etmektedir¹¹⁵. Ancak belirtmek gerekir ki, kişisel verilerin gizliliğini sağlamak her geçen gün daha da zorlaşmaktadır. Teknolojinin hızlı gelişmesi ve günlük yaşamın içerisine girmesiyle birlikte hem özel hem de kamu kesimin faaliyetlerini bu teknoloji, özellikle de bilgisayar ile birlikte sürdürmesine imkân tanımıştır. Bilgilerin bilgisayar ortamında muhafazasının olumlu tarafları yanında olumsuz tarafları da vardır. Olumlu tarafları olarak, bilgilerin eski usullere göre çok daha az bir alanda tutulmasının mümkün olması söylenebilir. Örneğin birkaç arşivde var olan belgelerin bir bilgisayar içinde muhafazası mümkündür. Ayrıca istenilen bilgiye de artık çok daha hızlı bir şekilde ulaşılmaktadır. Ancak bilgi güvenliği açısından bilgisayarlara uzaktan erişimin söz konusu olması önemli bir olumsuzluk olarak karşımıza çıkmaktadır. Zira bu durum ile bilgisayar ortamında yer alan kişisel veriler, ilgisinin rızası olmaksızın her an yetkisiz kişilerce ulaşılabilme, ifşa edilme, elektronik ortamlarda ilgilisi adına sahte işlemler yapılması gibi tehlike ve tehditlerle karşı karşıyadır¹¹⁶. Bu noktada kişisel verilerin saklanması, diğer ifadeyle verilerin gizliliğinin sağlanması gerekmektedir.

2.1.1.1. Kişisel Verilerin Saklanma Süresi

Kişisel verilerin, bu verileri toplayanların himayesi altında ne kadar süre ile bulundurulacağına ya da bulundurulması gerektiğine dair hukuki metinlerde düzenlemelere yer verilmiş olmakla birlikte, bu düzenlemelerin hiç birinde net bir süre belirlemesi yapılmamıştır. 95/46/AT sayılı Direktif m. 6/f. 1- b. (e)’de bu süre “*verilerin toplandığı veya sonrasında işlendiği amaçlar için gerekenden daha uzun olmayan süre boyunca...*” denilmek suretiyle belirlenen amaca ulaşma bakımından geçecek olan süre, kişisel verilerin saklanması bakımından makul kabul edilecektir. Bu hükmün yansıması olarak 6698 sayılı Kanun m. 4/f. 2- b. (d)’de de kişisel verilerin işlendikleri amaç için gerekli olan süre kadar elde bulundurulabileceği ifade edilmiştir. Amaca ulaşılmasına rağmen kişisel verilerin elde bulundurulmasına devam edilmesi, durumu hukuka aykırı hale getirecektir¹¹⁷. Ancak belirtmek gerekir ki kişisel verilerin işlenmesindeki amacın

¹¹⁵ Engin Dinç, *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye’nin Durumu* (Yayınlanmamış Yüksek Lisans Tezi), Diyarbakır 2006, 16-17

¹¹⁶ Eren Ersoy, *Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması*, 2, Erişim Tarihi: 05.01.2014, <http://ab.org.tr/ab06/bildiri/6.doc>.

¹¹⁷ Başalp, 39.

gerçekleşmiş olmasına rağmen kişisel verileri elde tutmaya, diğer bir ifadeyle saklamaya devam etmeye izin veren bir durum söz konusudur. Direktif m.6/f. 1- b. € hükmünün ikinci cümlesinde belirtilmiş olan tarihsel, istatistiksel veya bilimsel kullanım amaçları için uygun koruma önlemleri alınmak suretiyle kişisel veriler daha uzun süreli olarak muhafaza edilebilirler. Yani ancak kişilerin teşhisine olanak vermeyecek şekilde muhafaza edilmeleri söz konusu olabilecektir¹¹⁸. Aynı şekilde Kanun m. 7’de kişisel verilerin anonim hale getirilmesi düzenlenmiştir. Bu hükme göre bu Kanun veya diğer kanun hükümlerine uygun olarak kişisel veriler işlenmiş olsa da, veri işlenmesini gerektiren sebebin ortadan kalkması durumunda kişisel veriler resen veya ilgilinin talebi üzerine veri sorunlusu tarafından ya silinecek ya yok edilecek ya da anonim hale getirilecektir. 7. maddeden anlaşıldığı üzere kişisel verilerin elde bulundurulması bakımından net bir süre olmayıp bu süre veri işleme amacının gerçekleşmiş olmasına veya veri işleme sebebinin ortadan kalkmasına kadar geçecek süredir. Burada anonimleştirilmiş olan veriler, kişilerin teşhisine imkân tanımayacağından, bu verileri elinde bulunduranlar için daha uzun süreli muhafaza edilme noktasında sorumluluk gerektirecek bir durum da söz konusu olmayacaktır¹¹⁹.

2.1.1.2. Kişisel Verilerin Daha Sonra İşlenme İhtimali ile Saklanıp Saklanamayacağı Meselesi

Kişisel verilerin, hali hazırda saklı tutularak ihtiyaç duyulması halinde işlenmesi anlayışı söz konusu olabilir. Bu durumun mümkün olup olamayacağına dair açık bir düzenleme olmamakla birlikte, kişisel verilerin işlenmesinde var olan ilkelerden yola çıkılarak durum hakkında bir kanıya varılabilir.

İlk olarak kişisel verilerin işlenmesinde geçerli olan amaca bağlılık ilkesi gereğince kişisel veriler, önceden belli olan meşru amaç dâhilinde toplanabilir, işlenebilir veya muhafaza edilebilirler. Kişisel verilerin elde bulundurulması dahi başlı başına bir risk oluşturmaktayken, veri işleme amacı gerçekleştikten sonra verilerin elde bulundurulmasına devam edilmesi halinde bu risk de varlığını devam ettirecektir. Zira bu ilkenin varlığı ile bir kişinin bir kez verilerinin edinilmesi ile hayatı boyunca bu verilerinin bir yerde kayıtlı bulunacağı ve “*yeri geldiği zaman*” kullanılabileceği

¹¹⁸ Küzeci, 209.

¹¹⁹ Anonimleştirme ile ilgili olarak bkz. s. 36 vd.

düşüncesi ortadan kalkmış olacaktır¹²⁰. Aksi halde böyle bir ortamda veri koruma hukukunun temelinde yer alan, bireyin temel hak ve özgürlüklerinin korunması ki özellikle özel hayatın gizliliği, bireyin maddi ve manevi bütünlüğü, ihlal edilme tehlikesi altında kalacaktır¹²¹. Diğer yandan kişisel verilerin işlenmesi ile amaç arasında nedensellik bağının devam etmesi, yani sona ermemiş olması gerekir. Veri işleme ile amaç arasındaki nedensellik bağı, belirlenen amacın ortadan kalkması, kişisel veri işlemenin amaca ulaşmak açısından gereksiz hale gelmesi veya amaca ulaşılmış olması şekillerinde olabilir¹²². Bu durumda artık meşru bir amaç da ortada olmayacağından dolayı ya da o amaç için eldeki verilerin bir hükmü olamayacağından, kişisel verilerin muhafaza edilmelerini meşru hale getirecek hal de sona ermiş olacaktır. Bu durum karşısında Avrupa sisteminde verilere gerek kalmadığı takdirde bu veriler ya anonimleştirilerek saklanacak ya da ortadan kaldırılacaklardır¹²³. Bu doğrultuda verilerin ileride ihtiyaç halinde işleme ihtimallerine dayanarak saklanmasına yer olmayacağı anlaşılmaktadır¹²⁴.

Direktif m. 6/f. 1- b. (b), (c) hükümlerinde varlığını bulan gereklilik ilkesine göre toplanan veriler yalnızca önceden belli olan meşru amaç için gerekli ve önemli olmaları halinde işlenebileceklerdir¹²⁵. Bu ilkenin bir uzantısı olarak görülen depolama yasağına göre de öngörülen amacı, ilerleyen zamanlarda gerçekleştirebilecek verilerin depolanmasının yasaklanması, yani verilerin ileride muhtemel kullanılma durumuna dair erkenden toplanması mümkün olamayacaktır¹²⁶.

Konu ile bağlantılı diğer bir durum ise kişisel verilerin saklanma süresidir. Kanun m. 4/f. 2- b. (d) ve Direktif m. 6/f. 1- b. € hükümleri gereğince kişisel veriler, işlendikleri amaç için gerekli olan süreden daha fazla muhafaza edilemeyeceklerdir. Mevcut amaç için toplanmış olan veriler, amaç gerçekleştikten sonra artık muhafaza edilemeyecektir. Zira mevcut verilerin ileride hangi amaç için yeniden kullanılacağı belirsizdir. Bu durum ayrıca bireye, kişisel verilerinin toplanma amacı dışında başka bir

¹²⁰ Küzeci, 210

¹²¹ Küzeci, 210

¹²² Küzeci, 210

¹²³ Küzeci, 210

¹²⁴ Şimşek, 84

¹²⁵ Şimşek, 84; Başalp, 38

¹²⁶ Başalp, 38

amaç için işlenmeyeceğine dair bir güvence de vermeyecek, veri sahibi kişi açısından temel hak ve özgürlüklerin ihlali tehlikesi ortadan kalkmamış olacaktır.¹²⁷

2.1.2. Kişisel Verilerin Güvenliği

Kişisel verilerin güvenliği, veri koruma hukuku açısından oldukça önemlidir. Güvenlik duygusunun, günümüzün önemli sorunlarından biri olması bu önemi ortaya koymaktadır. Güvenlik sorunu, yalnızca bilgi ve iletişim teknolojileri açısından değil, kamu ve özel sektör kapsamında faaliyette bulunan kimseler tarafından endişe duyulan ortak bir sorundur. Kişisel verilerin korunması üzerine yürütülmekte olan tüm çalışmaların temelinde sistem ve cihazlar arasındaki uyumlu çalışmasının sağlanması yanında veri güvenliğinin sağlanabilmesi ön planda tutulmaktadır. Bu anlamda güvenliğin sağlanması kapsamında kişisel ve kurumsal güvenliğin yanında iletişim ağı güvenliği, iletişim sistem güvenliği, veri tabanı güvenliği, erişim güvenliği gibi güvenlik boyutları da yer almaktadır¹²⁸.

Burada belirtmelidir ki, kişisel verilerin güvenliği ile kişisel verilerin korunması anlam itibari ile aynı değildirler. Zira ilk durumda amaç bizzat kişisel verinin kendisini korumak iken, ikinci durumda kişisel veriler, güvenli ortamlarda muhafaza edilmek suretiyle, aksi ile ifade etmek gerekirse bu verilere hukuka aykırı olarak erişimin önlenmesiyle ilgili kişinin temel hak ve özgürlüklerinin korunması amaç edinilmiştir. Bu durumun devamı olarak da kişisel verilerin korunması ile verilerin güvenliği arasında bir amaç – araç ilişkisi olduğu söylenebilir¹²⁹. Benzer şekildeki açıklamalara Alman Hukukunda da yer verilmiştir. Alman Veri Koruma Kanunu m.1’de veri korumanın amacı; bireylerin kendilerine ait verilerin kullanımı esnasında, kişilik haklarının ihlaline karşı bir koruma sağlamak olduğu belirtilmişken, veri güvenliğinde, verilerin güvenli bir şekilde depolanması, aktarılması ve verilere güvenli bir şekilde ulaşılmasına ilişkin bir bütünlüğün söz konusu olması ön plandadır. Veri güvenliği ile ilgili esas düzenleme Federal Alman Veri Koruma Kanunu (BDSG) Teknik ve

¹²⁷ Şimşek, 85

¹²⁸ Köksal Özenç, *Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması*, 198, Erişim Tarihi: 5.1.2014, <http://www.iscturkey.org/s/2226/i/2007-26.pdf>

¹²⁹ Küzeci, 242; Şimşek, 95

Organizasyona ilişkin önlemler başlıklı 9. maddede düzenlenmiştir¹³⁰. Zira olası tehditlere karşı verilerin güvenliği sağlanarak kişinin temel haklarına gelebilecek müdahale önlenmiş, kişisel verilerin korunmasındaki amaç da gerçekleşmiş olacaktır.

İsviçre Veri Koruma Kanunu (DSG), 7. maddesinde veri güvenliğini, kişiye ilişkin bilgilerin makul teknik ve organizasyona ilişkin önlemler yoluyla, yetkisi olmaksızın işlemeye karşı korunması olarak düzenlemiştir. Maddenin ikinci fıkrasında Meclisin veri güvenliğine ilişkin asgari şartlara dair daha detaylı düzenlemeler yapabileceği, ayrıntıların Federal Konsey tarafından düzenlenebileceği de belirtilmiştir. Kanunun ilgili maddesinde verilerin güvenliği ile ilgili temel düzenlemenin doğrudan amacı kişiye ilişkin verilerin bilgi olarak korunduğu, dolaylı olarak bu koruma normu, Kanunun (DSG) tamamında olduğu gibi ilgili kişinin kişiliğinin de korunmasına da hizmet etmekte olduğu ifade edilmiştir. Nihai olarak verilerin korunması ve verilerin güvence altına alınması birbirinden ayrılmaksızın bağlantılı olarak bulunduğu, verilerin güvenliğinin, kişisel verilerin korunması bakımından temel bir element olduğu belirtilmiştir¹³¹. Ancak İsviçre doktrininde, kişisel verileri işleyen özel kişi veya devlet organlarının yükümlülüklerinin çok geniş şekilde ve belirsiz hukuki kavramlar kullanılarak tanımlandığı, kişisel verilerin güvenliğinin nasıl sağlanması gerektiğinin anlamının ancak yorum yoluyla çıkarılabileceği yönünde eleştiriler mevcuttur¹³².

Verilerin güvenliğine dair 108 sayılı Avrupa Sözleşmesi m. 7, 95/46/AT sayılı Direktif m. 17, OECD İlkeler m. 11’de düzenlemelere yer verilmiştir. Bu çerçevede 108 sayılı Avrupa Sözleşmesi’nde verileri korumak için bu verilerin kazaen veya izinsiz olarak imhasına, kaybolmasına, hukuka aykırı olarak elde edilmesine, değiştirilmesine ya da izinsiz olarak dağıtılmasına karşı uygun önlemlerin alınmasının zorunlu olduğu düzenlenmiştir. 95/46/AT sayılı Direktif’te daha ayrıntılı bir düzenleme yer almaktadır. Buna göre üye devletler, özellikle veri işlemenin bir ağ üzerinden iletilmesi durumunda ve işlemenin diğer yasa dışı tüm şekillerine karşı, yetkisiz açıklama veya erişim, değiştirme, kazara kayıp veya kazara ya da hukuka aykırı olarak tahrip edilmesine karşı uygun teknik ve kurumsal tedbirlerin alınması gerektiği belirtilmiştir. Alınacak olan bu

¹³⁰ Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri, *Einführung in Das Datenschutzrecht*, Oldenbourg Verlag, München 2012, 239

¹³¹ Christa Stamm – Pfister, (Editör: Maurer – Lambrou Blechta), *Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz*, 3. Auflage, Helbing Lichtenhahn Verlag, 2014 Basel, Art. 7 DSG, 182 - 183, N. 1-2

¹³² Christa Stamm – Pfister, Art. 7 DSG, 184, N. 7.

tedbirlerin, verinin yapısına ve işlemeden dolayı meydana gelebilecek risklere uygun düzeyde güvenlik sağlaması gerekmektedir. Ayrıca Direktif, veri işleminin işleyici aracılığı ile yapılması durumunda verileri işleyecek olan görevlinin yalnızca denetleyiciden gelecek talimatlara göre hareket etmesini ve m. 17/1'deki yükümlülüklerle işleyicinin de tabi olmasını şart koşmuştur. OECD İlkelerinde de benzer düzenlemeye yer verilmiştir. Buna göre de kişisel verilerin kaybolması veya izinsiz erişim, tahribat, kullanım, değiştirme veya verilerin ifşası gibi risklere karşı makul güvenlik tedbirleriyle korunması gerektiği düzenlenmiştir. 108 sayılı Sözleşme ve 95/46/AT sayılı Direktif'te verilerin korunmasına yönelik uygun önlemlerin alınması gerektiği, OECD İlkelerinde ise makul önlemler ifadesi kullanılmıştır. Hukuki metinlerde kullanılan uygun ya da makul tedbirlerde asıl amaç yukarıda da belirtildiği üzere verilerin güvenliğinin sağlanması suretiyle veri sahibi ilgili kişinin temel haklarının korunmasıdır¹³³.

Uluslararası düzenlemeler haricinde bilgi güvenliğinin sağlanmasına yönelik dünya genelinde kabul gören şartlar da mevcuttur. Buna göre;

- Önemli ve hassas bilgilerin istenmeyen biçimde yetkisiz kişilerin eline geçmesi önlenmelidir ve sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğu garanti altına alınmalıdır (Confidentiality - Gizlilik).
- Bilginin, sahibi dışındaki kişilerce değiştirilmesinin ve silinmesinin önlenmesi gerekmektedir (Integrity - Bütünlük)
- Bilgi veya bilgi sistemleri sürekli kullanıma hazır ve kesintisiz çalışır durumda olmalıdır (Availability - Sürekli Kullanılabilirlik)
- Kullanıcı kimliğinin doğrulanması gerekmektedir (Authentication – Kimlik doğrulama)¹³⁴.

Verilerin güvenliğine dair yukarıda bahsedilen hususlar neticesinde, veri güvenliğinin sağlanabilmesi için teknolojik tedbirlerin yanında kurumsal tedbirlerin de alınması gerekmektedir. Teknik önlemlere, elektronik ortamda veya bilgisayar ortamında verilerin bulunduğu dosyaların şifreli olması, virüs programları, güvenlik

¹³³ Şimşek, 96

¹³⁴ Hasan Yılmaz, *TS ISO / IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi*, 46-47, Erişim Tarihi: 10.08.2016, <http://kidder.dergipark.gov.tr/download/article-file/208742>; Oldouz Karimi / Adem Korkmaz, *Kişisel Verilerin Korunması*, 8-9, Erişim Tarihi: 10.08.20, <http://inet-tr.org.tr/inetconf18/bildiri/63.pdf>.

duvarları gibi durumlar örnek olarak verilebilir¹³⁵. Ayrıca veri güvenliğinin sadece dışarıdan gelebilecek tehdit ve tehlikelerle ortadan kalkmayacağı, bunun yanında veri işleyenlerden kaynaklı olarak da güvenlik sorunları yaşanabileceği dikkate alınmalıdır. Bu açıdan veri işlemeye yetkili olan kişilerin mümkün olan en az düzeyde veriye ulaşmalarının sağlanması ve bu kişilerin yapmış oldukları faaliyetlerin denetlenmesi gerekmektedir¹³⁶. Bu noktadan hareketle, bilgi güvenliğinin, kişisel verileri işlemeye yetkili kurum ve kuruluşlarda, iş süreçlerinin bir parçası olduğu, bu anlamda iş anlayışı, yönetim ve kurumsal kültür olarak değerlendirilmesi gerekmektedir¹³⁷.

Yukarıda yapılan açıklamalarla aynı yönde, veri güvenliğinin sağlanmasına yönelik olmak üzere iç hukukumuzda 6698 sayılı KVKK'nın 12. Maddesinin birinci fıkrasında veri sorumlusunun yükümlülükleri düzenlenmiştir. Maddede, veri sorumlusunun; kişisel verilerin hukuka aykırı olarak işlenmesini, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve bu verilerin güvenliğini sağlamak amacıyla uygun güvenlik düzeyini sağlamak için gerekli her türlü teknik ve idari tedbirleri almakla yükümlü olduğu hüküm altına alınmıştır. Alınması gerekli olan bu teknik ve idari tedbirlerin neler olduğuna dair Kanun'da bir düzenlemeye yer verilmemiştir. Burada alınacak teknik tedbirler, kişisel verilerin kayıtlı bulunduğu ya da muhafaza edildiği elektronik ortamların güvenliğinin sağlanması ile birlikte bu verilere hukuka aykırı olarak erişimin engellenmesine yönelik alınacak olan tedbirlerdir.

İkinci fıkrada veri sorumlusunun, kişisel verilerin kendisi adına başka bir gerçek ya da tüzel kişi tarafından işlenmesi halinde, birinci fıkrada belirtilen tedbirlerin alınması noktasında bu kişilerle birlikte müştereken sorumlu olacağı düzenlenmiştir. Buna göre veri sorumlusu, şirketine ilişkin kayıtları bir muhasebe şirketine tutturuyorsa, verilerin işlenmesine ilişkin birinci fıkrada belirtilen tedbirlerin alınmasına ilişkin olarak muhasebe şirketi ile birlikte müştereken sorumlu olacaktır¹³⁸.

Veri güvenliğinin sağlanmasına yönelik olmak üzere maddenin üçüncü fıkrasında veri sorumlusunun, kendi kurum ve kuruluşunda, Kanun hükümlerinin uygulanmasını ve kişisel verilerin Kanunda öngörülen usul ve esaslara uygun olarak işlenmesini

¹³⁵ Özenç, 190

¹³⁶ Küzeci, 244

¹³⁷ Ersoy, 3

¹³⁸ Bkz. KVKK m. 12 gerekçesi.

sağlamak amacıyla gerekli denetimleri yapma veya yaptırma yetki ve yükümlülüğüne sahiptir.

Dördüncü fıkrada ise veri sorumlusuna ve verileri işleyenlere yönelik bir yasaklama durumu söz konusudur. Bu yasaklama, aslında veri sorumlusu ile veri işleyenlerin sır saklama yükümlülüğüdür¹³⁹. Buna göre veri sorumlusu ve verileri işleyenler, öğrendikleri kişisel verileri, Kanun'a aykırı olarak başkalarına açıklayamayacaklar ve mevcut veri işleme amacı dışında kullanamayacaklardır. Fıkranın son cümlesinde bu kişilerin görevlerinden ayrılmaları halinde de bu yükümlülüğün devam edeceği hükme bağlanmak suretiyle, veri güvenliğinin daha etkin olarak sağlanması amaçlanmıştır.

2.2. KİŞİSEL VERİLERİN KORUNMASI

2.2.1. Tarihsel Gelişim ve Verilerin Korunması İhtiyacı

Günümüzdeki anlamıyla kişisel verilerin korunmasına dair ilk tartışmalar 1960'lı yıllarda ABD'de başlamış, hukuki düzenlemeler ise 1970'li yıllarda yapılmıştır. Bilim ve teknoloji alanındaki hızlı gelişmeler karşısında hem kamu hem de özel sektörde hizmetlerin ve/veya faaliyetlerin planlanması ve sunulması da değişime uğramıştır. Bu anlamda kişisel veriler hem kamu hem de özel kesimin arşivlerinde kayıtlı bulunmaya başlamıştır. Kişisel verilerin hızla işlenmeye devam etmesi kişilik haklarının alanının daralmasına neden olmaya başlamış, özellikle de özel hayatın gizliliğinin ihlalini beraberinde getirmiştir. Ancak bu durum hukuki açıdan kabul edilebilir nitelikte değildir. Teknik ve bilimsel gelişmelerin insan hayatına katkıları ve sağladığı kolaylıklar inkâr edilemez bir gerçektir. Bu noktada kişilik haklarının ihlaline imkân vermeden, gerekli yasal düzenlemelerin yapılarak bu gelişmelerin insanlığın hizmetine sunulması gerekmektedir¹⁴⁰.

Kişisel verilerin korunması, özel hayatın gizliliği kapsamında değerlendirildiğinde¹⁴¹, kavramın varlığı oldukça eskilere dayanmaktadır. Bugünkü adıyla olmasa da bireyler, kendilerine ait bazı bilgilerin gizli kalmasını istemişlerdir.

¹³⁹ Bkz. KVKK m. 12 gerekçesi.

¹⁴⁰ Başalp, 23

¹⁴¹ Ersoy, 47

Bazı meslek guruplarında, meslek mensuplarının, kişilerin özel hayatlarına dair edinmiş oldukları bilgileri sır saklama kapsamında gizli tutma ve açıklamama yükümlülükleri vardır. Özellikle hekimlerin durumu buna örnek verilebilir. Sır saklama yükümlülüğü ile kendilerine güvenilerek bilgi verilen meslek mensupları, bu bilgileri gizli tutarak ilgililerin kişisel verilerinin korunması amaçlanmıştır. Ancak o zaman dahi bu hak mutlak olarak korunmamakta, zira kamu yararının gerekli kıldığı durumlarda bu bilgilerin açıklanabilmesi de mümkün olabilmektedir. Bugün için bu duruma örnek olarak 1593 sayılı Umumi Hıfzıssıhha Kanunu kapsamında hekimin bulaşıcı hastalıkları bildirme yükümlülüğü gösterilebilir¹⁴².

Özel hayatın gizliliğinin korunmasına yönelik İnsan Hakları Evrensel Beyannamesi m. 12, Avrupa İnsan Hakları Sözleşmesi m. 8, Avrupa Birliği Temel Haklar Şartı m. 7 uluslararası alandaki düzenlemelerdir. İç hukukumuzda da 1982 Anayasası'nın II. Bölümü, IV. Özel Hayatın Gizliliği ve Korunması başlığı altında 20. vd. maddelerinde ilgili düzenlemelere yer verilmiştir. Bu düzenlemeler, kişisel verilerin korunmasını dolaylı olarak sağlamaktadır. Bu düzenlemelerin kaleme alındığı dönemlerde kişisel verilerin korunması ayrı bir hak olarak ele alınmamıştı. Yukarıda da belirtildiği üzere kişisel verilerin korunmasının ayrı bir hak olarak hukuki düzenlemeler içerisinde yer alması yine bilim ve teknolojinin gelişimi ve bu gelişmelerin de kamu ve özel sektörde yoğun şekilde kullanılmasıyla ortaya çıkmıştır. Çağdaş toplumlarda bilgi, gücün simgesi haline gelmiştir¹⁴³. Diğer bir ifadeyle bilgi ile güç arasında doğru orantı vardır. Sahip olunan bilgi ne kadar çoksa, güç de o oranda çok olacaktır. Bu anlamda kişilere ait bilgileri, dolayısı ile de kişisel verileri ellerinde bulunduranlar güce de sahip olacaklardır. Verileri ellerinde bulunduranların bu verilere müdahale imkânlarının artması ve bu verilerin açıklanması durumunda veri sahiplerinin özel hayatlarına zarar verme olasılığı karşısında¹⁴⁴ veri sahipleri güçsüz ve hukuki anlamda korunmaya muhtaç bir pozisyonla karşı karşıyadırlar. Bu gelişmelerin neticesinde verilerin korunmasına yönelik hukuki düzenlemelerin yapılması bir zorunluluk arz etmiştir¹⁴⁵.

¹⁴² Şimşek, 5 vd.

¹⁴³ Can Aksoy, 3

¹⁴⁴ Nuri Tortop, "Çağımızın Önemli Sorunu: Kişisel Bilgilerin Güvenliği Sorunu", *Amme İdaresi Dergisi*, 33(3), Eylül 2000, 2

¹⁴⁵ Şimşek, 10

2.2.2. Kişisel Verilerin Korunması Alanındaki Uluslararası Düzenlemeler

Kişisel verilerin korunması alanında pratikte ve teoride etkili olan uluslararası düzenlemeler mevcuttur.

2.2.2.1. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Bünyesindeki Durum

Kişisel verilerin uluslararası alanda ilk kez ele alınması OECD¹⁴⁶ tarafından gerçekleştirilmiştir. Örgüt, kişisel veriler ve verilerin korunması ile 1970’li yıllarda ilgilenmeye başlamış ve kişisel verilerin sınır ötesi akışını gerçekleştirmek için Örgüt bünyesinde bir ekip oluşturmuştur¹⁴⁷. Zamanla kişisel verilerin daha çok alanda kullanılması, kişisel verilerin toplanması ve transferinin eskiye oranla kolaylaşması bir yandan olumlu gelişme kabul edilirken, diğer yandan özellikle özel hayat ve özel hayatın gizliliğinin ihlali tehlikesini de gündeme getirmiştir¹⁴⁸. Ancak OECD’nin bu alana karşı olan duyarlılığının altında yatan sebep bireylerin özel hayatlarının ve gizliliğinin korunmasından ziyade üye devletlerin ticari ve ekonomik gelişmelerinin ilerlemesi düşüncesidir¹⁴⁹. Zira kişisel verilerin korunması alanında düzenleme yapılması, OECD ülkeleri arasındaki ekonomik işbirliği bakımından zorunluluk arz eden bir alan olarak değerlendirilmiştir¹⁵⁰. Örgüt tarafından 1980 yılında “Gizliliğin Korunması ve Sınır Ötesi Kişisel Veri Akışları Hakkında Rehber İlkeler” (Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data) yayınlanmıştır. Yayınlanan bu metinde, üye ülkelerce özel yaşamın korunması hususunda iç hukuklarında dikkate alınabilecek rehber nitelikte ilkeler düzenlenmekle birlikte amaç kişisel yaşamın korunması noktasında uluslararası boyutta bazı güvencelerin sağlanmasıdır¹⁵¹. Ayrıca ulusal düzeydeki yasal düzenlemelerin de

¹⁴⁶ “1961 Eylül’ünde, Avrupa İktisadi İşbirliği Teşkilat (OEEC)’ nin isminin değiştirilmesi ve üyelik kapsamının genişletilmesi ile faaliyetine başlamıştır. Kuruluşu 14 Aralık 1960 da Paris’te OEEC ülkeleri ile ABD, Kanada ve İspanya arasında imzalanan bir konvansiyonla sağlanmıştır. Batılı sanayileşmiş ülkeler arasında birlik, dayanışma ve işbirliği sağlayan, bu ülkelerin uluslararası ekonomik ve siyasal konularda görüşlerini belirleyip aralarında uyum sağlanmasına yardımcı olan bir kuruluş durumundadır.” Halil Seyidoğlu, *Ekonomik Terimler*, Geliştirilmiş 3. Baskı, İstanbul 2002, 160

¹⁴⁷ Özdemir, 19

¹⁴⁸ Özdemir, 19

¹⁴⁹ Aydın Akgül, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, Beta Yayınevi, İstanbul 2014, 170

¹⁵⁰ Tekin Akılhoğlu, *İdari Usul ve Kişisel Verilerin Korunması*, 1, Erişim Tarihi: 26.04.2014, www.idare.gen.tr/akkillioglu-idariusul.htm.

¹⁵¹ Tortop, 3

birbirleri ile uyumlu hale getirilmesinin sağlanması da bu düzenlemenin amaçları arasında yer almaktadır¹⁵². Bu kapsamda bu ilkelerle m. 6' da belirtildiği üzere, sınır ötesi kişisel veri akışını etkileyebilecek olan gizliliğin ve kişi özgürlüğünün korunmasına yönelik ek önlemlerle tamamlanabilecek asgari şartlar belirlenmiş olmuştur. Tavsiye niteliğindeki bu ilkeler bağlayıcı olmadığından üye ülkelerin iç hukuklarında yapacakları düzenlemelerde bu ilkelere uyma zorunlulukları da bulunmamaktadır¹⁵³. Kaldı ki OECD'nin yayınladığı bu rehber ilkeler, üye ülkelere yeterli ilgiyi de görmemiştir¹⁵⁴.

Rehber ilkelerin kapsamı 2 ila 6. maddeler arasında düzenlenmiştir. m. 2'de, kamu ya da özel sektörde olması fark etmeksizin, gizliliğin ihlali veya kişisel özgürlüklere yönelik risk oluşturan kişisel verilere uygulanacağı belirtilmiştir. 3. m. Rehber ilkelerin bir bütün olarak değerlendirilmesi gerektiği ifade edilmiştir. Devamında ise yanlış uygulanabilirliği önler nitelikte nasıl anlaşılması gerektiği düzenlenmiştir. Buna göre doğalarına ve toplandıkları, saklandıkları, işlendikleri veya neşredildikleri içeriğe göre, farklı kategorilerdeki kişisel verileri korumaya yönelik farklı koruyucu önlemlerin uygulanmasını önleme şeklinde; ya da ifade özgürlüğünü haksız bir şekilde sınırlayan bir yöntemde yorumlanmaması gerektiği belirtilmiştir. Ancak bu kapsama milli egemenlik, milli güvenlik ve kamu politikaları ile ilgili olarak istisnalar getirilebileceği de düzenlenmiştir.

OECD tarafından yayınlanan metnin 2. kısmında yer alan sekiz temel ilke şunlardır;

- Sınırlı toplama ilkesi,
- Verilerin kaliteli olması ilkesi,
- Amacın belirliliği ilkesi,
- Sınırlı kullanım ilkesi,
- Güvenlik tedbirleri ilkesi,
- Açıklık ilkesi,
- Bireysel katılım ilkesi,
- Sorumlu tutulabilirlik ilkesi.

¹⁵² Aksoy, 4

¹⁵³ Aynı yönde görüşler için bkz. Küzeci, 119; Özdemir, 19-20; Şimşek, 12 vd.; Aksoy, 4,

¹⁵⁴ Akıllıoğlu, 1-2

2.2.2.2. Avrupa Konseyi Bünyesindeki Durum

Avrupa Konseyi, özellikle İkinci Dünya Savaşı'nın Avrupa'da yarattığı siyasal, toplumsal ve ekonomik çöküntü neticesinde yeni bir Avrupa oluşturmak amacıyla on batı Avrupa ülkesinin 5 Mayıs 1949'da Avrupa Konseyi Statüsünü imzalamaları ile kurulmuştur¹⁵⁵. Avrupa Konseyi Statüsü başlangıç kısmında “...*halkların ortak varlığı olan ve her gerçek demokrasinin dayandığı kişi özgürlüğü, siyasal özgürlük ve hukukun üstünlüğü ilkelerine kaynaklık eden düşünce ve ahlaki değerlere, sarsılmaz bir biçimde bağlı olarak, bu ülkünün korunması için aynı hisleri paylaşan Avrupa ülkeleri arasında sıkı bir birlik kurulması zorunlu görüşmüştür.*” ifadeleri ile hedefi belirlenmiş, amaçları arasında, en önemlisi olarak nitelendirilebilecek, insan haklarının ve temel özgürlüklerin geliştirilmesi ve korunması yer almıştır¹⁵⁶. Bu amaç doğrultusunda yapılan çalışmalarla Konsey, insan haklarının sağlanması ve korunması dolayısıyla da kişisel verilerin korunması alanına önemli katkılarda bulunmuştur¹⁵⁷.

Avrupa Konseyi, 28 Ocak 1981 tarih ve 108 sayılı “ Kişisel Nitelikli Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme” yi kabul etmiştir. Sözleşmenin yürürlüğe girişi ise 1985 tarihinde mümkün olmuştur. Sözleşmede 1999 yılında değişiklikler yapılmış ve 2001 yılında sözleşmeye 181 sayılı Ek Protokol ile ilaveler yapılmıştır. Bu protokolle, taraf devletlerde ulusal kontrol makamlarının oluşturulması zorunlu hale getirilmiş ve kişisel verilerin, yeterli seviyede koruma sağlamayan ülkelere ve uluslararası örgütlere transfer edilmesi engellenmiştir. Türkiye de üye ülkelerle birlikte hem 108 sayılı Sözleşmeyi hem de 181 sayılı Ek Protokolü imzalamıştır. Ancak iç hukukumuzda hem 108 sayılı Sözleşme hem de 181 sayılı Ek Protokol'ün onaylanması uzun yıllar almıştır¹⁵⁸. 108 sayılı sözleşme her ne kadar üye devletler arasında imzalanmış olsa da sözleşmenin 23. maddesi kapsamında

¹⁵⁵ Şeref Gözübüyük, Feyyaz Gölcüklü, *Avrupa İnsan Hakları Sözleşmesi ve Uygulaması*, Turhan Kitapevi, 8. Baskı, Ankara 2009, 7-8; Nurettin Bilici, *Avrupa Birliği ve Türkiye*, Seçkin Yayıncılık, Ankara 2010, 37

¹⁵⁶ Gözübüyük, Gölcüklü, 8

¹⁵⁷ Küzeci, 125 vd.; Şimşek, 19-21

¹⁵⁸ 108 sayılı Sözleşmenin geç onaylanmasının sebebi olarak, sözleşmenin m. 4 hükmü gereği her akit tarafın, iç hukukunda verilerin korunmasına yönelik gerekli önlemleri alması zorunludur. Bu önlemler, en geç sözleşme yürürlüğe girdiği tarihte alınmış olmalıdır. Ülkemizde, verilerin korunmasına yönelik kanun tasarısı uzun yıllar kabul edilmediği için sözleşmenin de onaylanıp yürürlüğe girmesinin de gecikmiş olması gösterilebilir. Bkz. Songül Atak, “Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler”, *TBB Dergisi*, sayı 87, yıl 2010, 94

üye olmayan devletlerin de bu sözleşmeye katılmalarına imkân tanınmıştır¹⁵⁹. Sözleşmeye taraf 47 Devlet bulunmakla beraber bu devletlerden Uruguay hariç hepsi Avrupa Konseyi üyesi devletlerdir¹⁶⁰.

Sözleşmenin önemli niteliği, kişisel verilerin korunması alanında hukuki bağlayıcılığı olan tek uluslararası belge olmasıdır¹⁶¹. Zira her üye ülke, sözleşmenin dördüncü maddesi hükmünce kendi iç hukukunda, verilerin korunmasına dair belirtilmiş ilkelere işlerlik kazandıracak gerekli önlemleri en geç, sözleşmenin kendileri bakımından yürürlüğe girdiği tarihte almak zorunlulukları vardır. Ayrıca bu sözleşme hükümleri, dünya genelinde kişisel verilerin korunmasına yönelik kabul görmüş ve ulusal mevzuatların hazırlanmasında model metin olarak alınmıştır.

Sözleşmenin kabul ediliş amacı birinci maddesinde de belirtildiği üzere; üye devletler arasında, tabiiyet ve ikametgâh ayrımı yapılmaksızın gerçek kişilerin temel hak ve özgürlüklerinin, özellikle de kişisel verilerinin, otomatik işleme tabi tutulması karşısında özel yaşam haklarının güvence altına alınmasıdır.

Sözleşmenin kapsamı üçüncü maddesinde düzenlenmiştir. Buna göre hem kamu hem de özel sektör bünyesindeki kişisel verilerin otomatik işlenmesini kapsamaktadır. Ancak her devlet imza esnasında veya daha sonra bu sözleşmeyi isterlerse topluluklar, dernekler, vakıflar, şirketler, birlikler ve tüzel kişilikten yararlanan veya yararlanmayan ve gerçek kişileri doğrudan veya dolaylı olarak bünyesinde bulunduran diğer kuruluşlarla ilgili bilgiler hakkında uygulayacağını bildirebilir. Yine sözleşmeye taraf devlet, bu sözleşme hükümlerini, otomatik bilgi işlem konusuna girmeyen kişisel nitelikteki veriler hakkında uygulayabilme imkânına sahiptir. Ayrıca belirtmek gerekir ki 108 sayılı Sözleşme ile kişisel verilerin korunmasına yönelik asgari şartlar düzenlenmiş olup sözleşmenin 11. maddesi kapsamında üye devletlerin sözleşmede belirtilen koruma şartlarında daha geniş bir koruma sağlamalarına hiçbir engel de yoktur¹⁶².

¹⁵⁹ Atak, 93-94

¹⁶⁰ 01.08.2014 tarih ve 3182 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı gerekçesi, Erişim Tarihi: 04.04.2016, <http://www2.tbmm.gov.tr/d24/1/1-0966.pdf>.

¹⁶¹ Küzeci, 131-132

¹⁶² Küzeci, 132

Avrupa Konseyi bünyesinde kişisel verilerin korunmasına hizmet eden diğer bir düzenleme Avrupa İnsan Hakları Sözleşmesidir (AİHS). Belirtmek gerekir ki AİHS’de kişisel verilerin korunması ayrı bir hak olarak yer almamaktadır. Kişisel verilerin korunması, sözleşmenin 8. maddesinde düzenlenmiş bulunan Özel Hayatın ve Aile Hayatının Korunması hakkı kapsamında değerlendirilerek mümkün olabilmektedir¹⁶³. Avrupa İnsan Hakları Mahkemesi, kişisel verilerin korunması hakkını, AİHS m. 8 ile garanti altına alınan özel hayatın korunması hakkının kısmen özel bir görünüş şekli olarak nitelemiştir¹⁶⁴. Daha net bir ifade ile kişisel verilerin korunması hakkı, özel hayatın korunması hakkının altında, bu hakkın bir kısmını ifade eden bir haktır. Dolayısıyla da AİHS m. 8’in ihlali, aynı zamanda kişisel verilerin korunması hakkının da ihlali anlamına gelmektedir. AİHM’nin, *Gardel/Fransa*¹⁶⁵ davasındaki “*Sözleşme’nin 8. maddesi ile korunan özel yaşam ve aile yaşamına saygı hakkını kullanmak için, kişisel verilerin korunması büyük bir rol oynamaktadır.*” ifadeleri AİHS m.8 ile kişisel verilerin korunması arasındaki bağlantıyı açık şekilde ortaya koymaktadır.

2.2.2.3. Birleşmiş Milletler¹⁶⁶ Bünyesindeki Durum

Birleşmiş milletler genel asamblesi, 14 Aralık 1990 tarihinde “ Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Rehber İlkeler” i kabul etmiştir. Bu ilkelerin kabulü ile üye ülkelerin, verilerin korunması alanında asgari bir düzeye ulaşmaları hedeflenmiştir.

Rehber ilkelerin uygulama alanı 10 numaralı kenar başlığın altında düzenlenmiştir. Buna göre bu ilkeler, ilk etapta, ihtiyari uzatma ve uygun düzenlemeler

¹⁶³ Doktrinde, AİHS’de kişisel verilerin korunmasına dair ayrı bir hak yer almamasından dolayı oluşan boşluğu doldurmak üzere 108 sayılı Avrupa Sözleşmesinin imzalandığı ifade edilmiştir. Bkz. Şimşek, 21

¹⁶⁴ Şimşek, 32

¹⁶⁵ Bkz. Gardel / Fransa Davası, başvuru no: 16428/05, par. 62 [http://hudoc.echr.coe.int/tur#{"fulltext":\["gardel"\],"sort":\["kupdate Ascending"\],"languageisocode":\["TUR"\],"appno":\["16428/05"\],"documentcollectionid2":\["GRANDCHAMBER"\],"itemid":\["001-114548"\]}](http://hudoc.echr.coe.int/tur#{) (E.T. 01.07.2015)

¹⁶⁶ “ San Francisco’da imzalanan ve 24 Ekim 1945 tarihinde yürürlüğe giren Birleşmiş Milletler Antlaşması ile kurulmuştur. Türkiye diğer 50 ülke ile birlikte Örgütün kurucu üyeleri arasında yer almıştır. Birleşmiş Milletler Örgütü’nün amacı dünya barışını ve güvenliğini korumak, uluslararası ekonomik, toplumsal ve kültürel işbirliği oluşturmak şeklinde belirlenmiştir. Amaçlarına ulaşmak için, ülkeler arasındaki uyuşmazlıkların barışçı yoldan çözümünü teşvik etmekte barışa karşı tehdit, barışın bozulması ve saldırı durumunda ise çeşitli eylemler uygulamaya koyabilmektedir. Barış ve güvenliğe ilave olarak insan hakları, ekonomik ve çeşitli toplumsal konularda önemli faaliyetlerde bulunmaktadır.” Bilici, 34

suretiyle, elle işlenmiş dosyaların yanı sıra bilgisayarla işlenmiş kamu ve özel sektördeki tüm dosyalara uygulanabilir olmalıdır.

Bu metinde kabul edilen rehber ilkeler şunlardır;

- Yasallık ve dürüstlük ilkesi,
- Doğruluk ilkesi,
- Amacın belirliliği ilkesi,
- İlgili kişinin erişimi ilkesi,
- Ayrımcılık yapmama ilkesi,
- İstisna koyma yetkisi,
- Güvenlik ilkesi,
- Denetleme ve yaptırımlar,
- Sınır ötesi veri akışı.

2.2.2.4. Avrupa Birliği Bünyesindeki Durum

Avrupa Birliği, Avrupa Kıtası'nda yer alan ülkelerin ortak bir kaderi paylaşma, ulusal egemenlik haklarını kısmen, oluşturulan birlik yönetimine devretme anlamı taşımaktadır. Avrupa'daki bu bütünleşmenin altında ticari alanda liberalleşme, ulusal barış ve refahın daha hızlı bir şekilde artırılacağı inancı yatmaktadır. Yine Avrupa bütünleşmesi ile ülkelerin, milliyetçilik ve düşmanlık hisleriyle birbirlerinden ayrılmaları yerine işbirliği yapılarak insanların refah seviyelerinin artırılması amaçlanmıştır¹⁶⁷. Belirtmek gerekir ki Avrupa'da bu anlamda bir birlik oluşturulması fikri sürekli var olmuştur. Bu fikrin altında iktisadi anlamda büyümenin sağlanabilmesi için ortak bir pazarın etkisi, büyük ve egemen güç olma gibi nedenler yatmaktadır¹⁶⁸. Bu çerçevede ilk kurucu anlaşma 18 Nisan 1951 tarihinde imzalanan Avrupa Kömür ve Çelik Topluluğu Anlaşmasıdır. Akabinde 25 Mart 1957 tarihinde imzalanan Avrupa Atom Enerjisi Topluluğu ve Avrupa Ekonomik Topluluğu Anlaşmaları imzalanmıştır. Son olarak 7 Şubat 1992 tarihinde imzalanan ve 1 Kasım 1993 tarihinde yürürlüğe giren

¹⁶⁷ Bilici, 33

¹⁶⁸ Haydar Çakmak, *Türkiye Avrupa Birliği İlişkileri*, 3. Baskı, Ankara 2011, 13

Avrupa Birliği Anlaşması (Maastricht Anlaşması) ile bugünkü Avrupa Birliği kurulmuştur¹⁶⁹.

Avrupa'daki bu bütünleşme hareketi bölgesel anlamda küreselleşmenin bir örneğidir¹⁷⁰. Küreselleşme, hukuku etkilemiş ve ulusal ve uluslararası alanda onu tekrardan şekillendirmiştir. Zira hukuk iktisadi ve teknolojik gelişmelerle birlikte küreselleşmenin taşıyıcıları olmuşlardır¹⁷¹. Avrupa Birliği içerisinde hukuk alanında kabul edilen belge ve metinlerde bu anlamda bir küreselleşme etkisinin varlığı açıktır.

Avrupa Birliği bünyesinde kişisel verilerin korunmasına dair Avrupa Birliği Temel Haklar Şartı¹⁷² ve 95/46/AT sayılı, 97/66/AT sayılı, 2002/58/AT sayılı Direktiflerde düzenlemelere yer verilmiştir.

- Avrupa Birliği Temel Haklar Şartı: 7 Aralık 2000 tarihinde imzalanan Birlik Şartı ile Avrupa halkları arasında süreklilik esasına ve ortak değerlere dayalı, barışçıl bir gelecek paylaşmak üzere hedeflenen birliği oluşturmak noktasındaki kararlılığını ortaya koymuştur. Birlik, özgürlük, güvenlik ve adalet alanı yaratmak suretiyle bireyi bu doğrultuda odak noktası olarak belirlemiştir. Aynı zamanda dengeli ve sürdürülebilir gelişmeyi desteklemek; kişilerin, malların, sermayenin ve hizmetlerin serbest dolaşımını ve yerleşme serbestisini temin etmeyi de amaçlamaktadır. Bu amaç doğrultusunda sosyal değişimler, bilimsel ve teknolojik gelişmeler ışığında, temel hakların korunması, bu hakların ortak bir metinde düzenlenmesi ile güçlendirilmiştir¹⁷³.

Birlik Şartı içerisinde kişisel verilere dair düzenleme, bu konuda var olan uluslararası diğer düzenlemelerden bağımsız değildir. Başlangıç kısmında da belirtildiği üzere Avrupa Birliği Antlaşmasından ve Topluluk Antlaşmalarından, İnsan Haklarının ve Temel Özgürlüklerin Korunması Hakkında Avrupa Sözleşmesinden, Topluluk ve Avrupa Konseyi tarafından kabul edilen Sosyal Şartlardan ve Avrupa Toplulukları

¹⁶⁹ Bilici, 39-40

¹⁷⁰ Mustafa Erdoğan, *Küreselleşme, Hukuk ve Türkiye*, Turgay Uzun, Serap Özen (Ed.). *Avrupa Birliği Sürecinde Türkiye*, Seçkin Yayıncılık, Ankara 2004, 19

¹⁷¹ Erdoğan, 17

¹⁷² Birlik Şartı olarak ifade edilecektir. Avrupa Birliği Temel Haklar Şartı metni için bkz <http://www.eskisehirab.gov.tr/userfiles/files/AVRUPA%20B%C4%B0RL%C4%B0%C4%9E%C4%B0%20TEMEL%20HAKLAR%20%C5%9EARTI.pdf> (E.T. 01.08.2015)

¹⁷³ Avrupa Birliği Temel Haklar Şartı başlangıç kısmı.

Adalet Divanı ve Avrupa İnsan Hakları Mahkemesi içtihat hukukundan haklara atıfta bulunularak bu hakları teyit eder nitelikte olduğu belirtilmiştir¹⁷⁴.

Birlik Şartı'nda kişisel verilerin korunması hakkının düzenlenmesi, Avrupa Birliği içerisinde Avrupa Birliği vatandaşlarının ve Avrupa Birliği'nde yaşayan tüm bireylerin kişisel, siyasi ve ekonomik haklarını ilk kez tek bir metinde toplamış olması bakımından önemlidir¹⁷⁵. Birlik Şartı Başlangıç kısmında belirtildiği üzere, sosyal değişimler ve bilimsel ve teknolojik gelişmelerin ışığında, temel hakların korunması, bu hakların bir Şartta yer verilerek düzenlenmesi, bu hakları güçlendirecektir. Doktrinde de, kişisel verilerin korunması başlığı altında münhasır bir maddede bu hakkın, bir temel hak olarak düzenlenmiş olması, Avrupa Birliği içerisinde, kişisel verilerin korunması bakımından daha da güçlü bir koruma sağlayacağı ifade edilmiştir¹⁷⁶. Belirtmek gerekir ki 2000 yılında imzalanan Birlik Şartı hükümleri, 7 Aralık 2000 tarihinde imzalanmakla birlikte yürürlüğe 1 Aralık 2009 tarihinde girmiştir. Yürürlüğe giriş tarihine kadar Birlik Şartı hükümleri bağlayıcı olmamakla birlikte yol gösterici nitelikte önemli bir belge olma özelliğine sahipti¹⁷⁷. Birlik Şartı hükümlerinin yürürlüğe girmesi ile hukuki olarak Birlik üyesi devletler için bağlayıcı niteliği haiz bir belge olmuştur. Ayrıca (aydın Akgül devamı s.209)

Birlik Şartı m. 8'de ayrı bir hak olarak kişisel verilerin korunması düzenlenmiştir. Maddenin birinci fıkrasında herkesin kendisini ilgilendiren kişisel verilerinin korunmasını isteme hakkına sahip olduğu düzenlenmiştir. İkinci fıkrasında bu verilerin, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörölmüş diğer bir meşru temele dayanarak tutulabileceği belirtilmiştir. Bu fıkra hükmünün ilk cümlesinde, kişisel verilerin işlenmesinde dikkate alınması gereken ilkelerin yer aldığı anlaşılmaktadır. Fıkra hükmünün devamında da herkesin, kendisi ile ilgili toplanmış olan verilere erişimine ve bu verileri düzeltmesine imkân veren hakları yer almaktadır.

Avrupa Birliği içerisinde yeknesak bir hukuk düzenin oluşturulması çabaları¹⁷⁸, malların, hizmetlerin, kişilerin ve sermayenin serbestçe dolaşabilmesi dolayısıyla kişisel

¹⁷⁴ Şimşek, 70

¹⁷⁵ Küzeci, 158

¹⁷⁶ Şimşek, 69

¹⁷⁷ Küzeci, 159

¹⁷⁸ 95/46/AT sayılı Direktif 1. ve 8. paragraflar

verilerin serbest dolaşımın sağlanabilmesi¹⁷⁹ ve kişisel verilerin korunmasına dair özel düzenlemelere duyulan ihtiyaçlar nedeniyle Avrupa Parlamentosu ve Konsey 95/46/AT sayılı “*Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesi*”ni kabul etmiştir ve 24 Ekim 1995 yılında Direktif yürürlüğe girmiştir. Belirtmek gerekir ki 95/46/AT sayılı Direktif’in 3. paragrafında belirtilmiş olan malların, hizmetlerin, kişilerin ve sermayenin serbest dolaşımı aynı zamanda Avrupa Birliği’nin üzerine oturmuş olduğu temel düşüncedir. Bu düşüncenin gerçekleştirilmesi açısından kişisel verilerin toplanması ve işlenmesi kaçınılmaz bir durumdur¹⁸⁰.

Direktifin amacı, birinci maddesinde belirtildiği üzere, üye devletler, kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini korumak zorundadırlar. Bu kapsamda sağlanan koruma ile bağlantılı olarak üye devletler arasında kişisel verilerin akışı yasaklanmayacak ve engellenmeyecektir.

Direktifin kapsamı ise üçüncü maddesinde iki fıkra olarak düzenlenmiştir. Buna göre kişisel verilerin otomatik araçlar dışında işlenmesine ve kısmen veya tamamen otomatik araçlarla işlenmesinde uygulanacaktır. İkinci fıkrada istisnai durumlar belirtilmiştir. Ceza hukukundaki devlet faaliyetleri ve devlet güvenliği, savunma, kamu güvenliğine ilişkin verilerin işlenmesi durumunda Avrupa Birliği Anlaşmasının V. ve VI. Başlıklarında belirtilenler gibi Topluluk Hukuku kapsamı dışındaki bir faaliyet için uygulanmayacaktır. Yine bir gerçek kişi tarafından, tamamen kişisel veya ev içi faaliyeti olan durumlar Direktif kapsamı dışında kabul edilmiştir.

Avrupa Parlamentosu ve Konseyi 1997 yılında 97/66/AT sayılı “*Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Yönergesi*” ni, daha sonra 2002 yılında da “*Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi*” ni kabul etmiş ve yürürlüğe koymuştur. 2002 tarihli bu Direktif, hem de yürürlükten kaldırılan 97/66/AT sayılı direktif, 1995 tarihli genel Direktifi tamamlar niteliktedir. 2002/58/AT sayılı Direktifin 4. paragrafında belirtilen 97/66/AT sayılı Direktifi, halka açık elektronik haberleşme hizmetlerini kullanan kullanıcılarının kişisel verilerinin ve gizliliğinin eşit seviyede korunmasını sağlamak için elektronik haberleşme piyasaları ve teknolojilerine

¹⁷⁹ 95/46/AT sayılı Direktif 3. paragraf

¹⁸⁰ Başalp, 25

uyarlanmak zorundadır. Bu nedenle 97/66/AT sayılı direktifi yürürlükten kaldırılmış ve onun yerine 2002/58/AT sayılı Direktif yürürlüğe konulmuştur¹⁸¹. Kapsam olarak 2002/58/AT sayılı Direktifte, genel Direktiften farklı olarak tüzel kişiler de kapsama alınmıştır.

2006 yılında 2006/24/AT sayılı “ *Halka Açık İletişim Hizmetleri veya İletişim Ağlarına İlişkin Olarak Üretilen veya İşlenen Verilerin Saklanması İlişkin Direktif*” i kabul etmiştir. Bu direktif ile Avrupa’da cezai soruşturmalarda işbirliğinin sağlanması amaçlanmıştır. Yine bu Direktif ile elektronik haberleşme sağlayıcılarına bir takım yükümlülükler getirilmiştir. Bu bağlamda saklanacak veri kategorileri, saklama süreleri, saklama koşulları ve verilerin güvenliği ile ilgili düzenlemelere yer verilmiştir¹⁸².

Ayrıca, Avrupa Birliği çerçevesinde kişisel verilerin korunması, bir temel hak olarak 2001 yılında yapılan değişiklikle Avrupa Birliği Temel Haklar Şartı’nın 8. maddesinde yer almıştır¹⁸³.

2.2.3. Türk Hukukunda Kişisel Verilerin Korunması

Kişisel verilerin korunmasına dair iç hukukumuzda var olan 6698 sayılı KVKK ve konuya ilişkin diğer bazı mevzuattaki başlıca düzenlemeler, bu kısım altında ele alınacaktır.

2.2.3.1. 6698 sayılı KVKK’dan Önceki Durum

Kişisel verilerin korunmasına yönelik, hukukumuzda 24 Mart 2016 tarihine kadar genel bir kanunun olmadığından, ancak bu tarihe kadar muhtelif kanun tasarılarının TBMM’ye sunulduğundan bahsetmiştik. Hukukumuzda, kişisel verilerin, telekomünikasyon sektöründe işlenmesine ve gizliliğine dair bir yönetmelik mevcuttur. Yönetmeliğin ilgili maddesinde de belirtildiği üzere dayanak kanunlar Telgraf ve Telefon Kanunu ile Telsiz Kanunu’dur. Ancak, kişisel verilerin toplanmasına, korunmasına ve bu verilere erişilmesine dair diğer normlarda¹⁸⁴ da çeşitli hükümler

¹⁸¹ 2002/58/AT sayılı Direktif 4. paragraf

¹⁸² Doğan Kılınç, “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, *AÜHFD*, Sayı 61 (3), yıl 2012, 1128-1129

¹⁸³ Başalp, 27

¹⁸⁴ TCK m. 135-140, Anayasa m. 20/son

düzenlenmiştir. Bunun yanında Türkiye, kişisel verilerin korunması ile ilgili uluslararası sözleşmelere¹⁸⁵ de imza koymuş bulunmaktadır. Ancak yukarıdaki başlıklarda ifade edildiği üzere uluslararası bu sözleşmelerin gereği olarak, gerekli ulusal düzenlemelerin iç hukukumuzda yapılması uzun zaman sürdüğü için bu sözleşmeler ulusal hukukumuz açısından yürürlük kazanması da geç olmuştur¹⁸⁶. Türkiye’de kişisel verilerin korunmasına yönelik ilk çalışmalar 1988 yılında başlamıştır ve uzun bir süre devam etmiştir. Devam eden bu zaman zarfında kurulan komisyonca hazırlanan ilk Tasarı metni 2005 yılında Başbakanlık’a sevk edilmiştir. Tasarı metni Adalet Bakanlığınca 2007 yılında yeniden düzenlenerek Başbakanlığa gönderilmiş ve 2008’de de Meclise sevk edilmiştir¹⁸⁷. 2011 yılında yeniden ele alınan Kişisel Verilerin Korunması Kanun Tasarısı ilgili komisyon tarafından, hâlihazırdaki tasarıya getirilen eleştiriler ve öneriler de dikkate alınmak suretiyle yenilenerek 2012 yılında Başbakanlığa gönderilmiştir¹⁸⁸. İlgili tasarı metni¹⁸⁹ de 26.12.2014 tarihinde Meclis’e sevk edilmiştir. Son olarak 18.01.2016 tarihinde Başbakanlıkça kişisel verilerin korunmasına dair yeni bir tasarı metni¹⁹⁰ TBMM Başkanlığına sunulmuş ve bu metin üzerinde küçük bazı değişiklikler yapılarak 24.03.2016 tarihinde TBMM Genel Kurulunda kabul edilmek suretiyle 6698 sayılı KVKK bazı maddeleri yayımı tarihinden altı ay sonra olmak üzere esas itibarı ile yayımı tarihinde yürürlüğe girmiş ve ülkemiz bakımından münferit bir veri koruma kanununa sahip olmamanın olumsuzlukları da aşılmış bulunmaktadır.

2.2.3.1.1. 1982 Anayasası

Kişisel verilerin korunması hakkının daha çok yeni bir hak kavramı olması nedeniyle anayasalarda yer almadığı söylenebilir¹⁹¹. Ancak bu durum kişisel verilerin korunmasında anayasal bir temelin olmadığı anlamına da gelmemektedir.

¹⁸⁵ Kişisel verilerin korunması alanında, uluslararası düzeyde en önemli ve bağlayıcılığı olan 108 sayılı Avrupa Konsey Sözleşmesi olup bu sözleşme T.C. tarafından imzaya açıldığı tarih olan 28.01.1981 tarihinde imzalanmıştır.

¹⁸⁶ Bkz. 158. dipnot

¹⁸⁷ Kılınç, 1145

¹⁸⁸ Halil Çelik, *Türkiye’nin “Kişisel Verileri Koruma” Serüveni*, Erişim Tarihi: 01.07.2015, <http://hacehissiyasa.blogspot.com.tr/2014/01/turkiyenin-kisisel-verileri-koruma.html>.

¹⁸⁹ Son tasarı metni için bkz. Erişim Tarihi: 01.07.2015,

<http://www.kgm.adalet.gov.tr/Tasariasamaları/Tbmmkms/Tbmmkom/ki%C5%9Fisel%20veriler.pdf>.

¹⁹⁰ 18.01.2016 tarihli KVKK için bkz. Erişim Tarihi: 04.04.2016, <http://www2.tbmm.gov.tr/d26/1/1-0541.pdf>.

¹⁹¹ Küzeci, 262

Temel hakların düzenlendiği yer olan 1982 Anayasası'nda, kişisel verilere dair ilk düzenleme 2010 yılı anayasa değişikliği ile 20. maddeye eklenen üçüncü fıkrada yer almıştır. Bu düzenlemeden önce maddi ve manevi varlığı serbestçe geliştirme hakkı (m.17), konut dokunulmazlığı (m. 21), haberleşmenin gizliliği (m. 22), düşünce ve kanaatlerini açıklamaya zorlanamama hakkı (m. 25) kişisel verilerin korunmasında dayanak olabilecek diğer anayasal hükümlerdir¹⁹². Bu maddelerin varlığı, kişisel verilerin sınırsız olarak toplanmasına, kaydedilmesine, kullanılmasına ve devredilmesine karşı bireyin temel hak ve özgürlüklerini anayasal koruma altına almaktadır¹⁹³. Eklenen son fıkra hükmü, kişisel verilerin korunması hakkının temel ilkelerini ve kişilerin haklarını açıkça belirtmesi bakımından oldukça önemli bir düzenlemedir¹⁹⁴. Hemen belirtmek gerekir ki, Anayasal bir güvenceye kavuşmuş olan bu hakkın gerçek anlamda varlığının sağlanması ve etkin olarak korunabilmesi için bir takım ön şartların gerçekleştirilmesi gerekmektedir. Kişisel verilerin korunması alanında kullanılan başlıca kavramların tanımlanması¹⁹⁵, kişisel verilerin işlenmesinin genel ilke ve esaslarının, kişilerin haklarının korunmasına yardımcı olacak mekanizmaların ve kişisel verilerin işlenmesi esnasında ilgililer tarafından bu hakkın ihlal edilmesini önleyici ikincil düzenlemelerin ve bağımsız bir Veri Koruma Kurulunun oluşturulması kaçınılmazdır¹⁹⁶. Doktrinde kişisel verilerin tam ve daha etkili şekilde korunabilmesi için anayasal düzeyde korunmasının yerinde olduğu savunulmaktadır¹⁹⁷. Yazar, görüşünde haklı olarak, kişisel verilerin korunması hakkının ayrı bir hak olarak anayasa metninde yer alması gerektiğini ve bunun bir takım faydalarının da olacağını belirtmiştir. Yazara göre, kişisel verilerin korunmasına yönelik 1982 Anayasası'nda dayanak düzenlemeler yer alsa da, ayrı bir hak olarak ilgili hakkın düzenlenmesi halinde Anayasa koyucunun konuya verdiği önem anlaşılacak ve uygulamada da bu konu üzerinde daha duyarlı olunacaktır.

¹⁹² Kılınç, 1131

¹⁹³ Şimşek, 119

¹⁹⁴ T.C. Cumhurbaşkanlığı Devlet Denetleme Kurumu Denetleme Raporu, 781, Erişim Tarihi: 01.07.2015, <https://www.tccb.gov.tr/assets/dosya/ddk56.pdf>.

¹⁹⁵ Yargıtay Ceza Genel Kurul E. 2012/12-1510, K. 2014/331, T. 17.6.2014 kararında "...Bugüne kadar kişisel verilerin neler olduğuna dair kanunun çıkarılmaması nedeniyle TCK'ndaki 135 ve 136. Maddelerindeki hukuka aykırılığın hangi hallerde oluştuğuna ilişkin başvurulabilecek kapsayıcı bir kaynak ya da norm olmaması nedeniyle bu iki madde eksik norm sayılır. ... Bununla beraber adı geçen ceza maddeleri yürürlükte olduğundan uygulanması sırasında çok dikkatli olunması gerekir." görüşümüzü destekler ifadeler kullanmıştır.

¹⁹⁶ DDK Denetleme Raporu, 781

¹⁹⁷ Küzeci, 263

- İnsan Onuru

İnsanın, insanlığın geçirmiş olduğu mübadelelerden sonra, insana yaraşır şekilde yaşamını sürdürebilmesi için kabul edilen hukuki metinlerde, insan onuruna yer vermeye başlanmıştır. Bu doğrultuda 1945 tarihli Birleşmiş Milletler Antlaşması' nın amaçları içerisinde temel insan hakları, insan kişiliğinin onur ve değeri, 1948 tarihli İnsan Hakları Evrensel Beyannamesi m. 1'de bütün insanların onur ve haklar bakımından eşit doğdukları, m. 5'te hiç kimseye onur kırıcı davranışlarda bulunulamayacağı, 1966 tarihli BM Medeni ve Siyasi Haklar Sözleşmesi Başlangıç kısmında, insanlık onuruna doğuştan sahip olduğu ve bu metinde kabul edilen hakların insanlık onurundan türediği kabul edilmiştir. Yine Avrupa İnsan Hakları Sözleşmesi'nin 3. maddesinde hiç kimsenin onur kırıcı ceza veya işlemlere tabi tutulamayacağı düzenlenmiştir. Anayasamız da ise Başlangıç kısmının 6. paragrafında herkesin onurlu bir hayat sürdürme hakkı olduğu belirtilmiştir.

İnsan onuru, tanımlanması güç bir kavramdır¹⁹⁸. Bu kavramın altında insanın kişiliği, öz değerleri yatmaktadır. Çünkü insanın sahip olduğu akli ve ahlaki yetenekleri, onu maddi ve manevi açıdan kendine özgü bir değer sahibi kılmaktadır. Bu kapsamda da insan kendisini maddi ve manevi yönden gerçekleştirme imkânına sahip olmaktadır¹⁹⁹. Anayasa Mahkemesi bir kararında insan onurunu tanımlamıştır. Mahkemeye göre insan onuru “ *insanın ne durumda, hangi şartlar altında bulunursa bulursa sırf insan olmasının kazandırdığı değer tanınmasını ve sayılmasını anlatır*”²⁰⁰ hakkı olduğu belirtilmiştir.

İnsan onuru kavramının önemi, bu kavramın bireyin hak ve özgürlüklerinin ortak temeli olması ve en yüksek hukuksal değer olarak kabul edilmesidir²⁰¹. Bu doğrultuda bireyin insan olmasından dolayı sahip olduğu onur göz önünde tutularak ve bu onur ile bağdaşır şekilde, kişisel verilerin toplanması, işlenmesi ve üçüncü kişilere devri ve de diğer tüm faaliyetler yerine getirilmelidir.

¹⁹⁸ İnsan onurunun tanımlanması ile ilgili detaylı bilgi için bkz. Orhan Aldanmaz, *İnsan Onuru Işığında Kişisel Özerklik ve Yerellik İlkesi*, EÜHFD, XIV(1-2), 2010, 81 vd.

¹⁹⁹ Nihat Bulut, “Eski Yunan’dan Aydınlanma Çağına İnsan Onuru Kavramının Gelişimine Genel Bir Bakış”, EÜHFD, XII(3-4), 2008, 2.

²⁰⁰ AYMK, E. 1963/132, K. 1966/29, K.T. 28.06.1966, <http://www.kararlaryeni.anayasa.gov.tr/Karar/Content/b95ec65c-f13d-4bcd-a586-4f2b970f58c3?excludeGerekce=False&wordsOnly=False> (E.T. 01.07.2015)

²⁰¹ Şimşek, 129, İnsan onurunun, bütün hak ve özgürlüklerin temeli sayılmasının gerekçesi olarak bu kavramın, insanın öz değerini ifade etmesi, her türlü toplumsal, siyasal ve hukuksal müdahalelere karşı ileri sürülebilme özelliği taşıması söylenebilir. Bkz. Bulut, 2

- Maddi ve Manevi Varlığını Serbestçe Geliştirme Hakkı (m. 17)

Diğer bütün haklarda olduğu gibi bu hakkın da temeli insan onurudur. Ancak bu hak ile insan onuru birlikte var olabilecek bir haktır. Anayasamızın başlangıç kısmının 6. paragrafında onurlu bir hayat sürme ve maddi ve manevi varlığı geliştirme hakkından bahsedilmiştir. Bu noktada insanın onurlu bir hayat sürmesi, onun maddi ve manevi varlığını geliştirmesine bağlı olduğu anlaşılmaktadır. Ancak, bu noktada devletin, bireylerin bu hakları çerçevesinde maddi ve manevi varlıklarını geliştirebilmeleri için Anayasanın 5. maddesinde belirtilen tedbirleri alması gerekmektedir. Kişiler, kendilerine ait bilgileri, ne zaman, nerede, nasıl, ne kadar ve kime açıklayacağına kendisi karar verirler. Bu durum aksinin düşünülmesi, kişinin maddi ve manevi kişiliğinin geliştirilmesinin engellenmesi ve bireyin, istenildiği zaman ve istenilen şekilde ulaşılabilen bir nesne olması anlamına gelecektir. Sözü edilen durumda kişiliğin geliştirilmesi hakkının kullanılması mümkün olmayacaktır. Ayrıca bu durum insan onuru ile de bağdaşır nitelikte değildir²⁰².

Kişisel verilerin korunması esasında, kişilik değerlerinin korunması yatmaktadır. Bu anlamda da kişisel verilerin korunması insan onurunun korunmasına ve kişiliğin maddi ve manevi olarak geliştirilmesine hizmet etmektedir²⁰³.

Kişisel veriler, insan onuru ile yakından ilgili olması nedeniyle bu maddenin varlığı kişisel verilerin korunması hakkı açısından anayasal bir dayanak oluşturmaktadır.

- Özel Hayatın Gizliliği ve Korunması Hakkı (m. 20)

Özel hayatın gizliliği ile kişisel verilerin korunması hakları arasındaki ilişkiyi, diğer ifadeyle benzerliği ortaya koyabilmek için öncelikli olarak özel hayat ve özel hayatın gizliliği kavramlarının anlaşılması gerekmektedir. Öncelikle belirtmek gerekir ki özel hayat ve özel hayatın gizliliği, ulusal düzenlemeler yanında özellikle uluslararası düzenlemelerde de yer alarak hem güvence altına alınmış hem de uluslararası platformda bu hakkın önemi ortaya konulmuştur. Gerçekten de uluslararası alanda temel hak ve özgürlüklerin sağlanması ve korunması açısından önemli düzenlemeler olan Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesi (m. 17), Avrupa İnsan Hakları Sözleşmesi (m. 8) ve İnsan Hakları Evrensel Beyannamesi (m. 12) ilgili maddelerinde bu hak düzenlenmiştir. İç hukukumuzda ise bu hak 1982 Anayasası'nın 20. maddesinde

²⁰² Şimşek, 131

²⁰³ Şimşek, 119

kaleme alınmıştır. Ayrıca 5237 sayılı TCK m. 134'te de bu hakkın ihlali neticesindeki cezai durum hüküm altına alınmıştır. Önceki ana başlık altında, kişisel verilerin korunması hakkının, 20. madde içerisinde düzenlenmesinden önce de yine, özel hayatın gizliliği hakkı kapsamında korunmasının mümkün olacağına değinmiştik. Bu değişiklikten önce, kişisel verilerin korunması adı altında doğrudan bir düzenleme olmasa da, yayınlanan birçok ulusal ve uluslararası düzenlemelerde kişisel verilerin korunmasına ilişkin olarak kişinin özel hayatına atıfta bulunulmuştur. Bu atıflar da kişisel verilerin özünde kişinin özel hayatını ve bunun gizliliğini ilgilendirmesi münasebetiyle kişisel verilerin korunmasını, bu anayasal hak bünyesinde de mümkün olabileceğini göstermektedir²⁰⁴. Dolayısıyla Anayasa m. 20 Özel Hayatın Gizliliği ve Korunması Hakkı ile kişisel verilerin korunması hakkı birbiri ile alakalı, iç içe geçmiş haklardır. Diğer taraftan, 2010 yılı değişikliği ile kişisel verilerin korunması hakkının 20. madde içerisinde düzenlenmesi, aslında kişisel veriler ile özel hayatın gizliliği arasındaki bağılılığı göstermektedir.

Özel hayatın gizliliği, tanımının yapılması zor bir kavramdır. Doktrinde özel hayatı açıklamaya yönelik görüşler yer almaktadır. Her şeyden önce özel hayat, ilgili kişinin mahremiyetine dair her şeyin gizli kalması ve bu gizliliğin ihlal edilmemesini ifade etmektedir²⁰⁵. Yaygın olarak kabul edilen görüşte, kişinin hayatı üçe ayrılmakta ve bu ayrıma göre hukuki değerlendirmelerde bulunmaktadır²⁰⁶. Buna göre kişinin hayatı, kamuya açık, özel ve sır alanları olmak üzere tasnif edilmiştir. Kamuya açık alan, kişinin sosyal çevre içerisinde bulunduğu, bu çevre içindeki diğer bireylerle paylaşılan diğer bir ifadeyle bu çevredeki herkesçe bilinen ortak hayat alanıdır²⁰⁷. Bu alanın içerisinde kişinin adı, mesleği, ikametgâhı gibi sosyal hayatın tabiatı gereği olarak bir takım bilgiler yer almaktadır. Buna bağlı olarak da bu kişisel verilerin bu çevrede yer alan diğer kişilerce bilinmesi de doğal bir sonuçtur²⁰⁸. Her ne kadar kişinin bu hayat alanında yer alan verileri bilinebilir nitelikte ise de buradan bu hayat alanına serbest şekilde müdahale edilebileceği anlamı çıkarılmamalıdır²⁰⁹. Yani bireyin, bu

²⁰⁴ Küzeci, 267-268; Şimşek, 140 vd.

²⁰⁵ Nurdan Okur, *Anayasa Hukuku Açısından Özel Hayatın Gizliliği ve Korunması*, (Yayınlanmamış Doktora Tezi), Ankara 2010, 10

²⁰⁶ Ayhan Döner, *Şeffaf Devlette Bilgi Edinme Hakkı ve Sınırları*, 12 Levha Yayınları, İstanbul 2010, 255; Şimşek, 140; Özdemir, 114

²⁰⁷ Özdemir, 114; Döner, 255

²⁰⁸ Özdemir, 114-115

²⁰⁹ Döner, 255

sosyal yapı içerisinde bir takım kişisel verilerinin bilinmesi, onun özel hayatının gizliliğinin ortadan kaldırmayacaktır²¹⁰. Zira her kişisel veri, kişisel verilerin korunmasına ilişkin yasal düzenlemeler çerçevesinde koruma kapsamındadır ve kişisel verilerin korunması genel ilkeleri açısından da güvence içerisinde ki kişinin her ne kadar sosyal yaşam içinde olmasından dolayı kişisel verileri biliniyor olsa da bunların ilgili kişinin rızası olmadan, örneğin fotoğrafının çekilmesi, sesinin kaydedilmesi gibi çeşitli şekillerde kişisel verilerinin edinilmesi kişinin hem özel hayatının gizliliğinin hem de kişisel verilerinin korunmasının ihlali olarak kabul edilecektir²¹¹.

Kişinin özel hayatı olarak adlandırılan kısım da, kamuya açık alan kadar geniş olmamakla birlikte, kişinin belli bazı kişilerle paylaştığı hayat alanıdır²¹². Bu alandaki kişilere, kişinin ailesi, akrabaları ve yakın çevresi örnek verilebilir. Bu alan içerisinde kişiyi belirli veya belirlenebilir kılacak kişisel veri niteliğinde verileri yer almaktadır²¹³. Kişi, bu alanda yer alan kişilerle olan ilişkilerini ve verilerini toplumun geri kalanı ile paylaşmak istemeyebilir, ancak teknolojik gelişmeler karşısında kişi, özel hayatının gizliliğini koruma noktasında yetersiz kalabilmektedir²¹⁴. Bunun sonucu olarak da özel hayat, daha fazla korunmaya ihtiyaç duyan bir alan olduğu anlaşılmaktadır. Belirtmek gerekir ki bu alana hiçbir şekilde müdahalenin mümkün olmayacağı da söylenemez. Hukuki metinlerdeki düzenleme şekilleri dikkate alındığında önce bu alana dokunulamayacağı, devamında da hangi hallerde müdahale edilebileceği yer almaktadır. Dolayısıyla buradan anlaşıldığı üzere özel hayata müdahalede asıl olan müdahale edilemeyeceğidir. Anayasa Mahkemesi verdiği bir kararında²¹⁵ “Özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Orada cereyan edenlerin yalnız kendisi veya kendisinin bilmesini istediği kimseler tarafından bilinmesini istemek hakkı, kişinin temel haklarından biridir. Bu niteliği sebebiyledir ki, özel hayatın gizliliğine dokunulmaması, insan haklarına ilişkin beyanname ve sözleşmelerde korunması istenilmiş, ayrıca tüm demokratik ülke mevzuatında açıkça belirlenen istisnalar dışında bu hak devlet

²¹⁰ Şimşek, 142

²¹¹ Şimşek, 142

²¹² Özdemir, 115

²¹³ Özdemir, 116

²¹⁴ Özdemir, 115

²¹⁵ AYMK, E. 1986/24, K. 1987/8, KT. 31.03.1987, Erişim Tarihi: 01.07.2015, <http://www.kararlaryeni.anayasa.gov.tr/Karar/Content/07af904e-5b77-47e0-96a3-9abaa9b26fe8?excludeGerekce=False&wordsOnly=False>.

organlarına, topluma ve diğer kişilere karşı korunmuştur. İnsanın mutluluğu için büyük önemi olan özel hayata saygı gösterilmesi hakkı onun kişiliği için temel bir hak olup yeteri kadar korunmadığı takdirde kişilerin ve dolayısıyla toplumun kendini huzurlu hissedip güven içinde yaşaması mümkün değildir. Bu nedenlerle söz konusu gizliliği çeşitli biçimde ihlal eylemleri suç sayılarak ceza yaptırımlarına bağlanmıştır.” ifadeleri ile yukarıdaki açıklamalarımızı destekler yönde, kişinin hayatının bu alanının özel hayat olarak nitelendirilme sebebi ve daha sonra da bu alanın neden yasal olarak korunduğu belirtilmiştir.

Kişi hayatının üçüncü kısmı olan sır alanı ise, kendisi dışındaki tüm bireylerden gizli tuttuğu, ancak yine kendisinin inisiyatifi ile bazı kimselerin bilgi sahibi olmasını istediği hayat alanıdır²¹⁶. Bu alana hiçbir müdahale mümkün olamayacaktır ki bu alan kişinin dokunulmaz alını ifade eder²¹⁷. Çünkü bu hak kişilik hakkının temelini teşkil etmesi münasebetiyle bu hakkın başka hiçbir hak veya bir durum ile değer yarışına tabi tutulması mümkün olmayacaktır²¹⁸. Burada sır kavramının belirlenmesi, bu alanın tespiti için önem kazanmaktadır. İlgilisi dışındaki kişilerce bilinmeyen durum, olay veya bir davranış sır olarak kabul edilmektedir²¹⁹. Bu alan içerisinde kişiye ait kişisel veri olarak nitelendirilebilecek birçok bilgi vardır. Kişinin dini, felsefi, cinsel yaşamı, ırksal kökeni, sağlık durumu gibi hassas veri olarak kabul edilen veriler de bu alanda yer alabilir. Dolayısıyla kişinin özel hayatının sır alanına, ilgilinin rızası hilafına girilerek kişisel verilere ulaşılması, hem bu verilerin sır olmasını hem de kişisel verilerin korunması hakkını ihlal edecektir.

Devlet gerçekleştirmek durumunda olduğu kamu hizmetleri açısından, özel sektör de sunmak istediği kendi hizmetleri açısından bireylerin özel hayatlarına ait farklı farklı verilere sahip bulunmaktadır. Bu verilerin kamu kurum ve kuruluşları ile özel kuruluşların elinde bulunması, özel hayatın gizliliği ve doğal olarak da kişisel verilerin korunması hakkının ihlali ihtimalini doğurmaktadır²²⁰. Dolayısıyla bireylere ait bilgi güvenliğinin, özel hayatın gizliliği ve kişisel verilerin korunması hakları açısından oldukça büyük bir öneme sahip olduğu görülmekle birlikte kişisel verilerin korunmasına

²¹⁶ Özdemir, 117

²¹⁷ Şimşek, 140

²¹⁸ Şimşek, 140

²¹⁹ Özdemir, 117

²²⁰ Döner, 259

yönelik tali düzenlemelerden ziyade temel bir kanunun varlığının da önemi ve gerekliliği de hissedilmektedir.

Doktrinde diğer bir görüşe göre özel hayatın gizliliğinin kapsamında dört farklı alanın varlığı söz konusudur. Bunlar;

- Bilgi mahremiyeti : Kişi ile ilgili bilgilerin bulunduğu alan,
- Vücut mahremiyeti : Kişinin fiziksel bütünlüğü ile ilgili alan,
- İletişim mahremiyeti : Kişinin iletişim alanlarının ve araçlarının mahremiyeti,
- Yaşama alanı mahremiyeti: Kişinin konutu, işyeri gibi yaşam faaliyetlerini

sürdürdüğü alanlardır²²¹.

Özel hayat içerisinde bilgi mahremiyeti alanının varlığı, kişisel verilerin korunmasının, özel hayatın gizliliği hakkı kapsamında mümkün olabileceğinin göstergesi durumundadır. Ayrıca birçok ulusal düzenlemelerde, kişisel verilerin korunması hakkının anayasal temelinin, özel hayatın gizliliği ve korunması hakkı kapsamında olduğu belirtilmiştir²²².

- Haberleşme Özgürlüğü (m. 22)

Anayasa m. 22’de herkesin haberleşme hürriyetine sahip olduğu düzenlenmiş ve haberleşmenin gizliliğinin asıl olduğu belirtilmiştir. Ancak maddenin ikinci fıkrasındaki nedenlere dayanılarak haberleşme hürriyetinin sınırlandırılması söz konusu olabilecektir.

Haberleşme hürriyeti ile yapılan haberleşmelerin gizliliği ve güvenilirliği koruma altına alınmak istenmiştir. İnsanlar arasında bağlantı kurabilen, bu suretle bilgi veya haber ileterek haberleşmeyi sağlayan araçlar (telefon, faks, e-posta, telgraf vb.) bu özgürlüğün kapsamındadır²²³. Özellikle teknolojinin de gelişmesi ile birlikte haberleşme araçlarına, dolayısı ile de haberleşmenin içeriğine erişimin imkân dâhilinde olması, haberleşmenin gizliliğinin ihlali sonucunu doğurmaktadır. Bu ihlal, hukuka aykırı olarak haberleşmenin içeriğine ulaşılacak suretiyle kişisel verilerin ele geçirilmesi ve yayılması ihtimalini de kapsamaktadır. Bu durum kişisel verilerin işlenmesinde geçerli ilkelerden hukuka uygunluk ve dürüstlük ilkelerine de ters düşmüş olacaktır²²⁴. Diğer yandan haberleşme hürriyeti kapsamına ayrıca trafik verileri de diyebileceğimiz

²²¹ Okur, 11

²²² Küzeci, 261

²²³ Hayrunnisa Özdemir, “Haberleşmenin Gizliliği ve Kişisel Veriler”, *EÜHFD*, XIII(1-2), yıl 2009, 287

²²⁴ Şimşek, 149

kişilerin isimleri, adresleri, tarafların telefon numaraları gibi kişisel verilere de ulaşılması mümkündür²²⁵.

Yukarıda yapılan açıklamalarda görüldüğü üzere, haberleşme hürriyeti ve haberleşmenin gizliliği ile kişisel verilerin korunması açısından oldukça önem arz eden bir temel haktır. Bu çerçevede yapılan haberleşmenin içeriğinin ve bu içeriğin gizliliğinin anayasanın bu hükmü ile koruma altında olması, kişisel verilerin de anayasal bir korumaya sahip olduğunu göstermektedir.

- Düşünce ve Düşünceyi Açıklama Özgürlüğü (m.25-26)

Anayasanın 25. maddesinde düşünce ve kanaat özgürlüğü, 26. maddesinde de düşünceyi açıklama ve yayma özgürlüğü düzenlenmiştir. Düşünce özgürlüğü, madde 25/2 metninde yer alan “*Her ne sebep ve amaçla olursa olsun kimse, düşünce ve kanaatlerini açıklamaya zorlanamaz, düşünce ve kanaatleri sebebiyle kınanamaz ve suçlanamaz.*” ifadesinden de anlaşılacağı üzere mutlak surette korunan bir haktır. Ayrıca bir kimse için düşünce ve kanaat özgürlüğünün sınırlandırılması, bu düşünce ve kanaat dışı vurulmadığı müddetçe de mümkün olamayacaktır.

Kişisel verilerin korunması açısından, kişinin, bazı faaliyetleri, özellikle internet ortamında yapılan faaliyetlerin bir iz bırakması, bu izlerden ve diğer faaliyetlerinden yola çıkılarak kişinin düşünceleri ve kanaatleri hakkında bilgi sahibi olunabilmesinin mümkün olduğu söylenebilir²²⁶. Gerçekten de kişinin düşüncelerini ve kanaatlerini oluştururken örneğin okuduğu kitaplar, dergiler, gazeteler, internette ziyaret ettiği siteler gibi faaliyetleri, o kişinin düşüncelerine ve kanaatlerine dair bir fikir oluşturabilir. Burada, kişinin düşüncelerini açıklamak gibi bir niyeti olamamasına karşılık düşünce özgürlüğünün ihlali söz konusu olabilir. Böyle bir durum, kişisel verilerin korunması açısından önem arz edecektir.

Kişiler, Anayasa m. 26 kapsamında sahip olduğu düşünce ve kanaatleri, çeşitli araçlarla açıklama ve yayma özgürlüğüne sahiptirler. Bu hakkın varlığı, kişinin kendi iradeleriyle karar alabilmesi ve kendisini ifade edebilmesi için önemlidir²²⁷. Herkes bu hakka sahip olmakla birlikte, düşünceyi açıklama ve yayma hürriyeti, maddenin ikinci fıkrasında sayılan sebeplerle²²⁸ sınırlandırılması mümkündür. Diğer yandan kimi zaman

²²⁵ Özdemir, 287

²²⁶ Küzeci, 271

²²⁷ Şimşek, 145,

²²⁸ Anayasa m. 26/2 “...milli güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların

kişiler, mesleklerinden ya da bulundukları statülerden dolayı bazı disiplin kurallarına tabi olabilirler. Bu kurallar gereği de ifade özgürlüğü açısından bazı kısıtlamalara tabi tutulmaları söz konusu olabilir. Devlet memurları, avukatlar, doktorlar bu duruma örnek gösterilebilirler. Ancak bu durum ifade özgürlüğünün ihlali sayılmamaktadır.

Kişinin düşünce ve kanaatleri her türlü içeriğe dair olabileceği gibi kişisel verilere yönelik de olabilir. Kişinin bu tür verilere dair olan düşüncelerini serbestçe açıklaması, yayması, açıklamaması ve de açıklamaya zorlanamaması noktasında bu hakkın varlığı anayasal bir güvence sağlamaktadır.

- Toplantı Özgürlüğü (m. 34)

Anayasa m. 34'te düzenlendiği üzere, herkesin, önceden izin almaksızın, silahsız ve saldırısız olmak şartıyla, toplantı düzenleme yetkisi vardır. Bu hak mutlak olmayıp, maddenin ikinci fıkrasında düzenlenen özel sebeplerle sınırlandırılabilir.

Toplantı hakkı, bireyin topluma karşı kendisini ifade edebilme yollarından birisidir. Bu hak kişilerin fikir alış verişinde bulunmasına, bir araya gelerek ortak menfaatlerini savunmaya imkân tanıyan haktır²²⁹. Diğer bir ifadeyle kişilerin düşüncelerini açığa vurmak amacıyla toplanabilmelerini öngören özgürlüktür. Kişisel veriler açısından bakıldığında, bu yönde bir toplantıya katılan bir kişinin, bu toplantıya katılmakla, toplantının amacına göre siyasi, felsefi vb. düşünceleri, fikirleri herkesçe bilinmekte, ismi, kimliği belli olmaktadır. Bu durum ilgili kişi tarafından önceden öngörülebilecek bir durumdur. Zira bu durum, kamuya açık bir toplantıya katılmanın doğal sunucudur. Burada kişisel veriler açısından dikkat edilmesi gereken husus şudur ki, hukuka uygun olarak kullanılan toplantı hakkı neticesinde elde edilen bu kişisel verilerin hukuka aykırı olarak kullanılmaması gerekmektedir. Aksi durum kişilerin hem toplantı hak ve özgürlüğünü hem de kişisel verilerin korunması haklarının ihlali olacaktır²³⁰.

cezalandırılması, Devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amacıyla sınırlandırılabilir."

²²⁹ Şimşek, 147

²³⁰ Şimşek, 147-148

2.2.3.1.2. 5237 sayılı Türk Ceza Kanunu

5237 sayılı Ceza Kanununun Dokuzuncu Bölümü altında *Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar* düzenlenmiştir. Bölüm başlığı da göstermektedir ki, burada korunan hukuki değer özel hayat ve özel hayatın gizliliğidir. TCK'da özel hayatın tanımı yapılmamıştır, ancak kısaca özel hayat, kişinin genel hayatından daha dar kapsamlı olan, bu kapsamda sadece kişinin paylaştığı kişilerce bilinen, daha çok gizli kalmasını istediği hayatıdır²³¹. Kişisel verilerin, özel hayatın bir boyutu olması, bu verilerin de ancak ilgilinin bilmesini istediği kişilerce bilinmesi, yani kişisel veri sahibinin rızası bulunmadıkça her hangi bir işlem ya da eyleme tabi olamayacağından dolayı, kişisel verilerin korunmasına yönelik cezai hükümlerin bu bölüm altında düzenlenmesi yerinde olmuştur. TCK kapsamında kişisel verilerin tanımı yapılmamıştır. 135. maddenin gerekçesinde, gerçek kişiye ait her türlü verinin kişisel veri kabul edileceği belirtilmiştir. Bu belirleme, maddelerin uygulama alanının görülmesi ve dolayısıyla da kişisel verilerin korunması açısından önemlidir.

Bu bölüm içerisinde yer alan 135 vd maddeler, madde başlıklarından da anlaşılacağı üzere, doğrudan kişisel verilerin korunmasına yönelik düzenlemelerdir. Bölüm altındaki ilk üç madde ise haberleşmenin gizliliğinin, kişiler arasındaki konuşmaların dinlenmesinin ve kayda alınmasının ve özel hayatın gizliliğinin ihlaline yönelik hükümlerdir. Ancak yukarıdaki başlık altında da belirtildiği üzere, haberleşme özgürlüğü, özel hayatın gizliliği de kişisel verilerle yakından ilgilendiren kavramlardır. Burada 5237 sayılı kanun kapsamında doğrudan kişisel verilerle ilgili olan cezai hükümlere değinilecektir.

Özel Hayatın Gizliliğini İhlal (m. 134)

134. madde metninde kişilerin özel hayatlarını ihlal eden kimsenin cezalandırılacağı hüküm altına alınmıştır. Suçla korunan hukuki yarar, kişilerin özel hayatları ve özel hayatlarının gizliliğinin sağlanmasıdır²³². Bu suçun, her türlü eylemle işlenmesi mümkündür. Ancak birinci fıkranın ikinci cümlesinde ayrıca düzenlendiği üzere, bu suçun görüntü veya ses kaydı yapılmak suretiyle işlenmesi halinde daha ağır yaptırım uygulanacağı belirtilmiştir. Burada açıkça görüldüğü gibi, görüntü veya ses

²³¹ Okur, 6

²³² Ali Parlar, Muzaffer Hatipoğlu, *5237 Sayılı Türk Ceza Kanunu Yorumu*, Seçkin Yayıncılık, Ankara 2010, 2080; Veli Özer Özbek, *Yeni Türk Ceza Kanununun Anlamı*, Seçkin Yayıncılık, Ankara 2008, 940

kayıtlarının, doğrudan veya dolaylı olarak bir kişiye ait olmaları, onları belirlenebilir kılımları sebebiyle kişisel veri olarak kabul edilecek verilerdir. Kolaylıkla anlaşılacağı üzere özel hayatın gizliliğini ihlal suçu ile korunan hukuki yarar ile kişisel verilerin korunması hakkı kapsamında korunmak istenen menfaat örtüşmektedir.

- Kişisel Verilerin Kaydedilmesi (m. 135)

Günümüzde, teknoloji ve bilimin geldiği seviye ile birlikte bazı kurum ve kuruluşlar, hizmetlerin sunulmasında kişilerle ilgili bilgilere ihtiyaç duymaktadır. Bu bilgilerin toplandıkları amaç haricinde kullanılmaları veya yayılmaları, ilgili kişiler için tehlikeli sonuçlar doğurabilir. Bu nedenle, 5237 sayılı Kanun m. 135’de “(1) *Hukuka aykırı olarak kişisel verileri kaydeden kimseye ... hapis cezası verilir. (2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmü göre cezalandırılır.*” hükmü ile kişisel verilerin hukuka aykırı olarak kaydedilmesi suç olarak düzenlenmiştir. Bu madde kapsamında bir kişiye ait her türlü bilgi kişisel veri olarak kabul edilmektedir²³³. Yine bu suç ile korunan hukuki değer de özel hayatın gizliliği ve korunması hakkıdır²³⁴. Suçun oluşabilmesi için, madde metninde de açık olduğu üzere, verilerin hukuka aykırı olarak kaydedilmiş olması gerekmektedir. 5237 sayılı Ceza Kanununda düzenlenmiş olan hukuka uygunluk halleri burada önem kazanmaktadır. Tasarının kanunlaşması ile birlikte burada yer alan hukuka uygunluk halleri de dikkate alınacaktır.

Maddenin ikinci fıkrasında, kişisel veri türü olarak hassas verilerin kayda geçirilmesi suç olarak düzenlenmiştir. Dikkat çeken nokta, burada hassas verilerin kaydının hukuka aykırı olarak işlenmesi ibaresine yer verilmemiş olmasıdır. Buradan hassas verilerin hiç bir şekilde kayda alınamayacağı anlamı çıkarılmamalıdır²³⁵. Hassas verilerin kayda alınması ya da işlenmesi, hukuki metinlerde düzenlenen istisnai durumlarda mümkün olabileceğinden, bu istisnai haller haricindeki tüm kayıt ya da işleme faaliyeti suç oluşturmaktadır.

²³³ TCK 135. madde gerekçesi

²³⁴ Parlar, Hatipoğlu, 2087; Özbek, 948

²³⁵ Hassas verilerin hangi hallerde işlenebileceğine dair bkz. s. 18

Bir diğerk durum ise, kişisel verilerin ne şekilde kayıt altına alınacağıının, bu suçun oluşması açısından önem arz etmemesidir. Yani madde gerekçesinde de belirtildiğı üzere, verilerin elektronik aletlerle veya elle kayıt altına alınması, suçun oluşması için yeterlidir. Kanun koyucu haklı olarak burada ayrıma yer vermemiştir. Önemli olan, kişisel verilerin hukuka aykırı olarak kayıt altına alınması ile ilgili kişinin bu durumda karşı karşıya kalacağı tehlikelerdir. Diğerk bir ifade ile ilgili kişinin temel hak ve özgürlüklerinin ihlalinin söz konusu olmasıdır. Bu ihlalin oluşmasında verilerin elle veyahut bilgisayar ortamında kayda alınması arasında fark olmayacağı görüşündeyiz.

- Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme (m. 136)

Kanunun bu madde hükmüne göre, kişisel verileri, hukuka aykırı olarak başkalarına verme, yayma ya da bu verileri hukuka aykırı olarak ele geçirme suç olarak düzenlenmiştir. Suçun oluşması için madde metninde sayılan seçimlik eylemlerden birinin yapılması yeterlidir. Diğerk yandan madde gerekçesinde belirtildiğı üzere, bu suçun oluşmasında, suçu işleyen açısından, yaydığı ya da verdiği veya ele geçirdiğı kişisel verilerin hukuka uygun olarak kaydedilmiş olmasının önemi yoktur. Yani kişisel veriler ister hukuka uygun olarak kaydedilmiş olsun ister olmasın, bu verileri başkalarına yayma, verme ya da ele geçirme eylemlerinden birinin gerçekleşmesi suç tipinin oluşması için yeterli olacaktır.

- Verileri Yok Etmeme (m. 138)

Kanunun 138. maddesinde *“Kanunların belirlediğı sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde ... hapis cezası verilir.”* hükmü düzenlenmiştir. Önceki başlıklar altında da incelendiğı üzere, kişisel verileri kaydetme hakkına sahip olanlar, bu kayıtları süresiz olacak şekilde elinde bulundurma hakkına sahip değildirlr. Aksi halde ilgili kişi açısından temel hak ve özgürlüklerin sürekli bir tehdit altında olması durumu söz konusu olacaktır. 138. madde hükmü ile süresi içerisinde elinde bulundurduğu verileri yok etmeyen kimsenin cezalandırılması, bu anlamda bir koruma sağlamaktadır.

Bu düzenleme ayrıca, ihtiyaç duyulmayan, işlenmesiyle elde edilmek istenen amaç gerçekleştirilmiş olan kişisel verilerin yok edilmesi, verileri elinde bulunduranlar açısından keyfi uygulamaları da önleyici nitelikte olmasından dolayı önemlidir²³⁶.

Verileri yok etmeme suçunu ceza kanunu kapsamında, kişisel verilerin korunmasına yönelik diğer suçlardan ayıran bir nokta, bu suçun özgü suç olmasıdır. Bu suçun faili, kanunen kendisine kişisel verileri silme, yok etme yetkisi verilmiş olan kimsedir²³⁷.

2.2.3.1.3. 5271 sayılı Ceza Muhakemesi Kanunu

5271 sayılı kanun kapsamında da kişisel verileri kapsayacak düzenlemelere yer verilmiştir. CMK' nın "*Genetik inceleme sonuçlarının gizliliği*" yan başlıklı 80. maddesinde, 75, 76, 78. maddelere gönderme yaparak bu madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçlarının kişisel veri niteliğinde olduğu ifade edilmiştir²³⁸. Örneklerin neler olduğuna ilişkin düzenleme, m. 75/1' de "*Bir suça ilişkin delil elde etmek için şüpheli veya sanık üzerinde iç beden muayenesi yapılabilmesi ya da vücuttan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınabilmesine...*" hükmünden anlaşılmaktadır. Buna göre madde metninde sayılan kan veya benzeri biyolojik örnekler ile saç, tükürük ve tırnak gibi örnekler kişisel veri olarak nitelendirilmiştir. Aynı şekilde m. 76' da da m. 75' te sayılan örnekler zikredilmiştir. İki madde arasındaki fark kişisel veri olarak nitelendirilen bu verilerin şüpheli veya sanık ya da mağdurun vücudundan alınan örnekler olmasıdır. Madde 78/1' de "*75 ve 76. maddelerde öngörülen işlemlerle elde edilen örnekler üzerinde, soy bağıının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için zorunlu olması halinde moleküler genetik incelemeler yapılabilir. Alınan örnekler üzerinde bu amaçlar dışında tespitler yapılmasına yönelik incelemeler yasaktır.*" hükmü düzenlenmiştir. Madde metninden anlaşılaçağı üzere, 6698 sayılı Kanun kapsamında kişisel verilerin işlenmesinde geçerli olan amaca

²³⁶ Küzeci, 291

²³⁷ Zeki Hafizoğulları, Muharrem Özen, *Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*, Ankara Barosu Dergisi, yıl 67,s. 4, Güz 2009, 22

²³⁸ Erdener Yurtcan, *CMK Şerhi*, Cilt I, 7. Baskı, Adalet Yayınevi, Ankara 2015, 306; Fatih Selami Mahmutoglu, *Beden Muayenesi ve Vücuttan Örnek Alınması*, 23, Erişim Tarihi: 15.08.2016, <http://fsmahmutoglu.av.tr/pdf/76b00da1de336791f454b4977f6319d9cdf4656d7818071225.pdf>.

uygunluk ilkesine²³⁹ vurgu yapılmıştır. CMK kapsamında bu bulguların elde edilmesinin ve incelenmesinin amacı olarak, soruşturma veya kovuşturma konusu suç ile ilgili olmak üzere delil toplamaktır²⁴⁰. Buna göre beden muayenesi ve vücuttan örnek alınması ile genetik inceleme neticesinde elde edilen bulgular başka bir amaç için kullanılamayacak, CMK m. 80/ f. 2 hükmü gereğince de kovuşturmayaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararının verilip kesinleşmesiyle elde edilen bu veriler cumhuriyet savcısının huzurunda yok edilmesi gerekmektedir.

CMK m. 81'de üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren suçlarda, şüpheli veya sanığın kimliğinin tespit edilmesinin gerekli olması halinde fotoğrafının, beden ölçülerinin, parmak veya avuç içi izinin, teşhisi kolaylaştıracak diğer özelliklerinin, sesinin ve görüntülerinin kayda alınmak suretiyle soruşturma veya kovuşturma dosyasına konulmasına imkân sağlanmıştır. Madde metninde zikredilen bilgilerin de birer kişisel veri oldukları açık olup bunların da yine usulünce işlenmesi gerekmektedir.

2.2.3.2. 6698 sayılı Kişisel Verilerin Korunması Kanunu

6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında hangi hükümlerin düzenlendiği, veri koruma hukukuna ilişkin uluslararası düzenlemelerle karşılaştırılmasına değinmeden önce neden ayrı bir veri koruma kanununa ihtiyaç duyulacağının incelenmesinin faydalı olacağı düşüncesindeyiz.

2.2.3.2.1. Kişisel Verilerin Kanun Yoluyla Korunmasına Duyulan İhtiyaç

Kişisel verilerin iç hukukumuzda düzenlenecek özel bir kanunla güvence altına alınması çeşitli açılardan bir ihtiyaçtır. Hangi açılardan bu kanuna ihtiyaç duyulduğu aşağıda iki alt başlık altında açıklanmaya çalışılmıştır.

²³⁹ Amaca uygunluk ilkesi için bkz. s. 30 vd.

²⁴⁰ Haluk Çolak, Mustafa Taşkın, *Ceza Muhakemesi Kanunu Şerhi*, Seçkin Yayıncılık, Ankara 2007, 349 vd.

2.2.3.2.1.1. Kişisel Verilerin Esasını Oluşturan Hususların Bağımsız Bir Kanun ile Düzenlenmesi Açısından

Konu ile ilgili mevzuat içinde farklı hukuki düzenlemelerin bulunmasının, başlı başına veri koruma hukukunun amacını yansıtamayacağı ve bu noktada kişisel verilerin korunmasına duyulan ihtiyacı karşılayamayacağı ifade edilebilir. Örneğin 5237 sayılı TCK ilgili maddelerinde kişisel verilerle ilgili hükümler düzenlenmiştir. Bu hükümlerde karşımıza çıkacak olan, kişisel verilerle ilgili suç oluşturan eylemlerin işlenmesi durumunda, bu suçların karşılığı olan yaptırımlardır. Diğer bir ifade ile kişisel verilerle ilgili bir suçun işlenmesi durumunda TCK’ daki bu konuya ilişkin hükümlerin amacı bozulan kamu düzenini tekrar sağlamak olacaktır. Dolayısıyla bu şekilde değişik kanun hükümlerindeki düzenlemelerle kişisel veri, verilerin korunması, işlenmesi, transferi... gibi Veri Koruma Hukukunun temel anlayışını, ilkelerini, esaslarını ortaya koymak mümkün olmayacaktır. 2008 tarihli Kişisel Verilerin Korunması Kanun Tasarısı Genel Gerekçesinde bu durum “... bir ülkenin mevzuatında değişik düzenlemeler içinde yer alan farklı hükümlerin, bu konuya özgü felsefeden yoksun olması halinde kişisel verilerin korunması konusunda artan ihtiyaca cevap vermesi mümkün olmamaktadır...” ifadesi ile açık bir şekilde ortaya koyulmuştur²⁴¹. Gerekçenin devamında da kişisel verilerle ilgili farklı düzenlemelerde yer alan hükümlerin kişisel verilerin korunması amacıyla getirilen düzenlemeler olmadığı, bilakis bu düzenlemelerin ait oldukları alanın ihtiyaçlarını karşılamak üzere getirilmiş oldukları, doktrinde de benzer şekilde olmak üzere mevzuatımızda veri koruma ile ilgili dağınık düzenlemelerin yer aldığı, ancak bu düzenlemelerin veri korumanın temel ilkelerini yansıtmayacağı, bu durumun da önemli bir eksiklik olduğu açıkça belirtilmiştir²⁴². Bu ifadeler neticesinde kişisel verilerin korunmasına yönelik münhasıran bir kanuni düzenlemenin zorunluluk arz ettiği açıktır.

2.2.3.2.1.2. Uluslararası Üyeliklerin Gereklerinin Yerine Getirilmesi Açısından

Türkiye, birer uluslararası örgüt olan AK, BM ve OECD ‘nin üyesidir. Bu örgütler, önceki başlıklarda değinildiği üzere kişisel verilerin korunmasına yönelik uluslararası belgeler yayınlamışlardır. BM ve OECD tarafından yayınlanan bu belgelerde kişisel verilerin korunmasına yönelik rehber ilkelere yer verilmiştir ve bu

²⁴¹ Bkz. 2008 tarihli KVKKT Genel Gerekçesi

²⁴² Aynı yönde bkz. Şimşek, 191 vd.; Küzeci, 351

belgelerin üye devletler açısından bir bağlayıcılığı olmadığını daha önce belirtmiştik²⁴³. Bu belgeler daha çok devletlerin iç hukuklarında kişisel verilerin korunmasına yönelik yapacakları hukuki düzenlemelerde tavsiye niteliği taşımaktadırlar. Ancak AK'ın 108 sayılı sözleşmesi uluslararası alanda bağlayıcılığı olan bir düzenlemedir²⁴⁴. Bu sözleşmede yer alan hükümlerin üye devletlerin iç hukuklarında yürürlük kazanabilmeleri, üye devletlerin gerekli önlemleri almış olmaları şartına bağlanmıştır²⁴⁵.

Veri koruma hukukunun uluslararası temel hukuki metinlerinden birisi olan 1981 tarih ve 108 sayılı sözleşmesi ülkemizce imzalanmıştır. Ancak iç hukukumuzda kişisel verilerin korunmasına dair münhasır kanunumuz olan 6698 sayılı KVKK'nın 2016 yılında kabul edilmesi, bu uluslararası sözleşme hükümlerinin yürürlüğe girmesini de geciktirmiştir. Sözleşme hükümlerinin iç hukukumuz açısından yürürlüğe geç girmesi dolayısıyla yeterli güvencenin sağlanamadığı düşünülerek, uluslararası işbirliği ile yürütülmesi planlanan hususlarda yurtiçine veri transferi noktasında ciddi sorunlarla karşılaşmıştır²⁴⁶. Bu açıdan tasarının bir an önce yasalaşması ayrı bir önem arz etmekteydi.

Diğer yandan Türkiye'nin AB'ye Aralık 1999 tarihinde tam üye adayı olarak kabul edilmesinden itibaren birçok alanda mevzuat uyum çalışmaları başlatılmıştır. Bu alanlardan biri de veri koruma hukuku alanıdır. Her yıl Komisyon tarafından Türkiye

²⁴³ Bkz. s. 48 vd

²⁴⁴ Küzeci, s. 119, 124, 130

²⁴⁵ 108 sayılı AK Sözleşmesi m. 4

²⁴⁶ 2008 tarihli Tasarı Genel Gerekçesinde, adli yardım anlaşmalarının uygulanması çerçevesinde, Konseye üye diğer devletler, Türk mahkemelerince yapılan kişiler hakkındaki adres tespiti, istinabe gibi işlemleri, Türkiye'nin konuya ilişkin eşdeğer koruma mevzuatı bulunmadığı gerekçesi ile geri çevirmeleri ve gümrük birliği çerçevesinde, Türkiye ile AB üyesi devletler gümrük idareleri arasında bilgi transferi yapılamayacağı belirtilmiştir. 6698 sayılı Kanun Genel Gerekçesinde de benzer şekilde AB tam üyelik sürecinde, müzakere fasıllarından dördünün doğrudan kişisel verilerin korunmasına dair temel bir kanunun yürürlüğe girmesi ile alakalı olduğu, yine ayrı bir veri koruma kanunu olmaması sebebiyle EUROPOL ve EUROJUST kapsamında işbirliğinin yapılamadığı belirtilmiştir. Ayrıca AB Komisyonu, 2006 yılı ilerleme raporunda veri koruma alanında münhasır bir kanun bulunmaması nedeniyle gümrük işbirliğinin kolluk boyutunun pürüzsüz şekilde işleminin engellendiği, 2012 yılı ilerleme raporunda yine verilerin korunmasına ilişkin bir mevzuatın olmayışı, polis ve yargı organları arasındaki ve terörle mücadeledeki operasyonel işbirliğini engellediği, 2014 Yılı İlerleme Raporunda, Türkiye, suç ve terörle mücadeleyle ilişkin olarak polis işbirliği alanında ikili anlaşmalar imzaladığı, ancak Türkiye' de münhasır bir veri koruma kanunu bulunmamasının uluslararası düzeyde polis işbirliğini engellemeye devam ettiği, 2004 yılında Europol ile stratejik işbirliği anlaşması imzalanmış ancak yine münhasır bir veri koruma kanunu olmamasından dolayı operasyonel işbirliği anlaşması imzalanamadığı rapor edilmiştir. Belirtilen bu durumlar söz konusu münferit bir veri koruma kanununun olmamasından dolayı karşılaşılan sorunlara örnek oluşturmaktadır.

hakkında ilerleme raporları düzenlenmektedir²⁴⁷. 2006 yılı ilerleme raporunda, veri koruma alanında münhasır bir kanunun bulunmaması ve bu yüzden gümrük işbirliğinin kolluk boyutunun pürüzsüz işlemesinin engellendiği belirtilmiştir. 2007, 2008, 2011, 2012 yılları ilerleme raporlarında Türkiye'nin, kişisel verilerin korunması bakımından ulusal mevzuatını AB müktesebatı ile uyumlu hale getirmesi gerektiği rapor edilmiştir. İlk kez 2013 yılı ve devamında 2014 yılı İlerleme Raporlarında kişisel verilerin korunmasına ilişkin AB standartlarına uyumlu genel bir kanunun kabul edilmesi gerektiği rapor edilmiştir. Son olarak 2015 AB İlerleme Raporu²⁴⁸'nda kişisel verilerin korunmasına yönelik kapsamlı bir çerçeve kanunun kabul edilmesi gerektiği yinelenmiş, Avrupa standartlarıyla uyumlu, bağımsız bir veri koruma denetim otoritesinin kurulması yönünde ilerlemenin olmadığı ve Avrupa Konseyi Sözleşmesi'nin halen onaylanmadığı rapor edilmiştir.

Yukarıda yapılan açıklamalar altında Türkiye, hem AB standartlarına ulaşmak hem de uluslararası işbirliği alanında belirtilen olumsuz durumlarla karşılaşmamak için 2004, 2008, 2014 ve 2016 yıllarında Kişisel Verilerin Korunması Kanun Tasarıları hazırlanmış ve nihai olarak 24.03.2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu²⁴⁹ kabul edilerek iç hukukumuzda münhasır bir veri koruma kanunu yürürlüğe girmiştir. Böylelikle Türkiye, hem üyesi olduğu uluslararası kuruluşlarca düzenlenmiş olan rehber ilkeleri iç hukukuna yansıtmış, hem de bağlayıcı nitelikte olan 108 sayılı AK Sözleşmesinin gereğini yerine getirmiş olmuştur. Diğer yandan da AB Türkiye raporlarında, ayrı bir kişisel verilerin korunması kanunu olmamasından dolayı belirtilmiş olan eksiklikler giderilmiştir.

²⁴⁷ 2005 İlerleme Raporunda, AB Konseyi Aralık 2004'te, Türkiye ile katılım müzakerelerinin 3 Ekim 2005 tarihinde açılmasını kararlaştırmış ve planlandığı gibi bu tarihte müzakerelere başlamıştır. Bu tarih itibarı ile AB – Türkiye ilişkilerinde yeni bir döneme girildiği raporda belirtilmiştir. Bu nedenle 2005 yılı sonrası ilerleme raporları dikkate alınarak Türkiye'nin veri koruma alanındaki durumu değerlendirilmiştir. İlgili raporlara erişim için bkz., Erişim Tarihi: 15.05.20, <http://www.abgs.gov.tr/index.php?p=46224>.

²⁴⁸ 2015 yılı AB İlerleme Raporu'nda ayrıca Türkiye açısından kişisel verilerin korunması alanında gerekli düzenlemelerin yapılmasını gerekli kılan nedenlere de yer verilmiştir. Raporda, vize serbestisi kapsamındaki gereklilik yanında Eurojust ve Europol ile operasyonel işbirliği anlaşmalarının imzalanabilmesi ve terörle mücadele dâhil AB üye devletleri adli ve polis işbirliğinin güçlendirilmesi açısından gerekliliği belirtilmiştir. Ayrıca bu alanda gelişme kaydedilmemesinden dolayı Milli İstihbarat Teşkilatına ilişkin mevcut mevzuat ile Milli İstihbarat Teşkilatına ve Telekomünikasyon İletişim Başkanlığına geniş yetkiler veren İnternet Kanunundan dolayı duyulan endişelere de Raporda yer verilmiştir. 2015 yılı Türkiye Raporu için bkz. Erişim Tarihi: 15.05.2015, http://www.ab.gov.tr/files/000files/2015/11/2015_turkiye_raporu.pdf.

²⁴⁹ 6698 sayılı KVKK 07.04.2016 tarih ve 29677 sayılı RG'de yayımlanarak hükümlerinin büyük bir kısmı yayımı tarihinde, bir kısmı ise yayımından altı ay sonra yürürlüğe girecektir.

2.2.3.2.2. 6698 sayılı Kişisel Verilerin Korunması Kanun Hükümleri

Bu başlık altında Kanun'un sistematigi ve Kanun metni kapsamında düzenlenen hükümlere yer verilecektir. Önceki başlıklarımız altında 108 sayılı Avrupa sözleşmesi, 95/46/AT sayılı Direktif, OECD ve BM Rehber İlkeleri ve Kanun hükümleri birlikte değerlendirilerek açıklamalarda bulunulduğu için burada genel bir inceleme yoluna gidilecektir.

2.2.3.2.2.1. Kanun'un Sistematiği Görünümü

6698 sayılı Kanun'un sistematik yapısına bakıldığında Kanun'un yedi bölümden oluştuğu görülmektedir.

Birinci bölümde, Kanun'un amacı, kapsamı ve bu Kanun'un uygulanmasında kullanılan kavramların tanımlarına yer verilmişken; ikinci bölümde ise “*Kişisel Verilerin İşlenmesi*” başlığı altında kişisel verilerin işlenmesinde geçerli olan ilkeler, bu verilerin hangi şartlar altında işlenebileceği hususları düzenlenmiştir. Kanun'un üçüncü bölümünde kişisel verilerin işlenmesi kapsamında veri sorumlusunun yükümlülüğü ve ilgilinin sahip olduğu haklar, “*Haklar ve Yükümlülükler*” başlığı altında hüküm altına alınmıştır. Dördüncü bölümünde “*Başvuru, Şikâyet ve Veri sorumluları Sicili*” hakkında düzenlemelere yer verilen Kanun'un beşinci bölümünde ise “*Suçlar ve Kabahatler*” başlığı altında 5237 sayılı Türk Ceza Kanunu'na atıfta bulunulmak suretiyle kişisel verilere ilişkin suçlar bakımından esas alınacak kanun hükümleri belirlenmiştir. 6698 sayılı Kanun'un beşinci bölümünde ayrıca bu Kanun'un çeşitli maddelerindeki düzenlemelere aykırı davrananlara uygulanacak idari para cezaları da açıkça düzenlenmek suretiyle aydınlığa kavuşturulmuştur. Kanun'un altıncı bölümünde, bu Kanunla verilen görevleri yerine getirmekle görevli Kişisel Verileri Koruma Kurumu ve Teşkilat yapısı hakkında düzenlemelere yer verilmiş; yedinci ve son bölümde ise “*Çeşitli Hükümler*” başlığı altında Kanun'un uygulanmayacağı haller başta olmak üzere çeşitli uygulama ve geçiş hükümlerine yer verilmiştir.

2.2.3.2.2.2. Kanun Hükümleri

Kanun'un “*Amaç*” yan başlığını taşıyan 1. maddesinde, AB ilerleme raporlarında da istenildiği üzere 95/46/AT sayılı Direktife ve 108 sayılı Avrupa Konseyi

Sözleşmesine uygun olarak “...*kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları esas ve usulleri düzenlemektir.*” hükmüne yer verilmiştir. Madde metninden ve madde gerekçesinden da anlaşıldığı üzere kişisel verilerin işlenmesinin bir disiplin altına alınması ve bu suretle mahremiyet ve bilgi güvenliği haklarının da korunmasını kapsama dâhil etmek üzere kişi temel hak ve özgürlüklerinin korunması amaçlanmıştır.

Kanun’un 2. maddesinde Kanun hükümlerinin, kişisel verileri işlenen gerçek kişiler ile bu verileri işleyecek olan gerçek ve tüzel kişiler hakkında uygulanacağı belirtilmek suretiyle Kanun’un kapsamı düzenlenmiştir. Hem 95/46/AT sayılı Direktif hem de 108 sayılı sözleşme hükümleri sadece gerçek kişiler için uygulama alanı bulacağını en başta belirtmiştik. İç hukukumuz açısından ise 2008 tarihli Tasarıda kişisel verilerin hem gerçek hem de tüzel kişiye ait olabileceği ilgili madde metninde ifade edilmişti. 2014 tarihli Tasarı ve yürürlükte bulunan 6698 sayılı Kanun’da ise tüzel kişilere ait verilerin bu kanun kapsamında değerlendirilmeyeceği, maddenin lafzından anlaşılmaktadır. Tüzel kişiler Kanun’un bu düzenlemesi ile kapsam dışı bırakılarak uluslararası düzenlemelerle uygun hükme yer verilmiş olunmuştur²⁵⁰. Aynı madde kapsamında, kişisel verilerin otomatik veya otomatik olmayan yollarla işlenmesi arasında bir fark gözetilmemiş, her iki surette işleme yapılması durumunda uyulması gereken kurallar düzenlenmiştir. Kanun’a göre, verileri işleyecek olan kamu veya özel sektör olması fark etmeksizin Kanun hükümleri uygulanacaktır.

Kanun’un 4. maddesinde, uluslararası düzenlemelere benzer şekilde olmak üzere kişisel verilerin işlenmesinde genel ilkelere yer verilmiştir. Maddenin birinci fıkrasında, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul esaslara uygun olarak işlenebileceği ifade edilerek, veri koruma alanında kanunilik ilkesinin yeri belirlenmiştir. Belirtmek gerekir ki, bu ilkenin varlığı uygulamada keyfiliğin önlenmesi açısından önem arz etmektedir. Kanun gerekçesinde düzenlemenin içeriğine dair bir açıklama yer almaz iken 2008 tarihli Tasarıda aynı düzenlemeye karşılık gelen madde gerekçesinde kanunilik ilkesi ile bireylerin özel hayatlarının korunması ve verilerin işlenmesinde keyfiliğin önüne geçilmesi amaçlandığı belirtilmiştir. Tasarı gerekçesinde belirtilen amaç aynı zamanda bu ilkenin, kişisel verilerin korunması altında yatan,

²⁵⁰ Tüzel kişilerin veri koruma kapsamında değerlendirilmesi ile ilgili olarak bkz. s.4 vd.

bireylerin temel hak ve özgürlüklerinin korunması amacı açısından ne kadar önemli olduğunu da ortaya koymaktadır. İkinci fıkrada beş bent halinde kişisel verilerin işlenmesine ilişkin ilkeler düzenlenmiştir. Buna göre kişisel veriler belirli, açık ve meşru amaçlar için toplanmalı ve toplandıkları amaçlara aykırı olarak tekrar işlenmemek üzere toplandıkları amaç ile bağlantılı, yeterli ve ölçülü olacak şekilde doğru ve güncel tutulmak suretiyle, hukuka ve dürüstlük kurallarına uygun olarak işlenmelidir. Son olarak da ilgili kişilerin kimliklerini belirtecek şekilde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar muhafaza edilmesi gerektiği düzenlenmiştir.

Kanun'un 5. maddesinde²⁵¹ kişisel verilerin işlenme şartlarına yer verilmiştir. 2008 tarihli Tasarı'da madde başlığı "*Hukuka uygunluk halleri*" iken 2014 tarihli Tasarı ve 6698 sayılı Kanun'da, madde başlığını "*Kişisel verilerin işlenme şartları*" olarak değiştirilmiştir. Madde başlıkları farklı olsa da madde içerikleri benzer hükümler ihtiva etmektedirler. Söylenebilir ki, kişisel verilerin işlenmesinde, işlemenin hukuka uygun olması, bu işlemenin hangi şartlar altında yapılacağı ile ilgilidir. Dolayısıyla bu şartlar aynı zamanda veri işleme eylemini hukuka uygun kılacağı için her iki madde başlığı da nitelik olarak farklılık arz etmemektedir. Bu anlamda kişisel verilerin korunması hukukunda verilerin işlenememesi kural, işlenebilmesi istisna olduğundan²⁵², kişisel verilerin işlenme şartları ayrı bir önem arz etmektedir. Maddenin birinci fıkrasında ilgilinin açık rızası olmaksızın kişisel verilerin işlenemeyeceği hükmü ile ilk şart olarak rıza beyanı düzenlenmiş, ancak rızanın tanımı yapılmamıştır. Madde gerekçesinde ise 95/46/AT sayılı Direktif m.2/h' ye atıfta bulunularak buradaki tanıma yer verilmiştir. Maddenin ikinci fıkrasında ise yedi bent halinde kişisel verilerin işlenmesinde diğer şartlar düzenlenmiştir. Bu şartlar, aslında ilgili kişinin rızası olmasa dahi bazı hallerde kişisel verilerin işlenebilmesinin öngörüldüğü durumlar olarak

²⁵¹ 6698 sayılı Kanun'un 5. maddesi şu şekilde düzenlenmiştir: "(1) *Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"*

²⁵² Şimşek, 208

düzenlenmiştir. Ayrıca 5. madde ile bağlantılı şekilde Yedinci Bölüm, İstisnalar başlığı altında m. 28’de²⁵³ bu Kanun hükümlerinin uygulanmayacağı durumlara yer verilmiştir. Bu istisnalardan birinci fıkrada düzenlenenler tamamen Kanun kapsamı dışında tutulmuşken, ikinci fıkrada düzenlenen durumlar ise kısmen Kanun kapsamı dışında tutulmuştur. Zira birinci fıkrada belirtilen durumlara bu Kanun hükümleri hiçbir zaman uygulanamayacaktır. İkinci fıkra hükmüne göre ise, kural olarak bu fıkrada sayılan haller kanun hükümlerine tabi olmakla birlikte, sadece fıkrada belirtilen kanun maddelerinde düzenlenen hükümler bakımından istisna tutulmuştur.

Kanun’un 6. maddesinde²⁵⁴, önemli hususlardan biri olan özel niteliği olan kişisel veriler düzenlenmiştir. Doktrinde hassas veriler²⁵⁵ olarak da adlandırılan bu tür verilerin, başkalarınca öğrenilmesi durumunda özellikleri gereği ilgili kişinin mağduriyetine yol açabilecek ve ayrımcılık tehlikesi oluşturabilecek nitelikte veriler

²⁵³ 6698 sayılı Kanun’un 28. maddesi şu şekilde düzenlenmiştir: “(1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz: a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi. b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi. c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi. ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi. d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi. (2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz: a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması. b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi. c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması. ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.”

²⁵⁴ 6698 sayılı Kanun’un 6. maddesi şu şekilde düzenlenmiştir: “(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. (3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanın planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir. (4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.”

²⁵⁵ Hassas veri kavramı için bkz. s. 7 vd.

olmaları sebebiyle işlenemeyecekleri hüküm altına alınmıştır. Kural, bu tür verilerin işlenememesi olmakla birlikte hemen devamında belli şartların varlığı halinde özel niteliği olan bu verilerin işlenmesine müsaade eden düzenlemeye yer verilmiştir. Buna göre, özel hayatın ve aile hayatının gizliliğinin korunmasını sağlayacak yeterli tedbirlerin alınması durumunda yine maddenin ikinci fıkrasında yedi bent halinde sayılan hallerde hassas verilerin işlenmesi de mümkün olabilecektir.

Maddenin üçüncü fıkrasında, yine bu türden verilerin işlenmesine dair istisnai duruma yer verilmiştir. Buna göre birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki veriler, kanunlarda öngörülen hallerde ilgilinin açık rızası olmadan da işlenebilecektir. Cümlemin devamında ise sağlık ve cinsel hayata ilişkin hassas verilerin, ilgisinin açık rızası olmaksızın işlenebileceği istisnai durum düzenlenmiştir. Buna göre de bu tür veriler ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi gibi amaçlarla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebilecektir.

Kanun'un 7. maddesiyle hukuka uygun olarak işlenmiş olan kişisel verilerin, işlenmesini gerektiren sebebin ortadan kalkması durumunda söz konusu verilerin resen veya ilgilinin talebi üzerine silineceği, yok edileceği veya anonim hale getirileceği düzenlenmiştir. Bu hüküm, madde metninde ifade edildiği gibi artık işlenme sebebi ortadan kalkmış olan kişisel veriler bakımından, tekrar işlenmek üzere muhafaza edilmemesi veyahut yetkisiz kimselerin eline geçmesinin önlenmesi için oldukça önemli bir düzenleme içermektedir.

Kanun'un 8. maddesinde, toplanmış olan kişisel verilerin üçüncü kişilere aktarılmasına ilişkin hükümler düzenlenmiştir. Madde metninden anlaşılacağı üzere kişisel verilerin üçüncü kişilere aktarılması kural olarak yasaktır. Kişisel verilerin aktarılması, tıpkı kişisel verilerin işlenmesinde olduğu gibi ilgili kişinin açık rızasının varlığı halinde mümkün olabilecektir. Maddenin ikinci fıkrasında iki bent halinde açık rıza aranmaksızın veri aktarmanın istisnaları düzenlenmiştir. Buna göre Kanun'un m. 5/f. 2'de sayılan açık rıza olmaksızın kişisel verilerin işlenmesi şartlarından ve m. 6/f. 3'te belirtilen sağlık ve cinsel hayata ilişkin kişisel verilerin rıza olmaksızın işlenebilmesi şartlarından birinin varlığı halinde kişisel verilerin üçüncü kişilere aktarılması mümkün olabilecektir.

Kanun'un 9. maddesinde kişisel verilerin yurt dışına aktarılması ayrıca düzenlenmiştir. Kural olarak kişisel verilerin yurt dışına aktarımı yasaktır. Ancak istisnai olarak ilgili kişinin açık rızası ile kişisel verilerin yurt dışına aktarılması mümkün olabilecektir. Bu madde kapsamında da ilgilinin açık rızası olmadan verilerin aktarılmasına istisnai olarak izin verilmiştir. Buna göre 8. madde açık rıza aranmaksızın veri aktarımına imkân tanıyan hükme ek olarak aktarımın yapılacağı yabancı ülkede kişisel verilerin korunmasına ilişkin yeterli korumanın bulunması, eğer yeterli koruma bulunmuyorsa Türkiye'deki ve yabancı ülkedeki veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması şartıyla açık rıza olmaksızın, kişisel veriler yurt dışına aktarılabilir.

Kanun'un 10. ve 11. maddelerinde, kişisel veri sahibi açısından son derece önem arz eden aydınlatma yükümlülüğü ve ilgilinin hakları düzenlenmiştir. Buna göre kişisel verilerin elde edilmesi sırasında veri sorumlusuna veya onun yetkilendirdiği bir kişiye 10. madde çerçevesinde sayılan hususlarla ilgili olarak ilgili kişileri aydınlatma zorunluluğu getirilmiştir. Maddede beş bent halinde sayıldığı üzere ilgili kişilerin, veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin kimlere hangi amaçla aktarılabilirliği, veri toplamanın yöntemi, hukuki sebebi ve muhtemel sonuçları ile ilgili kişinin Kanun'un 11. maddesinde kapsamında ilgilinin sahip olduğu haklarına yönelik bilgilendirilmesi zorunludur. Bu maddenin varlığı, kişisel verileri işlenecek olan kişinin, verilerin işlenmesinde açık rıza beyanının elde edilmesi açısından son derece önem taşımaktadır²⁵⁶.

İlgili kişinin, bu Kanun kapsamında sahip olduğu hakları m. 11'de hüküm altına alınmıştır. Buna göre herkes, veri sorumlusuna başvurmak suretiyle bilgi edinme, düzeltme, itiraz etme ve kişisel verilerinin hukuka aykırı işlenmesi sonucu bir zarar söz konusu ise bu zararın giderilmesini talep etme hakkına sahiptir. İlgilinin bilgi edinme hakkı kapsamında, maddenin (a), (b), (c) ve (ç) bentlerindeki düzenlemeler yer almaktadır. Zira bu bent hükümlerinin hepsinde ilgilinin bir durumun varlığını öğrenme ya da bir duruma ilişkin bilgi talep etmesi söz konusudur.

Yine veri koruma hukuku açısından önem arz eden bir diğer durum veri güvenliği hususudur. Veri Koruma Kanunu'muz, 12. maddede veri sorumlusuna veri güvenliğinin

²⁵⁶ Bkz. s. 92 vd. 1. Aydınlatma Yükümlülüğü

sağlanması amacıyla bir takım yükümlülükler getirmiştir. Buna göre veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini, bu verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmek için gerekli tüm teknik ve idari tedbirleri almakla yükümlü olacak ve bu yükümlülüklerin yerine getirilmemesi durumunda bizzat sorumlu olacaktır. İkinci fıkra ise veri sorumlusu adına başka bir gerçek ya da tüzel kişi tarafından veri işlenmesi durumunda, bir önceki fıkroda belirtilen tedbirlerin alınması noktasında birlikte müştereken sorumludur.

Veri sorumlusu, üçüncü fıkra hükmü gereğince kendi kurum ve kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak için gerekli denetimleri bizzat yapabileceği gibi yaptırma imkânına da sahip olacaktır. Bu sayede gerekli tedbirlerin alınıp alınmadığı, dolayısıyla da veri güvenliğinin sağlanıp sağlanmadığı da anlaşılabacaktır.

Maddenin dördüncü fıkrasında, veri güvenliği için getirilmiş diğer bir hüküm yer almaktadır. Bu fıkra hükmü ile aslında veri sorumluları ile veri işleyenlerin sır saklama yükümlülüğü düzenlenmiştir²⁵⁷. Buna göre veri sorumluları ile veri işleyenler, kişisel veri işleme esnasında öğrendikleri kişisel verileri başkalarına açıklayamaz ve işleme amacı dışında kullanamazlar. İlgililer görevlerinden ayrılmış olsalar da bu yükümlülüklerinin devam edeceği kanunda belirtilmiştir.

Kanun'un 13. maddesinde ilgili kişinin, veri sorumlusuna başvuru usul ve esasları düzenlenmiştir. Maddede belirtildiği üzere ilgili, bu Kanunun uygulanmasına ilişkin talebini yazılı olarak veya Kurulun belirleyeceği diğer bir yöntemle öncelikle veri sorumlusuna iletebilir. Veri sorumlusu, başvuruda yer alan talepleri en kısa sürede ve en geç otuz gün içinde sonuçlandırması gerekmektedir. Yapılan bu işlemler ücretsiz olmakla birlikte işlemin ayrıca bir maliyet gerektirmesi halinde, Kurul tarafından belirlenecek tarife göre bir ücret alınabilir. Maddenin üçüncü fıkra hükmüne göre veri sorumlusu, ilgilinin başvurusuna karşı ya kabul ya da gerekçesini de belirtmek suretiyle ret edebilir. Eğer başvuru, veri sorumlusu tarafında kabul edilmişse yine kendisi tarafında başvurunun gereği de yerine getirilir.

²⁵⁷ KVKK m. 12 gerekçesi

Kanun'un. 14. maddesi, bir önceki madde kapsamında ilgili kişinin başvurusunun reddedilmesi halinde veya başvuruya verilen cevabın yetersiz görülmesi ya da hiç cevap verilememesi halinde ilgilinin, Kurula şikâyet başvurusu düzenlenmiştir. Başvurusu kabul edilmeyen ilgili, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz, her halde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyetinde bulunabilir. Maddenin ikinci fıkrasında ilgilinin öncelikli olarak veri sorumlusuna başvurusunun zorunlu bir başvuru yolu olduğu, bu başvuru yolu tüketilmeden şikâyet yoluna gidilemeyeceği düzenlenmiştir. Zorunlu başvuru yolu olarak düzenlenmesinin altında yatan neden ise uyuşmazlıkların belirli bir kısmının veri sorumluları tarafından çözülmesi, böylece Kurula yoğun bir iş yükü kalmasının önlenmesidir²⁵⁸.

Kurul tarafından yapılacak incelemenin usul ve esasları 15. maddeyle düzenlenmiştir. Kurul, görev alanına giren konularda, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda kendiliğinden gerekli incelemeyi yapabilecektir. Ancak Kurul, 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6. maddesinde²⁵⁹ belirtilen şartları taşımayan başvuruları incelemeye almayacaktır. Kurul, inceleme kapsamında veri sorumlularından devlet sırrı dışında kalan her türlü bilgi ve belgeyi isteyebilir. Veri sorumlusu, kendisinden istenen bilgi ve belgeleri on beş gün içinde Kurula göndermek zorundadır. Ayrıca Kurul, yerinde inceleme yapma gereği görmesi halinde veri sorumlusu, bu incelemenin yapılması için imkân sağlamak durumundadır.

Maddenin 4. fıkrasında, Kurulun, şikâyet üzerine yaptığı inceleme neticesinde ilgisine bir cevap vermesi öngörülmüştür. Şayet şikâyet tarihinden itibaren altmış gün içinde bir cevap verilememişse, ilgilinin talebi reddedilmiş sayılacağı hükme bağlanmıştır. Kanunda belirtilen altmış günlük sürenin önemi idari yargıda dava açma süresinin tespiti açısından önemlidir. Zira şikâyet tarihinden itibaren altmış günlük sürenin geçmesiyle idari yargıda dava açma süresi başlayacaktır²⁶⁰.

²⁵⁸ KVKK m. 14 gerekçesi

²⁵⁹ 3071 sayılı Kanun m. 6' da TBMM'ye veya yetkili makamlara verilen ya da gönderilen dilekçelerden belirli bir konuyu içermeyen, yargı mercilerinin görevine giren konularla ilgili olan ve de m. 4'te belirtilen şartlardan birini taşımayan dilekçelerin incelenmeyeceği düzenlenmiştir. 3071 sayılı Kanunun 4. maddesine göre ise dilekçe sahibinin adı, soyadı ve imzası ile iş veya ikametgâh adresinin dilekçede bulunması gerekmektedir. 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun metni için bkz. Erişim Tarihi: 14.04.2016, <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3071.pdf>.

²⁶⁰ KVKK m. 15 gerekçesi

Kanunun 16. maddesinde veri sorumlularının kaydedileceği Veri Sorumluları Sicili düzenlenmiştir. Kanun hükmüne göre sicil, Kişisel Verileri Koruma Kurulu gözetiminde Başkanlık tarafında kamuya açık olacak şekilde tutulacaktır. Veri sorumluları, veri işlemeye başlamadan önce bu sicile kaydolmak zorundadırlar. Maddenin üçüncü fıkrasında sicile kayıt başvurusunda bildirilmesi gereken hususlar belirtilmiştir. Bu kapsamda veri sorumluları ve temsilcisinin kimlik ve adres bilgileri, hangi amaçla veri işleneceği, veri konusu kişi gurupları ve bu kişilere ait veri kategorileri hakkında açıklama, verilerin aktarılabileceği alıcı veya alıcı gurupları, yabancı ülkelere aktarımı öngörülen veriler, veri güvenliğine ilişkin alınan tedbirler, verilerin işlendikleri amaç için gerekli olan azami süreye ilişkin hususlar sicile kayıt başvurusu ile bildirilir.

Kanunun beşinci bölümün altında kişisel verilere ilişkin suçlar ve kabahatler ile cezai yaptırımları, 5237 sayılı Türk Ceza Kanunu'na atıfta bulunulmak suretiyle düzenlenmiştir. 6698 sayılı KVKK m. 17'de kişisel verilere ilişkin suçlar bakımından 5237 sayılı TCK'nın 135 ila 140. maddelerinin uygulanacağı belirtilmiştir. 18. madde ile de kabahatlere ilişkin düzenlemeler hüküm altına alınmıştır. Maddenin birinci fıkrasında, Kanunun 10. maddesinde öngörülen aydınlatma, 12. maddesinde öngörülen veri güvenliğine, 16. maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüklerine aykırı davranılması ve 15. madde uyarınca Kurul tarafından verilen kararların yerine getirilmemesi durumunda uygulanacak idari yaptırımlar düzenlenmiştir. Belirtilen yükümlülükler aykırı davranışlar kabahat olarak öngörülmekte ve yaptırım olarak da idari para cezası uygulanmaktadır.

Maddede, kabahatlere karşı uygulanacak olan idari para cezalarına ilişkin düzenlemeye bakıldığında, bu idari para cezalarının alt ve üst sınırlarının oldukça geniş bırakıldığı dikkat çekmektedir. Örneğin 12. maddede zikredilen yükümlülükler aykırı davranılması durumunda ilgili hakkında 15.000 Türk lirasında 1.000.000 Türk lirasına kadar idari para cezası uygulanacağı belirtilmiştir. Kanunun madde gerekçesinde bu alt ve üst sınır arasındaki aralığın bilinçli olarak geniş tutulduğu ifade edilmiştir. Çünkü bu düzenleme ile 5326 sayılı Kabahatler Kanunu m. 17/ f. 2 hükmü²⁶¹ dikkate alınarak söz

²⁶¹ 5326 sayılı Kabahatler Kanunu m. 17/ f. 2 hükmü “İdarî para cezası, kanunda alt ve üst sınırı gösterilmek suretiyle de belirlenebilir. Bu durumda, idarî para cezasının miktarı belirlenirken işlenen kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumu birlikte göz önünde bulundurulur.”

konusu kabahatlerin farklı ekonomik güce sahip gerçek ve özel hukuk tüzel kişileri hakkında uygulanacak olmasından dolayı hakkaniyetin sağlanması amaç edinilmiştir²⁶². Diğer yandan kabahatlere uygulanacak idari para cezalarında üst sınırların oldukça yüksek olması, Kanunda düzenlenen yükümlülüklerle uymama noktasında caydırıcılığın sağlanması açısından gerekli ve önemli olduğu kanaatindeyiz.

Maddenin ikinci fıkrasında, kabahatlere ilişkin öngörülen idari para cezalarının veri sorumluları olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanacağı ifade edilmiştir. şayet kabahat oluşturacak eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğinde meslek kuruluşları bünyesinde işlenmesi halinde, Kurulun yapacağı bildirim üzerine eylemi yapan memur ve diğer kamu görevlileri hakkında disiplin hükümlerine göre işlem yapılacaktır.

Kanunun altıncı bölümünde, Kişisel Verileri Koruma Kurumu, Kurumun görevleri, Kişisel Verileri Koruma Kurulu, Kurulun görevleri, çalışma esasları ve teşkilat düzenlenmiştir.

19. madde hükmüne göre Kişisel Verileri Koruma Kurumu, idari ve mali özerkliğe sahip, kamu tüzel kişiliği haiz bir kurumdur. Kurum, Başbakanlıkla ilişkili olup merkezi Ankara'dır. Kurum, Kanunumuzun şekillenmesinde ve çıkarılmasında etkili olan AK'nın 108 sayılı Sözleşmesi ve AB'nin 95/46/AT sayılı Direktifi'nde, kişisel verilerin işlenmesine ilişkin ilkelerin uygulanmasını izlemek ve yönlendirmek üzere fonksiyonel açıdan bağımsız şekilde görev yapacak otoritelerin kurulmasını öngörmesi üzerine kurulmuştur²⁶³. Kanunun 20. maddesiyle Kurumun görevleri beş bent halinde sayılmıştır.

Kanunun 21. maddesiyle Kişisel Verileri Koruma Kurulu düzenlenmiştir. Kurul, Kurumun karar organı olup bu Kanun ve diğer mevzuatla kendisine verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Kurul, AK'nın 108 sayılı Sözleşmesi ve AB'nin 95/46/AT sayılı Direktifi'ne uygun şekilde bağımsız olarak kurgulanmış, görev alanına giren konularda hiçbir organ, makam, merci veya kişinin Kurula emir veremeyeceği düzenlenmek suretiyle bu bağımsızlık temin

²⁶² KVKK m. 18 gerekçesi

²⁶³ KVKK m. 19 gerekçesi

edilmeye çalışılmıştır²⁶⁴. Kurum, sahip olduğu bu özellikleri ile bir Bağımsız İdari Otorite olarak değerlendirilebilir.

Maddenin diğer fıkraları ile Kurulun oluşumu, üyelerin nitelikleri, seçimi ve görev süreleri düzenlenmektedir. Hükme göre Kurul, dokuz üyeden oluşmakta ve üyelerden beşi TBMM, ikişer üye Cumhurbaşkanı ve Bakanlar Kurulu tarafından atanmaktadır. Kurul üyesi olabilmek için Kurumun görev alanındaki konularda bilgi ve deneyim sahibi olmak aranan ilk şart olarak düzenlenmiştir. 657 sayılı DMK'nın 48. Maddesinde belirtilen ilgili nitelikleri taşımak, herhangi bir siyasi parti üyesi olmamak, en az dört yıllık lisans düzeyinde yükseköğrenim görmüş olmak ve de 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 olmak gerekmektedir.

Maddenin devam eden fıkralarında yer alan hükümlerde, Kurulun bağımsızlığını temin etmeye yönelik düzenlemelerin var olduğu dikkat çekmektedir. Zira 5. fıkroda TBMM tarafından yapılacak üye seçiminde her bir siyasi parti gruplarının üye sayısı oranında belirlenecek üye sayısının ikişer katı aday gösterileceği ve bu adaylar arasında TBMM Genel Kurulunda seçimin yapılacağı hükme bağlanmıştır. Ayrıca siyasi parti guruplarında, TBMM'de yapılacak seçimlerde kime oy verileceği ile ilgili görüşme yapılamayacağı ve bu konuya ilişkin karar alınamayacağı da hükümde düzenlenmekle, bağımsızlık unsurunun sağlanmasına katkı sağlanmıştır. Yine bağımsızlığı sağlamaya yönelik olmak üzere 10. fıkroda üyelerin, Kuruldaki resmi görevlerinin yürütülmesi dışında resmi veya özel hiçbir görev alamayacakları, dernek, vakıf, kooperatif ve benzeri yerlerde yöneticilik yapamayacakları, ticaretle uğraşamayacakları, serbest meslek faaliyetinde bulunamayacakları, hakemlik ve bilirkişilik yapamayacakları düzenlenmiştir. Bağımsızlık unsurunun sağlanması açısından önemli bir diğer husus da 13. fıkroda düzenlenmiş olan Kurul üyelerinin süresi dolmadan herhangi bir nedenle görevlerine son verilemeyeceği hükmüdür.

23. maddeyle Kurulun çalışma esasları düzenlenmiştir. Bu kapsamda, Kurulun toplantı yeter sayısı başkan dâhil en az altıdır ve karar yeter sayı da üye tam sayısının salt çoğunluğudur ve kanun hükmü ile üyelerin çekimser oy kullanmaları

²⁶⁴ KVKK m. 21 gerekçesi.

engellenmiştir. Aksi kararlaştırılmadıkça da altıncı fıkra hükmü gereğince Kurul toplantılarındaki görüşmeler gizli olarak gerçekleştirilir. Maddenin üçüncü fıkrasında Kurul üyelerinin kendilerini ve yakınlarını ilgilendiren konularda yasaklılıkları ve dördüncü fıkra da sır saklama yükümlölükleri düzenlenmiştir.

Kanunun 24 ila 27. maddelerinde Kurul başkanı, başkanlığın oluşumu ve görevleri, kişisel verileri koruma uzmanı ve uzman yardımcıları ile personele ve özlük haklarına ilişkin hükümler düzenlenmiştir.

Kanunun Yedinci Bölümü altında Çeşitli Hükümler düzenlenmiştir. 28. madde istisnalar başlığı ile Kanunun kapsamı dışında tutulan huşular hüküm altına alınmıştır. Maddenin birinci fıkrasında, Kanunun tamamen dışında tutulan durumlar düzenlenmişken, ikinci fıkrasında kural olarak Kanun kapsamında olmakla birlikte, sadece fıkra da belirtilen kanun maddelerinde düzenlenen hükümler açısından kısmen kapsam dışı tutulmuş durumlar düzenlenmiştir.

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİ SAHİBİNİN AYDINLATILMASI VE HAKLARI

3.1. AYDINLATMA YÜKÜMLÜLÜĞÜ

Kanun tarafından veri sorumlusu veya onun yetkilendireceği bir diğer kişiye yüklenmiş bir yükümlülük olarak aydınlatma yükümlülüğü, Kanun gerekçesinde belirtildiği üzere 95/46/AT sayılı Direktif hükümlerine uygun olarak 6698 sayılı Kanun'un 10. maddesinde düzenlenmiştir. Önemli bir yükümlülük olan aydınlatmaya, 95/46/AT sayılı Direktif'in 10. ve 11. maddelerinde²⁶⁵ kişisel verinin veri öznesinden ve veri öznesi dışında başka bir kişiden alınması durumları ayrı maddelerde olmak üzere, 108 sayılı Sözleşme'nin 8. maddesinde²⁶⁶ ve OECD Rehber İlkeleri 13. paragrafında²⁶⁷ da yer verilmiştir.

²⁶⁵ 95/46/AT sayılı Direktif m. 10 “Veri öznesinden verilerin toplanma durumlarında bilgilendirme. Üye Devletler, önceden mevcut olması haricinde, kendine dair bilgilerin toplandığı bir veri öznesine, denetleyici ve temsilcisinin en azından aşağıdaki bilgileri vermesini sağlamalıdır: a) Denetleyici ve varsa temsilcisinin kimliği; b) Kastedilen veri işleme amaçları; c) Aşağıdakiler gibi herhangi bir başka bilgi; - verilerin alıcıları veya alıcı kategorileri, - yanıt vermemenin olası sonuçlarının yanı sıra soruların yanıtlarının zorunlu veya gönüllü olup olmadığı, - (özneyle) ilgili verileri düzeltme hakkının ve verilere erişim hakkının olması, bu tür başka bilgilendirmenin gerekli olmasına göre, verilerin toplanmasındaki özel koşulları göz önünde bulundurarak veri öznesine ilgili kişinin adil işlemeyi garanti etmelidirler.” M. 11 “Verilerin veri öznesinden elde edilmediğinde bilgilendirme. 1. Veriler veri öznesinden elde edilmediğinde, üye devletler, (veri öznesinin bu bilgilere) önceden sahip olması hariç, kişisel verilerin kaydının yapılması esnasında ya da üçüncü bir şahsa ifşa öngörüldüğünde, verilerin ilk ifşa zamanından önce, denetleyici veya temsilcisinin en azından aşağıdaki bilgileri veri öznesine vermesini sağlayacaktır: a) Denetleyicinin ve varsa temsilcisinin kimliği; b) İşlemenin amaçları; c) Aşağıdakiler gibi herhangi bir başka bilgi; - verilerin alıcıları veya alıcı kategorileri, - yanıt vermemenin olası sonuçlarının yanı sıra soruların yanıtlarının zorunlu veya gönüllü olup olmadığı - (özneyle) ilgili verileri düzeltme hakkının ve verilere erişim hakkının olması, (özneyle) ilgili verileri düzeltme hakkının ve verilere erişim hakkının olması, bu tür başka bilgilendirmenin gerekli olmasına göre, verilerin toplanmasındaki özel koşulları göz önünde bulundurarak veri öznesine ilgili kişinin adil işlemeyi garanti etmelidirler. 2. Kayıt veya ifşa açıkça yasayla belirtilirse ya da aşırı bir çaba gerektirecek ya da imkânsızlığı kanıtlanan verilerin sağlanması için, tarihsel veya bilimsel araştırma amaçları için veya istatistiksel amaçlar için işleme durumunda; Paragraf 1 uygulanmayacaktır. Bu durumlarda, Üye Devletler uygun koruma önlemleri sağlayacaktır.

²⁶⁶ 108 sayılı AK Sözleşmesi m. 8 İlgili kişi hakkındaki ek güvenceler “Herkes: (a) Kişisel nitelikteki verilerin otomatik işleme tâbi tutulduğu fişiyelerin mevcudiyetini, temel amaçlarını, fişiye yöneticisinin kimliğini ve mutata ikâmetgâhı ile esas müessesesini öğrenmek; (b) Makul aralıklarla ve süreye bağlı olmaksızın veya aşırı masrafa girmeden kendisi ile ilgili kişisel nitelikteki verilerin otomatik fişiyede bulunup bulunmadığının teyidini yaptırmak ve bu bilgilerin anlaşılır bir biçim altında bildirilmesini sağlamak;...”

²⁶⁷ İbrahim Korkmaz, Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, 129, Erişim Tarihi: 01.05.2016, <http://tbbdergisi.barobirlik.org.tr/m2016-124-1571>.

3.1.1. Aydınlatma Yükümlülüğünün Önemi

Herkes, hukuken tasarruf yetkisi sınırlandırılmamış haklarını serbestçe kullanma yetkisine sahiptir. Ne var ki bu yetkilerini kullanmadan önce kişilerin, üzerinde tasarruf yetkisini kullanacakları ilgili haklarına dair bilgi sahibi olmaları, bu hakların amaçlarına uygun şekilde kullanılmaları bakımından fazlasıyla önem arz etmektedir²⁶⁸. Kişisel verilerin korunmasına yönelik yasal metinlerde yer alan haklarla, bireylere aktif bir rol oynama imkânı verilmiştir. Bireyin sahip olduğu haklarla kişisel verilerine erişebilme, verilerinin düzeltilmesini isteyebilme, veri işlemesine itiraz edebilme yetkileri bu aktif rolü açıkça ortaya koymaktadır. Bunun yanında Kanun'da veri sorumlusu, Direktif' te veri denetçisi veya temsilcisi olarak ifade edilen kimselere de kişisel veri sahibinin aydınlatılması yükümlülüğü getirilmiştir. Aydınlatma yükümlülüğü, veri öznesi tarafından kullanılmadığından, ilgili kişinin pasif bir hakkı olarak da nitelendirilebilir. Veri kütüğü sahibi veya veri denetçisine yüklenen bu yükümlülük, veri sahibi kişilerin kişisel verilerinin geleceğini belirleyebilmesi açısından da ayrı bir öneme sahiptir²⁶⁹.

Aydınlatma kavramı “*bir sorunun ya da bir kavramın tüm içerimleriyle açıklanması*²⁷⁰.” şeklinde tanımlanmıştır. Bilgilendirme kavramının tanımı ise “*Bir konuda özet olarak verilen bilgi veya açıklama.*²⁷¹” şeklindedir. Yapılmış olan tanımlardan da anlaşılacağı üzere aydınlatma kavramı, ilgili konu hakkında detaylıca açıklama yapılmasını gerektirmekteyken, bilgilendirmenin özet olarak bilgi verme işi olduğu anlaşılmaktadır. Dolayısıyla aydınlatma kavramı bilgilendirmeye göre daha geniş kapsamlıdır. Gerçekten de ilgilinin Kanun m. 10, 95/46/AT sayılı Direktif m. 10 kapsamında sahip olduğu bilgi edinme hakkı açısından, kişisel verilerinin amacına uygun işlenip işlenmediği veya kullanılıp kullanılmadığı hususunda bilgi edinebilmesi, öncesinde ilgili kişinin, kişisel verilerinin işlendiğine dair bilgilendirilmesi ile doğrudan bağlantılı olduğu açıktır. Diğer yandan ilgilinin düzeltme hakkını kullanması açısından aydınlatma yükümlülüğü, ilgili kişinin işlenmiş olan kişisel verilerinin ilgilisi tarafından

²⁶⁸ Şimşek, 88

²⁶⁹ Küzeci, 212

²⁷⁰ *Büyük Türkçe Sözlük*, Erişim Tarihi: 29.10.2015,

http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.563f0b98be0390.80067468.

²⁷¹ *Büyük Türkçe Sözlük*, Erişim Tarihi: 29.10.2015,

http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.563f07a47d0847.21903184.

bir nevi denetimine olanak tanıyan bir öneme sahip olacaktır. Şöyle ki; kişisel verileri işlenmiş olan kişinin, verileri işlenmeden önce kendisi, kişisel verilerin işlenmesi hususunda ilgililerce aydınlatılmış olması, diğer bir anlatımla kişisel veri sahibine, aydınlatma yükümlülüğü altında bulunanlarca, konuya ilişkin etraflıca açıklama yapılması, ilerleyen aşamada veri sahibi kişinin bu açıklamalar ışığında, hakkında yapılmış olan veri işleme faaliyetini neticesinde ilgili haklarını amacına ve gerçek anlamına uygun şekilde kullanabilmesine olanak tanıyacaktır.

Veri koruma hukukunda, aydınlatma yükümlülüğü farklı yönlerden önem arz etmektedir. İlk olarak aydınlatma yükümlülüğü, kişisel verileri işlenecek olan kişinin, kişisel verilerinin işlenmesi ile sahip olacağı haklarını tam anlamıyla kullanabilmesine hizmet edecektir. Aksi halde ilgili kişinin, hakkında kişisel veri işlendiğinden haberdar olmaması, onun haklarını kullanamaması durumunu ortaya çıkaracaktır²⁷². Aydınlatma yükümlülüğünün önemli olduğu diğer husus ise, devletin ya da idari birimlerin kişisel veri işleme faaliyetleri kapsamında şeffaflığın sağlanmasında oynadığı roldür. Zira devlet, çeşitli faaliyetlerini ve kamu hizmetlerini daha iyi şekilde yerine getirebilmek için bireylere ait birçok kişisel veri niteliğinde bilgiye sahip durumdadır.

Şeffaflık kavramı doktrinde, hukuk biliminde ifade ettiği anlam bakımından, *saydamlık, açıklık, aleniyet, idari açıklık, yönetimde şeffaflık, demokratik yönetim, hesap verebilir idare* olarak ifade edilmiştir. Şeffaflık kavramına yüklenen bu anlamı ile birlikte devlet idaresi alanında gizliliğin kalmaması, yapılan faaliyetlerin, bireyler tarafından öğrenilmesine olanak tanınması ve yapılan faaliyetlerin görünür olması ifade edilmek istenmiştir. Devlet idaresi altındaki faaliyetlerin şeffaflığının sağlanmasında amaç ise bilginin zamanında ve güvenilir şekilde talepte bulunanlara sunulmasıdır²⁷³. Bu bağlamda ilgililerin kişisel verilerinin amaçlarına uygun işlenip işlenmediği bizzat ilgilisi tarafından hem öğrenilmiş hem denetlenmiş hem de devlet birimleri tarafından veri işleme faaliyetlerinde şeffaflık sağlanmış olacaktır.

3.1.2. Aydınlatma Yükümlülüğünün Gerekliliği

Yukarıda yapılan açıklamalarda, kişisel veri sahibinin, sahip olduğu haklarını tam anlamıyla kullanabilmesi açısından aydınlatma yükümlülüğünün önemi vurgulanmış

²⁷² Şimşek, 88

²⁷³ Döner, 19-20

olmakla birlikte yapılan açıklamalar, bu yükümlülüğün gerekliliğini ortaya koymaktadır. Zira hukuken sahip olunan hakların esas itibarı ile uygulanabilmesi için gerekli hususların yükümlülerce yerine getirilmesi bu anlamda zorunludur. Aksi halde bu haklar kâğıt üstünde var olacak ve bu durum da hukuk devleti ile bağdaşmayacaktır.

Aydınlatma yükümlülüğünün gerekli olduğu diğer bir durum ise Kanun'un 5 ve 6. maddelerinde düzenlenmiş olan kişisel verilerin işlenmesi şartlarından ilk ve en önemlisi niteliğinde kişisel verilerinin işlenmesine ilişkin ilgili kişinin, vereceği açık rıza beyanıdır. Hukuka uygunluk nedenleri başlığı altında, rızanın niteliğine ilişkin açıklamalara yer verilmişti²⁷⁴. Burada kişisel verileri işlenecek olan ilgili kişinin, kişisel verilerinin işlenmesine yönelik vereceği açık rıza beyanında aydınlatma yükümlülüğünün rolü ortaya çıkmaktadır. Çünkü bu yönde verilecek olan bir rıza beyanının genel nitelikte olmayıp, ilgili kişinin, kişisel veri işlenecek duruma yönelik özellikli (spesifik) bir rıza beyanının alınması gerekmektedir. Ayrıca veri işleme yapılacak konu, amaç ya da durumun da kişisel veri sahibi kişiye tüm yönleri ile açıklanmış olması şarttır. Zira veri sahibinin, hakkında yapılacak olan tüm kişisel veri işlenmesi faaliyetlerine yönelik genel bir rıza beyanında bulunması, hukuka uygunluk şartının yerine getirilmesi bakımından yeterli görülmeyecektir²⁷⁵.

Kişisel verilerin işlenmesinde rıza beyanından beklenen faydanın sağlanması açısından veri sahibi kişinin, kişisel verilerinin işlenmesinde neye rıza gösterdiğini bilebilmesi için bu konuda aydınlatılması gerekir. Yani ilgili kişi, kişisel verilerinin işlenmesine rıza göstermesi veya göstermemesi durumunda karşılaşacağı durumlar hakkında bilgilendirilecek ve bunun neticesinde rızasını beyan edecektir. Ancak bu durumda kişisel veri sahibinin rızası aydınlatılmış bir rıza olacaktır²⁷⁶. Diğer yandan Direktif m. 7/a' daki düzenlemeye uygun olması için rızanın açık, kesin ve net olarak verilmesi gerekliliğinin sağlanması da ancak yukarıda açıklandığı üzere gerçekleştirilecektir. Kişisel veri sahibinin, hakkında veri işlenmesine yönelik rızasını netleştirmesi, açık şekilde anlaşılmaktadır ki bu hususta etraflıca bilgilendirilmesine bağlıdır.

²⁷⁴ Bkz. s. 18 vd.

²⁷⁵ Küzeci, 223

²⁷⁶ Küzeci, 223-224

3.1.3. Kavramsal Tartışma

6698 sayılı Kanun'un 10. madde kapsamında *aydınlatma yükümlülüğü* ifadesine, madde başlığında yer verilmiştir. Maddenin sonunda da "... bilgi vermekle yükümlüdür." ibaresiyle kanun koyucu, veri sorumlusunun yükümlü olduğu durumu belirtmiştir. Bu iki kavram, madde metninde birbiri yerine kullanılmış olmakla birlikte, bu kavramların anlamları ve kapsamaları aynı olmadığı, dolayısıyla bu şekildeki kullanımın karışıklığa yol açacağı sonucuna varılabilir.

Yukarıda aydınlatma yükümlülüğünün önemine dair açıklamalarda bulunulurken, "*aydınlatma*" ifadesinin anlamına yer verilmişti. Hatırlanacağı üzere tanımda bir hususa ilişkin etraflıca açıklama yapılması, aydınlatma olarak ifade edilmişti²⁷⁷. Bilgi vermek ise yapılmış olan bir iş ya da bitmiş bir durum hakkında ilgisine malumat vermektir.

Ayrıca Kanun'un üçüncü maddesi içerisinde açık rıza, belli bir konuya ilişkin olarak bilgilendirmeye dayanan ve ilgilinin özgür iradesiyle açıklanan rıza olarak tanımlanmıştır. Bu tanımda da belirtmek gerekir ki *bilgilendirme* kavramı *aydınlatma* kavramının yerine kullanılmıştır. Yine aydınlatma yükümlülüğünün önemine dair yapılan açıklamalarda *bilgilendirme* kavramının tanımına yer verilmişti²⁷⁸. Yani Kanun'un ilgili maddelerinde kullanılmış olan *aydınlatma*, *bilgilendirme*, *bilgi vermek* kavramları kanun koyucu tarafından aynı anlamda olmak üzere birbirlerinin yerine kullanılmışlardır.

Bu kavramlardan aydınlatma ve bilgilendirme birbirine yakın ifadeler olsalar da bilgi vermek ifadesi nitelik bakımından diğerlerinden ayrılmaktadır. Madde metni²⁷⁹ içerisinde, veri sorumlusunun aydınlatma yükümlülüğü kapsamında ilgisine hangi hususlarda açıklamalarda bulunacağı dikkate alındığında, bu yükümlülüğün ilgilinin kişisel verilerinin işlenmeden yapılması gerektiği anlaşılmaktadır. Gerçekten de ilgili kişi, kişisel verileri işlenmeden maddede yer alan hususlarda veri sorumlusu tarafından

²⁷⁷ Bkz. s. 92 vd.

²⁷⁸ Bkz. s. 92 vd.

²⁷⁹ 6698 sayılı Kanun m. 10 "(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür."

aydınlatılması halinde kişisel verilerinin işlenmesine dair rıza gösterebilecektir. Aksi halde örneğin kişisel verileri işlenmiş olan bir kişi için, verileri işlendikten sonra bunun hangi amaçla yapıldığının pek bir önemi kalmayacak, zira rıza olmaksızın veri işleme gerçekleşmiş ve kişisel verilerin korunması altında yatan insan haklarının korunması temel amacı ihlal edilmiş olacaktır. Gerçekten de madde metninde yer alan hususlarda veri sorumlusu, ilgili kişiye sadece somut, net bilgiler vermektedir. Ancak bilgilendirme, tam ifadesiyle aydınlatma ise ilgilisinin, hakkında kişisel ver işlenmesi yapılacak hususta etraflıca donatılması, örneğin yapılacak olan bu işlemin ilgisine ne gibi faydaları olacağı ya da veri işleminin muhtemel sonuçlarının neler olacağı gibi hususlarda bilgi sahibi olmasının sağlanmasıdır. 2008 tarihli Tasarı'nın aydınlatma yükümlülüğünü düzenleyen 11. maddesinde (ç) kişisel veri toplamanın *muhtemel sonuçları* hakkında da bilgilendirileceği düzenlenmişti. Bu ifadenin varlığı, aydınlatma yükümlülüğünün altınca yatan asıl amacın göstergesidir.

Yukarıdaki açıklamaları destekler yönde ayrım Alman Veri Koruma Kanunu (BDSG)'de yer almaktadır. Veri Koruma Kanunu (BDSG) Kamusal Makamların Veri İşlemesi başlıklı ikinci kısım altında İlgilinin Hakları başlıklı ikinci alt kısım m. 19'da İlgilinin Bilgilendirilmesi (Auskunft an den Betroffenen), ve m. 19a' da Haber Verme (Benachrichtigung)'ye ilişkin hükümler düzenlenmiştir. M. 19'da ilgilinin talebi üzerine, ilgiliye ilişkin kaydedilmiş veriler, kaydedilmiş bu verileri alan kişiler ve üçüncü olarak da kişisel verilerin kaydedilmesinin amacı onunla paylaşılır. Yine BDSG Kamusal Olmayan Makamların Veri İşlemesi başlıklı üçüncü kısım altında ikinci alt kısımda ilgilinin hakları düzenlenmiştir. Bu kısımda da m. 33'te İlgilinin Haberdar Edilmesi (Benachrichtigung des Betroffenen) ve m. 34'te İlgilinin Bilgilendirilmesi (Auskunft an den Betroffenen) düzenlenmiştir. 33. maddenin birinci fıkrasında kişiye ilişkin veriler, ilgisinin haberi olmaksızın, belli bir amaç için ilk defa kaydedilmişse, ilgili bu kaydedilmeden, verinin türünden, elde bulundurulma amacından, işlenmeden ve sorumlu makamdan haberdar edileceği düzenlenmiştir. Madde metinlerinden anlaşılacağı üzere haber verme ile ilgili m. 19 ve m. 33'te ilgili kişi, hakkında kişisel veri işlemesi yapıldıktan sonra gerek kendi talebi gerekse ilgili makam ya da kişisel verileri işleyen tarafından, yapılan kişisel veri işlemesi hakkında haberdar edilmesi söz konusudur. Alman Hukukunda, bu iki kavram birbirinden farklı durumlar arz etmesi nedeniyle ayrı iki madde de hüküm altına alınmıştır.

Dolayısıyla Kanun’umuz kapsamında veri sorumlusunun aydınlatma yükümlülüğü içerisinde *bilgi vermek* ifadesi yerinde olmayan bir kullanım olduğu görüşündeyiz.

3.1.4. Aydınlatma Yükümlülüğünün Yerine Getirilmesi

Veri öznesinin aydınlatılması, kişisel verilerin bizzat kendisinden alınması durumunda aydınlatılması ve kişisel verilerin veri öznesi haricinde üçüncü kişilerden toplanması hallerinde aydınlatılması olmak üzere iki durumda söz konusudur. Bu durumlardan ilki Direktif m. 10’da, ikinci durum ise m. 11’de düzenlenmiştir. Kişisel verilerin, veri öznesinden alınması durumundaki aydınlatma yükümlülüğünün kapsamında 10. maddeye göre denetleyici veya temsilci tarafından asgari olarak aşağıda sayılan hususlar yer almalıdır:

- Sorumlu kişinin ve varsa temsilcisinin kimliği,
- Verilerin işlenmesindeki amaç,
- Verilerin alıcıları veya alıcı kategorileri,
- Sorulara cevap vermenin zorunlu veya isteğe bağlı olup olmadığı ve cevap vermeme durumunda olası sonuçlar,
- Veri öznesinin kişisel verileri hakkında bilgi alma ve düzeltme haklarının olduğu.

Ayrıca belirtmek gerekir ki, veri öznesine aydınlatma yükümlülüğü kapsamında verilecek olan bu bilgilerin doğru ve eksiksiz şekilde verilmesi gerekmektedir²⁸⁰.

Bazı durumlarda verilerin işlenmesi, veri işlemeye yetkili kişilerin doğrudan veri öznesinden almadığı verileri gerektirebilir. Verilerin bu gibi durumlarda veri öznesine sorulmadan, üçüncü kişilerden toplanması durumlarında, yasal olarak ifşa edilsin veya edilmesin, veri öznesinin durum hakkında en az m. 10’da belirtilen hususlarda bilgilendirilmesi gerekmektedir. Bu bilgilendirme veriler kaydedildiğinde veya en geç veriler ilk kez bir üçüncü kişiye ifşa edildiğinde yapılmalıdır²⁸¹.

Direktif m. 10 ve m. 11, kişisel verilerin edinildiği kaynak bakımından bizzat veri öznesi olması noktasında farklılık göstermektedir. Bunun yanında m. 11/f. 2 ile birinci fıkra hükmüne bir istisna getirilerek, aydınlatma yükümlülüğünün uygulanmayacağı

²⁸⁰ 95/46/AT sayılı Direktif, 38 numaralı paragraf.

²⁸¹ 95/46/AT sayılı Direktif, 39 numaralı paragraf.

haller düzenlenmiştir. Buna göre veri öznesinin önceden durumdan haberdar olması, veri öznesine bilgi ulaştırmak imkânsızsa ve bu imkânsızlık kanıtlanmışsa veya aşırı bir çaba gerektiriyorsa, verileri kaydetme ve açıklama açıkça yasayla belirtilmişse veya bilimsel, tarihsel ya da istatistiksel amaçlar için kişisel veri işlemesi söz konusuysa bu yükümlülük uygulanmayacaktır²⁸².

Kanun kapsamında aydınlatma yükümlülüğü, Direktif hükümlerine uygun olarak düzenlenmiş,²⁸³ ancak Direktif’teki gibi kişisel verilerin veri öznesinden toplanması ve veri öznesinden elde edilmediği ayrımına yer verilmemiştir. Kanun’un 9. maddesinde tek fıkra halinde düzenlenen aydınlatma yükümlülüğünde, veri sorumlusu, kişisel veri sahibi kişiye,

- Kendisinin ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- 11. maddede sayılan diğer hakları,

konusunda bilgilendirmekle yükümlü olduğu belirtilmiştir. 2008 tarihli KVKK’nın aydınlanma yükümlülüğünün düzenlendiği madde metninde, veri sorumlusuna kişisel veri toplamanın hukuki sebebinden sonra *kişisel veri toplamanın muhtemel sonuçları* ifadesi yer almaktaydı. Bu ifadeye Kanun kapsamında yer verilmemiştir. Bu ifade son derece önem arz etmektedir. Zira kişi, hakkında yapılan işlemin ne olduğunu bilmesi yanında yapılan işlemin sonucuna dair bilgi sahibi olması, onun hakkında yapılacak olan bu işleme rıza beyanında bulunmasında da etkili olacağı düşüncesindeyiz.

3.2. KİŞİSEL VERİ SAHİBİNİN 6698 SAYILI KANUN KAPSAMINDA YER ALAN HAKLARI

3.2.1. Bilgi Edinme Hakkı

Bilgi edinme hakkı, veri sahiplerinin, kendilerine ait verilerle ilgili durumlardan haberdar olmalarına, bu sayede özel hayatları ile ilgili ileriye dönük olarak karar

²⁸² 95/46/AT sayılı Direktif, 40 numaralı gerekçe.

²⁸³ 6698 sayılı Kanun m. 10 gerekçesi.

almalarına imkân tanımaktadır. 95/46/AT sayılı Direktif'te erişim hakkı başlıklı m. 12, 108 nolu Avrupa Sözleşmesi'nin ek güvenceler başlıklı 8. maddesinde, Avrupa Birliği Temel Haklar Şartı m. 8²⁸⁴, de ve iç hukukumuzda 6698 sayılı Kanun m. 11'de veri sahibinin bilgi edinme hakkı düzenlenmiştir²⁸⁵. Bu hak altında veri sahibi kişiler, kendilerine ait verilerin işlenip işlenmediğini, verilerin hangi işlemlere tabi tutulduğunu ve bu işlemlerin temel amacının ne olduğunu ve bu amaca uygun kullanılıp kullanılmadığını, kişisel verilerinin yurt içinde veya yurt dışında aktarılması söz konusu ise bu verilerin kime aktarıldığını öğrenebileceklerdir.

Bu hakkın nasıl kullanılacağına dair Direktif, 108 sayılı Sözleşme ve Kanun'un ilgili maddelerinde bazı düzenlemelere yer verilmiştir. Öncelikle veri sahibi kişi, bir süreye bağlı kalmaksızın, makul aralıklarla ve sınırlama olmaksızın, aşırı gecikme olmadan ve de aşırı masrafa yol açmadan, başvuruda bulunmak süratiyle kişisel verilerine dair dilediği bilgiyi edinmek isteyebilecektir. Süreye bağlı olmaksızın ifadesinden, ilgili kişinin istediği her zaman başvuruda bulunarak bu bilgilere ulaşabileceği anlaşılmaktadır. Bu hak, bir defa kullanmakla tüketilebilen bir hak olmadığından²⁸⁶, ilgili düzenlemelerde makul aralıklarla tekrar kullanılabilmesi mümkündür. Diğer yandan kişisel verileri hakkında bilgi isteyen kişiye, bu verilerin aşırı bir gecikme olmaksızın bildirilmesi gerekmektedir ki aksi bir durumda ilgili açısından bu hak ile istenilen amacın yerine getirilemediği ve hakkın gereği gibi kullanılamadığının düşünülmesi yersiz olmayacaktır. Ayrıca bilgi edinme hakkını kullanmak isteyen kişi, bu hakkını ücretsiz olarak kullanabilecektir. Ne var ki ilgilinin talebi dolayısıyla yapılan işlem ayrıca bir ücreti gerektirmesi durumunda, Kurulca belirlenmiş olan tarife üzerinden ilgiliden ücret alınabilecektir. Ancak 95/46/At sayılı Direktif m. 12/a'da, diğer düzenlemelerden farklı olarak masraf olmaksızın bu hakkın kullanılabilmesi düzenlenmiştir.

Bilgi edinme hakkının kullanım şekline dair Kanun'un 13. maddesinde bir takım düzenlemelere yer verilmiştir. Kanun m. 13' e göre başvuru, yazılı şekilde veya

²⁸⁴ AB Temel Haklar Şartı m. 8'de Kişisel verilerin korunması madde başlığı ile genel anlamda veri korumaya ilişkin bir düzenlemeye yer verilmiş, madde içerisinde herkesin, kendisi hakkında toplanmış olan kişisel verilere erişim hakkının olduğu ismen zikredilmiş olup hakla ilgili detaylı bir hükme yer verilmemiştir.

²⁸⁵ Kişisel verilerin korunmasında Bilgi Edinme Hakkı Kanunu'nun yeri ve önemi daha sonraki konu başlığı altında incelenecektir. Bu nedenle, bu kısım altında sadece 108 sayılı sözleşme, 95/46/AT sayılı Direktif ve Kanun hükümlerine yer verilmiştir.

²⁸⁶ Başalp, 48

Kurulun belirleyeceği diğer yöntemlerle yapılmalıdır ve bu talebe, talebin niteliğine göre en kısa sürede ancak en geç otuz gün içinde cevap verilmelidir. Maddenin ikinci fıkrasında tıpkı Direktif hükmünde olduğu gibi, veri sorumlusu ilgilinin başvurusunu ücretsiz olarak sonuçlandırması gerekmektedir. Ancak, işlemin ayrıca bir maliyeti gerektirmesi durumunda, Kurulun belirlemiş olduğu tarife üzerinden ücret alınması olabilecektir.

Bilgi edinme hakkının kullanılması kapsamında talepte bulunan kişiye, istenilen kişisel veri ile ilgili bilgilerin ve işlenen bilgi türlerinin tamamı, verilerin işlenmesinin hukuki dayanağı ve amacı, hangi kişisel verilerin üçüncü kişilere aktarılabilirliği ve aktarılan kişilerin kimlikleri, anlaşılır bir şekilde bildirilmesi gerekmektedir. Burada belirtmek gerekir ki ilgilinin talebi üzerine kendisine yapılacak olan bilgi verme işleminin anlaşılır şekilde yapılması gerekir. Zira otomatik yollarla verilerin işlenmesi durumunda, teknik bilgiden yoksun olunma karşısında, başvuru sahibi ilgili kişilere basit, anlayabilecekleri şekilde bilgi verilmelidir²⁸⁷.

Bu hakkın kullanılmasının hangi hallerde sınırlandırılacağına yönelik Direktif m. 13 ve Avrupa Sözleşmesi m. 9'da bazı hükümlere yer verilmiştir. Kanun'un 28. maddesinin ikinci fıkrasında kapsamında da bu metinlerle aynı yönde sınırlama sebepleri düzenlenmiştir. Buna göre bu hakkın kullanılması, milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi, devletin mali menfaatleri, suçların önlenmesi, veri sahibi kişinin veya diğer bir kişinin hak ve özgürlüklerinin korunması amaçlarıyla sınırlandırılması mümkün olabilecektir.

3.2.2. Verilerin Düzeltmesini, Silinmesini ve Yok Edilmesini İsteme Hakkı

Bir önceki başlık altında belirtildiği üzere, veri sahibinin hakları ayrı maddelerde düzenlenmeyip, ilgili madde içerisinde bütün olarak yer almıştır. İlgili kişinin verilerinin düzeltilmesini, silinmesini veya yok edilmesini isteyebilme hakkı, ilgilinin bu Kanun kapsamındaki diğer bir hakkı olan bilgi edinme hakkının bir uzantısıdır²⁸⁸. 95/46/At sayılı Direktif'in 12. madde başlığı *Erişim Hakkı* olsa da maddenin (b) bendinde veri sahibinin düzeltme, silme ve engelleme haklarına yer verilmiştir. 108 sayılı Avrupa Sözleşmesi m. 8/c kapsamında veri sahibinin düzeltme ve silme haklarına

²⁸⁷ Başalp, 49,

²⁸⁸ Küzeci, 217

yer verilmiş, ancak engelleme hakkı düzenlenmemiştir. Kanun’umuzun 11. Maddesinde de veri sahibinin tüm hakları bir arada ifade edilmiştir. Hemen belirtmek gerekir ki veri sahibi, bu düzenlemeler kapsamında kişisel verilerin düzeltilmesini, silinmesini ya da yok edilmesini bizzat kendisi gerçekleştirmemektedir. Bu kapsamda veri sahibi, verilerinin düzeltilmesini, silinmesini veya yok edilmesini isteme haklarına sahiptir. Ayrıca veri sahibi, talebi doğrultusunda kişisel verileri üzerinde yapılan bu işlemlerin üçüncü kişilere bildirilmesini isteme hakkına da sahiptir. 2008 tarihli Tasarıda ilgilinin verilerin aktarımının engellenmesini isteyebilmesi de düzenlenmişti. İlgiliye ait kişisel veriler, m. 8 uyarınca yine ilgilinin rızası olmaksızın hem yurt içine hem de yurt dışına aktarılamayacağı için, ilgili kişi kişisel verilerinin aktarılmasına açık rıza göstermeyerek, 2008 tarihli Tasarıda yer alan kişisel verilerin aktarılmasını engelleme hakkını dolaylı olarak kullanma imkânına sahip olacaktır.

11. madde lafzından veri sahibinin, sahip olduğu kişisel verilerin düzeltilmesini, silinmesini veya yok edilmesini isteme haklarını her durumda kullanamayacağı anlaşılmaktadır. Kişisel verilerin düzeltilmesini isteme hakkının düzenlendiği maddenin (d) bendi metninden kişisel verilerin, ancak eksik veya yanlış işlenmiş olması durumunda düzeltilmesinin istenebileceği açık olarak anlaşılmaktadır. Dolayısıyla ilgilisinin her zaman kendisine ait olsa da kişisel verilerinin, kendi dilediği şekilde kayıtlı olmasını isteme imkânı olmayacaktır. Belirtmek gerekir ki bu hakkın temelinde, 95/46/AT sayılı direktif m. 6/1-d ve 108 sayılı Avrupa Sözleşmesi m.5/d maddelerinde düzenlenmiş olan verilerin doğru ve gerektiğinde güncel olması ilkesi yer almaktadır²⁸⁹. Benzer hükme iç hukukumuzda 6698 sayılı Kanun’un 4. maddesinin ikinci fıkrasının (b) bendinde yer verilmiştir. Bir kimse hakkındaki doğru ve en güncel bilgileri kişinin kendisi bilebileceği düşünüldüğünde, kişi bu hakkını kullanmakla ilgili madde hükümlerine hizmet etmekte, hem de verilerin yanlış veya güncel olmamasından kaynaklanacak tehlikelerden kendisini korumuş olacaktır. Aynı zamanda da veri sahibine, yukarıda belirtildiği şekilde, kişisel verilerinin ilgilisinin dilediği şekilde kayıt altında olması gibi bir tutum sergileme izni de verilememiş olacaktır.

Verilerin silinmesi ile yok edilmesi aslında verilerin tamamen ortadan kaldırılması olmakla birlikte, verilerin bilgisayar ortamında kayıtlı olması durumunda, talepte

²⁸⁹ Küzeci, 217

bulunana ait verilerin kayıtlarının silinmesi, verilerin elle kaydedilmiş olması durumlarında ise kayıt evraklarının yok edilmesi kastedilmektedir²⁹⁰.

3.2.3. İtiraz Hakkı

Veri öznelere itiraz hakkı, 95/46/AT sayılı Direktif m. 14' te düzenlenmiştir. Bu maddeye göre veri öznesine iki durumda itiraz etme imkânı tanınmıştır. Bu durumlardan ilki, Direktif'in 7. maddesinin (e) ve (f) bent hükümleri gereğince verilerin, kamu yararına olmak üzere bir görevin yerine getirilmesi için işlenmesi ve haklı çıkarların korunması halleridir. İkincisi ise, kişisel verilerin doğrudan pazarlama amacı ile işlenmesinin öngörüldüğü halde, veri öznesinin önceden itiraz hakkı hususunda bilgilendirilmesi şartıyla ve ücret ödemeksizin bu hakkını kullanması durumudur. Direktifin 45 numaralı paragrafında da belirtildiği üzere bir gerçek veya tüzel kişiye, bunların meşru menfaatleri veya kamu otoritesi ya da kamu menfaati gerekçesiyle yasal olarak işlenebileceği durumlarda, yine de kendisine ait her hangi bir verinin işlenmesine itiraz etmek için izin verilebileceği düzenlenmiştir. Hatırlanacağı üzere Direktif m. 7/e – f hükümleri, verilerin işlenmesinde hukuka uygunluk hallerinden iki tanesidir. Buna rağmen veri öznesinin özel durumuna ilişkin meşru ve mecburi gerekçelerin varlığı halinde izin verilmesi gerektiği belirtilmiştir. Ancak özel durumun ve mecburi gerekçelerin ne olduğuna dair bir açıklama yoktur. Bununla birlikte üye devletlerin, bu durumun aksine iç hukuklarında düzenleme yapabilecekleri paragrafın devamında belirtilmiştir.

Veri öznesi, m. 14/f. 1- b. (a) kapsamında, ulusal mevzuatlarda aksi durumun düzenlenmemiş olması şartıyla itiraz hakkını her zaman kullanabilecektir. Maddenin birinci fıkrasının (b) bendi hükmüne göre ise itiraz hakkının işlemden önce kullanılacağı çıkarılmaktadır. Hakkın işlemden önce kullanılması, hakkın özüne zarar vereceği gerekçesi ile eleştirilmektedir²⁹¹.

Kanun'da itiraz hakkı ayrı başlık altında olmayıp, Kanun'un dördüncü bölümü altında *Veri sorumlusuna başvuru* yan başlıklı 13. maddesi ile *Kurula şikâyet* yan başlıklı 14. maddesinde düzenlenmiştir. 13. maddeye göre ilgili kişi, bu Kanunun uygulanması ile ilgili bir talebinin olması durumunda, bunu yazılı olarak veya Kurulun

²⁹⁰ Başalp, 50, kişisel verilerin silinmesi ve yok edilmesi ile ilgili olarak bkz. s. 17 vd.

²⁹¹ Detaylı bilgi için bkz. Başalp, 51

belirleyeceği diğer bir yöntemle veri sorumlusuna iletebilecektir. Talebi alan veri sorumlusu, başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içerisinde sonuçlandırmak durumundadır. İlgilinin talebi veri sorumlusu tarafından kabul edilebilir veya gerekçesi yazılmak şartıyla reddedilebilir ve veri sorumlusu tarafından verilen kabul ya da ret cevapları yazılı olarak veya elektronik ortamda ilgisine bildirilir. Talebin kabulü halinde gereği veri sorumlusu tarafından yerine getirir. Talebin reddi durumunda veya verilen cevabın başvuru sahibi tarafından yetersiz görülmesi ya da süresinde başvuruya cevap verilememesi hallerinde 14. madde gereğince ilgili kişi, Kurula şikâyetle bulunabilir. Şikâyet başvurusu ilgili kişi tarafından, veri sorumlusunun cevabının öğrenildiği tarihten itibaren otuz gün, her hâlükârda başvuru tarihinden itibaren altmış gün içinde yapılmalıdır. Kurul, 15. maddeye göre şikâyet üzerine gerekli incelemeyi başlatır. Maddenin beşinci fıkrasına göre Kurul, inceleme neticesinde ihlalin varlığı kanaatine varırsa, tespit edilen bu hukuka aykırılıkların giderilmesini veri sorumlusundan isteyeceği gibi telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırı bir durumun olması halinde, yedinci fıkra hükmüne dayanarak kişisel verilerin işlenmesinin veya bu verilerin yurt dışına aktarılmasının durdurulmasına karar verebilecektir.

Madde metinlerine dikkat edilirse itiraz ile ilgili hiçbir ifadeye yer verilmeyip ilgilinin talebi ve şikâyet şeklinde düzenleme yapılmıştır. Oldukça geniş yorumlanan bu hakkın²⁹², uluslararası düzenlemeler ve Kanun'un lafzının birlikte değerlendirilmesi ile ilgilinin itiraz hakkının, iç hukukumuz açısından 13. ve 14. maddeler kapsamında kullanılabilecek bir hak olduğu anlaşılmaktadır. Zira 13. maddede başvurunun, bu Kanunun uygulanması ile ilgili taleplerle ilgili olarak bu düzenlemenin var olduğu ve bu taleplerin de neler olabileceğinin belirlenmesi gerekmektedir. 95/46/AT sayılı Direktif'in 14. maddesi kapsamında ilgili kişinin kendisine dair verilerin işlenmesine ve doğrudan pazarlamaya ilişkin durumlara her zaman itiraz edebileceği ifade edilmiştir. Kanun'un 13. maddesi bünyesinde de bu talepler içerisinde ilgilinin kişisel verilerinin işlenmesine dair bir olumsuzluğu, başvuru ile veri sorumlusuna bildirmesi mümkün olabilecektir. Ayrıca 2008 tarihli Tasarı'nın 12. maddesinde *İlgili kişinin hakları* ve 13. maddesinde de *Başvuru usulü* düzenlenmişti. 13. madde metninde yer alan "12 inci maddeye göre başvurular..." ifadesinden, bu maddenin açıkça ilgilinin bu Kanun

²⁹² Küzeci, 218-219

kapsamında sahip olduğu haklarının kullanılmasına yönelik olduğu anlaşılmaktaydı. 6698 sayılı Kanun'da, Tasarı hükmünde olduğu gibi açık bir göndermeye yer verilmemiş olmasına rağmen, Kanun'un genel sistematüğinden ilgilinin itiraz hakkını m. 13 ve 14 kapsamında kullanabileceğı anlaşılmaktadır. Yine 15. madde metninde yer alan “... yapılan inceleme sonucunda, ihlalin varlığının anlaşılması halinde...” ifadesinden ilgilinin, hakkında kişisel verilere ilişkin yapılmış olan bir işleme karşı itirazda bulunmak üzere şikayete bulunduğu anlaşılmaktadır.

3.2.4. Zararın Giderilmesi Hakkı

3.2.4.1. Kanuni Düzenleme

İlgilinin haklarının düzenlendiğı 11. maddenin son bendinde ilgili kişi, kişisel verilerinin, kanuna aykırı işlenmesi neticesinde bir zarara uğraması durumunda, bu zararın giderilmesini talep edebileceğı hüküm altına alınmıştır. Madde metnindeki düzenlemede, zararın maddi veya manevi olacağına dair bir ifade olmamakla birlikte, bu zararın nereden, kimden ve nasıl talep edileceğine de yer verilmemiştir. Madde metni ve Kanun sistematüğü birlikte değerlendirildiğinde ilgilinin, zarara uğraması durumunda öncelikle veri sorumlusuna başvurmak suretiyle bir talepte bulunabileceğı, devamında Kurula şikâyet yoluyla talebini iletmek suretiyle bu zararının giderilmesini isteyebileceğı anlaşılmaktadır.

Ancak Kurula şikâyeti düzenleyen 14. maddenin üçüncü fıkrasında ilgilinin kişilik haklarının ihlal edilmesi halinde, genel hükümlere gönderme yapılmak suretiyle tazminat istenebileceğı düzenlenmiştir. Buna göre zarar gören ilgili kişi, veri sorumlusunun özel hukuk gerçek ya da tüzel kişi olması durumunda adli yargı, kamu hukuku tüzel kişisi olması durumunda idari yargı dava açmak suretiyle zararının giderilmesini isteyebilecektir²⁹³.

3.2.4.2. Genel Hükümlere Göre Zararın Giderilmesi

Kişilik hakları ihlal edilen kişisel veri sahibi, veri sorumlusunun, özel hukuk gerçek ya da tüzel kişisi olması durumunda, Borçlar Kanunu hükümlerine göre adli

²⁹³ 6698 sayılı Kanun m. 14 gerekçesi

yargıda maddi veya manevi tazminat talep edebilme hakkına sahip iken, veri sorumlusunun kamu hukuku tüzel kişisi olması durumunda idari yargıda tam yargı davası ile bu zararının tazminini isteyebilecektir.

3.2.4.2.1. 6098 sayılı Borçlar Kanunu'na Göre Zararın Giderilmesi

İlgili kişi, özel hukuk gerçek ya da tüzel kişi veri sorumlusunun kişisel verileri işlenmesinden kaynaklanan zararını, 6098 sayılı BK'na göre maddi ve manevi tazminat davaları ile gidermesi mümkün olabilecektir.

3.2.4.2.1.1. Maddi Tazminat Davası

Maddi tazminat davası, haksız fiil neticesinde zarara uğrayan kimsenin, haksız fiili işleyen kimseden uğradığı bu zararın giderilmesini talep ettiği davadır. Bu davanın konusu, karşı tarafa zarar veren kişi ya da kişilerin, mağdurun uğradığı zararı, diğer bir ifadeyle mağdurun malvarlığında meydana gelen eksilmeyi ödemeye mahkûm edilmesidir²⁹⁴.

TBK m. 49/f. 1 hükmünde maddi tazminat davasının esas düzenlenmiştir. Buna göre kusurlu ve hukuka aykırı bir fiille bir başkasına zarar veren kimse, vermiş olduğu bu zararı gidermek zorundadır. Bu hüküm uyarınca kişilik hakkının ihlali nedeniyle açılacak olan maddi tazminat davalarında kusur sorumluluğu esas olup 6698 sayılı Kanun m. 14/f. 3 hükmü gereğince kişilik hakları ihlal edilen veri sahibi kişi, TBK'nın bu hükmüne dayanarak uğradığı zararın giderilmesini talep edebilecektir. TBK uyarınca veri sahibinin, zararını tazmin ettirebilmesi için TBK m. 50 uyarınca karşı tarafın kusurunu ve kendisinin uğradığı maddi zararı ve bu zararın miktarını ispat etmesi gerekmektedir²⁹⁵. Bunların yanında haksız fiil nedeniyle ilgilinin tazminat talep edilebilmesi için, haksız fiil sorumluluğunun şartları olarak ortada bir fiilin bulunması, bu fiil neticesinde bir zararın doğması, bu zarar ile fiil arasında illiyet bağının var

²⁹⁴ Eren, 724, Kemal Oğuzman, Turgut Öz, *Borçlar Hukuku Genel Hükümler*, Cilt 2, Gözden Geçirilmiş 10. Bası, Vedat Kitapçılık, İstanbul 2013, 67 vd.

²⁹⁵ Eren, 724

olması ve nihayet fiili işleyen kişinin bu fiili kusurlu şekilde işlemiş olması gerekmektedir²⁹⁶.

3.2.4.2.1.2. Manevi Tazminat Davası

Kişisel verileri hukuka aykırı olarak işlenmesi dolayısıyla kişilik hakları ihlal edilenlerin, kişiliğin korunması ve dolayısıyla da kişisel verilerinin korunmasını sağlayacakları bir diğer yol da manevi tazminat davasıdır²⁹⁷. TBK m. 58/f. 1 hükmü gereğince kişilik hakkı zedelenmesi neticesinde zarara uğrayan kişi, uğradığı manevi zarara karşılık manevi tazminat talebinde bulunabilecektir. Bu anlamda manevi tazminat davası, mağdurun isteği dışında kişilik değerlerinde bir eksilmenin olması, kişilik hakkını ihlal edici davranış neticesinde manevi olarak duyulan acı, üzüntü, ızdıraptan kaynaklanan zararların giderilmesi amacına hizmet etmektedir²⁹⁸. TBK'nın bu hükmü kişilik hakları ihlal edilenleri korumaya yönelik özel hükümler (TBK m. 56 gibi) haricinde var olan genel bir sorumluluk hükmüdür²⁹⁹. Eren'e göre şeref, haysiyet, ticari itibar, kişinin sır ve özel hayat alanı, aile hayatı ve çevresi, özgürlükler, resim hakkı gibi sosyal ve duygusal kişilik değerlerinin ihlalinden doğan manevi zararlar, TBK m. 58 kapsamında değerlendirilmektedir. 58. madde kapsamında değerlendirilecek hallere dikkat edildiğinde, bunların kişisel veri kavramı içerisinde değerlendirilebilecekleri görülmektedir. Dolayısıyla da kişisel verilerin işlenmesi suretiyle kişilik hakları ihlal edilenlerin, bu hüküm uyarınca uğradıkları zararları tazmin edebilmeleri yerinde bir yol olacaktır.

Kişilik hakkı ihlal edilen kişisel veri sahibinin, TBK m. 58 uyarınca manevi tazminat davası açabilmesi için bir takım şartların var olması gerekmektedir. Öncelikle bir kişilik hakkının ihlal edilmiş olması gerekmektedir. Akabinde bu ihlal neticesinde manevi bir zararın doğmuş olmalıdır. Hukuka aykırı bir fiille bu manevi zararın ortaya çıkması gerekmektedir. Ortaya çıkan manevi zarar, hukuka aykırı fiilin neticesinde

²⁹⁶ Bkz. Eren, 516 vd., Oğuzman, Öz, 11 vd., Ahmet Kılıçoğlu, *Borçlar Hukuku Genel Hükümler*, Genişletilmiş 17. Bası, Turhan Kitabevi, Ankara 2013, 273 vd.

²⁹⁷ Aksoy, 88

²⁹⁸ Eren, 780 vd.; Oğuzman, Öz, 253 vd.; Kılıçoğlu, 432 vd.

²⁹⁹ Eren, 792

doğmuş olmalı, diğer bir ifadeyle zarar ile fiil arasında illiyet bağı var olmalıdır. Son olarak da ihlali gerçekleştirenin sorumlu olmasını gerektiren kusuru var olmalıdır³⁰⁰.

3.2.4.2.2. Tam Yargı Davası ile Zararın Giderilmesi

İlgili kişinin kişisel verilerinin işlenmesi nedeniyle uğrayabileceği zarar, kamu tüzel kişiliğine sahip ya da devlet tüzel kişiliği altındaki bir veri sorumlusunun kişisel veri işleme faaliyeti bünyesinde de gerçekleşebilir. Bu durumda ilgili kişi, uğrayacağı bu zararın tazminini idari yargıda tam yargı davası ile tazmin etmesi mümkün olabilecektir.

İdari Yargılama Usul Kanunu (İYUK) m. 2' de idari dava türleri arasında düzenlenen tam yargı davası, idarenin yapmış olduğu eylem ya da işlemler nedeniyle kişilik hakları doğrudan doğruya ihlal edilen bireyler tarafından uğradıkları zararların tazmin edilmesi için açılacak bir idari davadır³⁰¹. Diğer bir anlatımla tam yargı davası, tazminat davasının idare hukukundaki görünümüdür³⁰². Kişisel verilerinin işlenmesi dolayısıyla hakları ihlal edilen veri sahibinin, uğradığı zararların tazmini için tam yargı davası açabilmesi, yani davaya taraf olabilmesi için dava ehliyetine sahip olması yanında *hak ihlali şartının* da gerçekleşmesi gerekmektedir. Buradan çıkan sonuca göre kişisel bir hakkı ihlal edilenler bu davayı açabileceklerdir³⁰³. 6698 sayılı Kanun'un 14. maddesinin son fıkra hükmü lafzında da net şekilde kişilik hakları ihlal edilenlerin genel hükümlere göre tazminat hakkı olduğu görülmektedir. Bu kapsamda kişisel verileri ihlal edilen veri sahibinin İYUK hükümleri gereğince, veri sorumlusu idari birime karşı tam yargı davası açabilmesi mümkün olabilecektir.

Belirtmek gerekir ki tam yargı davaları idari işlemlere karşı açılabilmesi gibi idari eylemler ve idari sözleşmeler neticesinde doğacak zararlara karşı da açılabilir. Bu ayırım tam yargı davalarında önkarar yönünden önemlidir³⁰⁴. İYUK m. 12 kapsamında açılacak olan tam yargı davasında ilgilinin hakkı bir idari işlem neticesinde ihlal edilmiş olması durumu söz konusudur ve bu durumda tam yargı davası açılmadan önce idareye

³⁰⁰ Bkz. Eren, 792 vd.; Oğuzman, Öz, 256 vd.

³⁰¹ Şeref Gözübüyük, Turgut Tan, *İdare Hukuku Cilt: II İdari: Yargılama Hukuku*, Güncelleştirilmiş 7. Bası, Ankara 2014, 942, Kemal Gözler, Gürsel Kaplan, *İdare Hukuku Dersleri*, Güncelleştirilmiş 15. Baskı, Bursa 2014, 837

³⁰² Gözler, Kaplan, 837

³⁰³ Gözler, Kaplan, 840

³⁰⁴ Gözübüyük, Tan, 615 vd.; Gözler, Kaplan, 839

başvuru şartı aranmamaktadır³⁰⁵. Ancak m. 13'e göre hakları ihlal edilenler, belli süreler dâhilinde idareye başvurarak haklarının yerine getirilmesini talep etmeleri yani bir önkarar almaları gerekmektedir³⁰⁶. İlgilinin rızası olmaksızın kişisel verilerinin, kamu hukuku tüzel kişisi veya veri sorumlusu idare tarafından yurt içinde veya yurt dışına aktarılması, idari eylem nedeniyle tam yargı davası açılmasına örnek olabilecek durumdur.

3.3. KİŞİSEL VERİ SAHİBİNİN DİĞER HAKLARI

6698 sayılı Kanun dışında, diğer kanunlarda yer alan hükümlerle de ilgilinin kişisel verilerinin, dolayısıyla da kişisel verilerin korunmasının temel amacı olarak kişilerin temel hak ve özgürlüklerinin korunması mümkün olabilecektir. Bu başlık altında hukukumuzda hiç düzenlenmemiş ancak oldukça önem arz eden unutulma hakkı ve 4982 sayılı Bilgi Edinme Hakkı Kanunu kapsamında bilgi edinme hakkı incelenmiştir.

3.3.1. Unutulma Hakkı

Unutulma hakkı, kişisel verilerin korunmasını da yakından ilgilendirecek şekilde, son dönemde bilişim teknolojileri alanındaki gelişmeler neticesinde gündeme gelmiş bir haktır. Bilgisayar teknolojisinin yanında internetin de hızlı bir şekilde insanlığın günlük yaşamı içerisine girmesi ile sanal ortamda yapılan işlemlerin arkasında iz bırakması ya da bu sanal ortamlarda bilerek veya bilmeyerek kişilerin bir takım veriler paylaşması ve paylaşılan bu verilerin sanal ortamlarda kalıcı olması, verilerin sürekli tehlike altında kalmasına neden olmaktadır. Belirtmek gerekir ki bu ortamlarda paylaşılan verilerin büyük bir kısmı kişisel veri olarak nitelendirilebilecek türdendir. Örneğin kişiler Facebook, Twitter, Google+ gibi sanal sosyal ağlarda, kendilerine profil oluştururken, kendilerini tanıtmaya yönelik bilgiler kullanmakta, bu profillerde fotoğraf, adres, eğitim bilgileri, video vb. veriler paylaşmaktadırlar. Ayrıca internet üzerinden alış-veriş siteleri veya online bankacılık hizmetlerinde de kişisel veriler kullanılmakta ve saklanmaktadırlar. Kişilere ait bu profiller başkaları tarafından görüntülenebilmekte ve hatta burada paylaşılan verileri ziyaretçi, kendi profiline aktarılabilir. Bu da

³⁰⁵ Gözler, Kaplan, 841,

³⁰⁶ Gözler, Kaplan, 841; Gözübüyük, Tan, 621 vd.

göstermektedir ki kişilerin özel hayatları alenileşmekte, kişisel verilerin, veri öznesinin izni olmaksızın üçüncü kişilerin eline geçme tehlikesi söz konusu olmaktadır. Diğer bir anlatımla sanal ortamda temel hak ve özgürlüklerin ihlaline yönelik suçlar işlenmektedir³⁰⁷. Kişilerin, sahip oldukları haklar üzerinde serbestçe tasarrufta bulunabilecekleri de dikkate alındığında, altında bulundukları olası tehlikelerden korunmak adına bu hakka sahip olmaları bir ihtiyaçtır.

Unutulma hakkı, daha ziyade dijital ortamda kaydedilmiş olan kişisel verilere, kişinin iradesi ve rızası dışında erişimin engellenmesini esas aldığından, özü itibarıyla bu hakkın, “*dijital bir silgi*” işlevi gördüğünü söylemek mümkündür³⁰⁸.

Hakkın ortaya çıkışı noktasında Alman hukukunda, genel olarak kişilik haklarının etkili olduğu söylenebilir. Bu anlamda özel hayatın gizliliği hakkı bünyesinde kişilik hakları, insanın bedensel ve ruhsal bağımsızlığını ve bütünlüğünü de korumaktadır ve bu hakkın kaynağı anayasadır. Bunun yanında mahkemeler de bu hakkın güvence altına alınmasına ilişkin içtihatlar oluşturmuşlardır³⁰⁹. Unutulma hakkı, Alman Hukukunda Kanunda açıkça düzenleme altına alınmamış olmakla birlikte, Federal Almanya Veri Koruma Yasası (Bundesdatenschutzgesetz, BDSG)’nda bu hak, hangi şartlar altında kişiye ilişkin verilerin silinebileceği çerçevesinde ele alınmaktadır³¹⁰. Yine bunun yanı sıra, ceza hukuku kapsamında işlenen suçların kayıt sürelerine ve bunların muhafaza sürelerine dair kanuni düzenlemeler de bulunmaktadır. Hamburg Eyalet Mahkemesi (OLG Hamburg), 2015 yılında verdiği bir kararında³¹¹ bu konuya değinmiştir. Karara konu olayın özünde, internet ortamında arama motoruna, ilgilinin isminin yazılması suretiyle bulunan veya ulaşılan kişisel verilere erişimin engellenmesi söz konusudur. Mahkeme kararının önemli olan yanı ise bu şekilde internet ortamında sadece ilgili

³⁰⁷ Serdar Güleler, Dijital Hafızın Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak “Unutulma Hakkı”, 225, Erişim Tarihi: 24.06.2014, <http://tbbdergisi.barobirlik.org.tr/m2012-102-1218>; Aslıhan Bozkurt, Sanal ortamda “unutulmak” bir hak mı?, 94, Erişim Tarihi: 24.06.2014, http://www.bilisimdergisi.org/s161/pages/s161_web.pdf.

³⁰⁸ Bu yönde bkz. Cai Rienäcker, “*Mehr Datenschutz im Internet EU fordert "Recht auf Vergessen" im Netz*” Erişim Tarihi: 17.01.2016, <http://www.tagesschau.de/ausland/datenschutz288.html>.

³⁰⁹ Heinrich Amadeus Wolff, Das Recht auf Vergessen im Datenschutzrecht-Nationalrechtliche und europarechtliche Begründungen, Forderungen sowie deren Bewertung, 34, Erişim Tarihi: 24.06.2014, http://www.rewi.europa-uni.de/de/lehrstuhl/or/staatsrecht/_dokumente/arbeiten/Kozirolek-SPB3-USP-OeR-HA.pdf.

³¹⁰ Bu kapsamda bkz., BDSG, § 20 (Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht).

³¹¹ İlgili karar için bkz. Erişim Tarihi: 17.01.2016, <http://www.internet-law.de/2015/08/das-olg-hamburg-und-das-recht-auf-vergessenwerden.html>.

kişinin isminin arama motoruna girilmesi ile kişiyle ilgili önemli habere ulaşılmasında, ilgili kişi, bu haberin arşivden silinmesini isteyebilme hakkına değil, bu arşivde yer alan habere ilgilinin isminin arama motoruna yazılması suretiyle erişimin engellenmesini talep hakkı olduğu yönünde karar verilmesidir.

Yukarıdaki açıklamalarla birlikte unutulma hakkı, dijital hafızada veya sanal ortamda yer alan kişisel içeriğe ilişkin verilerin, kişinin talebi üzerine kalıcı olmak üzere silinmesi şeklinde tanımlanabilir³¹². Bu hakkın, temel insan hakları içerisinde kabul edilmesinde Avrupa Komisyonu' nun konuya ilişkin olarak verdiği 25 Ocak 2012 tarihinde verilerin korunması hakkında değişiklik teklifinin³¹³ öncülük yaptığı ve etkili olduğu söylenebilir. İlgili teklifin Değişiklik ve Silme başlıklı üçüncü bölümü altında, 17. maddede unutulma hakkı düzenlenmiştir. Düzenleme hükmüne göre veri denetçisi, veriler çok uzun süredir kullanılmıyorsa ve bu verilerin kullanılmasına rıza gösterilmiyorsa, verileri silmek zorundadır ve daha fazla yayılmalarının engellenmesinden sorumlu olacaktır. Maddenin üçüncü fıkrasında istisnai durumlar düzenlenmiştir. Buna göre de ifade özgürlüğünün korunması, genel sağlığı ilgilendiren konuda kamu yararının bulunması, tarihsel, istatistiksel ve bilimsel amaçlarla veya üye devletlerin hukuk sistemlerinin gerekli kıldığı durumlarda veriler tutulabilecek ve saklanabilecektir³¹⁴.

Alman Anayasa Mahkemesi, unutulma hakkına dair, kişilik hakkıyla birlikte kural olarak kişinin kendisine ilişkin verilerin açıklanması ve bunların kullanılmasıyla ilgili yetkisini ve kendisine ilişkin bilgiler üzerindeki kaderini tayin etme yetkisi anlaşılması gerektiğini belirtmiştir. Ancak kendi kaderini tayin etme kişiye, kendisini görmek istediği şekil için başkalarından bir talepte bulunma hakkı vermeyecektir. Aksi durumda hem hak amacını aşmış olacak hem de üçüncü kişilerin özgürlük alanları ihlal edilmiş olacağı belirtilmiştir. Bu açıklamalarla, Alman Anayasası kapsamında, verinin kendisinin değil, kişinin özgür gelişiminin korunmak istendiği ifade edilmiştir³¹⁵.

Unutulma hakkı, İsviçre Federal Mahkemesi kararlarında da yer almış bir kavramdır. Unutulma hakkı kavramıyla Federal Mahkeme, İsviçre Medeni Kanunu

³¹² Güleener, 226.

³¹³ İlgili değişiklik teklifinin tam metni için bkz. Erişim Tarihi: 24.06.2014, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

³¹⁴ Güleener, 234

³¹⁵ Wolff, 35

(ZGB) m. 28'deki çerçeve normlardan yola çıkarak somutlaştırmaktadır. Unutulma hakkı akılda kalan bir kavramdır ancak tam olarak da tanımlanmış değildir. Federal Mahkeme'ye göre unutulma hakkı kavramı esas olarak doğru hatırlanma kavramının karşısında yer almaktadır. Kişi hakkında sahip olunan bilginin iyi bir bilgi olmadığı durumlarda bu, unutulma hakkının ihlali olarak kabul edileceği belirtilmiştir³¹⁶. Federal Mahkeme 1970li yılların sonunda vuku bulan Irniger Davası'nda unutulma hakkını, İsviçre Medeni Kanunu m. 28'deki genel klostlardan geliştirmiştir³¹⁷.

Türkiye' de, unutulma hakkı ile ilgili yasal bir düzenleme mevcut değildir. Ancak kişilerin özel hayatlarına, haberleşme özgürlüklerine, kişisel verilerin hukuka aykırı olarak kaydedilmesi ve kullanılması ve kişilik haklarına saldırı durumunda genel kanunlardaki hukuki korumalardan istifade etmek suretiyle bu hakkın, dolaylı olarak kullanılması söz konusu olabilecektir.

Yargıtay, 2015 yılında vermiş olduğu bir kararında unutulma hakkından söz etmiştir. İlgili kararda unutulma hakkı “ *üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerinin silinmesini ve yayılmasının önlenmesini isteme hakkı...*” olarak tanımlanmıştır. Hatta kararda yer alan tanım Yargıtay tarafından genişletilmiş; unutulma hakkının sadece dijital ortamlarda yer alan durumlara yönelik olmadığı, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilerin de bu kapsamda yer alması gerektiği belirtilmiştir. Bu nedenle, unutulma hakkının, yalnızca kişiye ilişkin dijital ortamda saklanan verilerin, sürekli bir biçimde erişime açık olmasının engellenmesini değil, buraya dâhil olmayan ancak kolayca ulaşılabilen verilere de ulaşımın engellenmesini kapsadığını rahatlıkla söyleyebiliriz. Yargıtay'a göre unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, esas olarak kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Çünkü kararda belirtildiği üzere her iki hakkın da temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır.

³¹⁶ Bruno Glaus, “Das Recht auf Vergessen und das Recht auf korrekte Erinnerung” 2004, Heft 4, 82, Erişim Tarihi: 24.06.2014, <http://wifimaku.com/medienrecht-schweiz/files/5669173/Recht+auf+Vergessen+und+das+Recht+auf+korrekte+Erinnerung.pdf>-

³¹⁷ İlgili karar ve benzer kararlar için bkz. Glaus, 81 vd

Unutulma hakkı ile kişinin geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay dolayısıyla kişinin geleceğinin olumsuz şekilde etkilenmesinin engellenmesine yöneliktir. Bu sayede kişi, geçmişinde yaşadığı olumsuz etkilerden kurtulmak suretiyle geleceğini şekillendirebilecektir³¹⁸.

3.3.2. 4982 sayılı Bilgi Edinme Hakkı Kanunu Kapsamında Bilgi Edinme Hakkı

İlgilinin, hakkında kişisel verilerine dair yapılmış olan her türlü işleme dair bilgi edinmesine olanak sağlayan diğer bir durum da genel kanun olan 4982 sayılı BEHK'dır.

3.3.2.1. Genel Olarak Bilgi Edinme Hakkı

Avrupa Birliği'ne uyum sürecinde, 09.10.2003 tarihinde 4982 sayılı Bilgi Edinme Hakkı Kanunu (BEHK) kabul edilmiş ve yürürlüğe girmiştir. 2010 yılı Anayasa değişikliği ile 1982 Anayasası'nın 74. madde başlığı "*Dilekçe, Bilgi Edinme ve Kamu Denetçisine Başvurma Hakkı*" olarak değiştirilmiş, madde metnine de "*Herkes, bilgi edinme ve kamu denetçisine başvurma hakkına sahiptir.*" fıkrası eklenmiştir. Anayasada yapılan bu değişikliklerle "*Bilgi Edinme Hakkı*" anayasal bir hak olmuştur.

Bilgi edinme hakkı, BEHK m. 4 hükmüne göre, kişilerin, bu kanunun sınırları dâhilinde, kamu kurum ve kuruluşları bünyesinde bulunan bilgi ve belgelere erişebilme hakkı olarak tanımlanabilir. Doktrinde de bilgi edinme hakkına ait yapılmış tanımlar yer almakla birlikte tanımlar arasında birlik olmadığı, zira bu kavramın henüz yeni gelişmekte olan bir kavram olmasından dolayı farklı anlamlar da taşıdığı belirtilmiştir. Yapılan tanımların ortak noktalarında yola çıkarak bilgi edinme hakkının "*devletin / idarenin tek taraflı iradesiyle, kişilerin ve toplumun hukuki durumunda değişiklik oluşturan eylem, işlem ve kararlarına ilişkin bilgilerin herhangi bir özel yararın ispatına gerek olmaksızın, bireyler tarafından elde edilmesini garanti altına alan bir insan hakkı*" olarak tanımlanmıştır³¹⁹.

Bilgi edinme hakkı, kişilerin temel hak ve özgürlüklerini kullanmaları açısından var olması gereken bir haktır. Zira kişinin kendisini ilgilendiren ya da kendisine ait ne tür bilgi ve belgelerin, nerede veya kimin elinde olduğunu öğrenmek, bilmek istemesi,

³¹⁸ Yargıtay Hukuk Genel Kurulu'nun E. 2014/4-56, K. 2015/1679 sayılı kararı

³¹⁹ Döner, 96 vd.

kişinin en doğal hakkıdır. Diğer yandan bu hak, demokratik ve şeffaf bir yönetimin varlığı için önemli rol oynamaktadır³²⁰. Bireylerin, yaşadığı toplumun durumu ve kendilerini yönetenler hakkında bilgi sahibi olmaları için, resmi belgelere erişim hakkı sağlanarak devlet yönetiminde şeffaflığın ve hesap verilebilirliğin yerleştirilmesi, ayrıca eşitlik ilkesinin daha iyi uygulanabilmesi için bilgi edinme hakkının varlığı muhakkaktır³²¹.

Bu kanun kapsamında, bilgi edinme hakkı kullanılmak üzere, sadece kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarına başvuruda bulunulacaktır. Diğer bir ifadeyle özel sektör olarak ifade edilebilecek birimlerden, bu kanun hükümlerine dayanılarak bilgi edinme hakkı kapsamında talepte bulunulamayacaktır.

BEHK m. 4 hükmüne göre, herkes, bilgi edinme hakkına sahip olmakla birlikte, hakkın kullanılması açısından Türkiye Cumhuriyeti vatandaşları ile yabancılar arasında farklılık söz konusudur. Vatandaşlar, bu hakka mutlak olarak sahiptirler. Türkiye’de ikamet eden yabancılar ile Türkiye’de faaliyette bulunan yabancı tüzel kişiler, ancak karşılıklılık ilkesi çerçevesinde ve talepte bulundukları bilgilerin kendileri ve faaliyetleri ile ilgili olması şartıyla bu haktan yararlanabileceklerdir.

Bilgi edinme hakkı kapsamında hak sahiplerinin talebi üzerine, ilgili kurum veya kuruluş, istisnalar saklı kalmak üzere, her türlü bilgi ve belgeyi başvuru sahibinin yararlanmasına sunmak durumundadır. Ancak belirtmek gerekir ki, başvurulmuş kurum ve kuruluşun bu zorunluluğu, başvurulmuş kurum ve kuruluşun elinde bulunan veya görevleri gereği bulunması gereken bilgi ve belgeler ise mevcut olacaktır. Diğer yandan istenilen bilgi veya belgeler ayrı veya özel bir çalışma, araştırma veya inceleme neticesinde elde edilebilecekse, bu durumda ilgili kurum veya kuruluş, yapılan başvurulara olumsuz cevap verebilir³²².

Bilgi edinme hakkının kullanılması kapsamında başvuruda bulunulan kamu kurum ve kuruluşları, başvuru sahibine olumlu veya olumsuz olmak üzere³²³, mutlaka

³²⁰ BEHK m. 1

³²¹ Firuz Demir Yaşamış, *Türkiye Barolar Birliği Bilgi Edinme Paneli*, Türkiye Barolar Birliği Yayınları: 62, Ankara 2004, 42

³²² BEHK m. 7

³²³ Ayhan Küçük, *Bilgi Edinme Hakkının Sınırları ve Bu Hakkın İhlalinde İdare ve Kamu Görevlilerinin Sorumluluğu*, Sayıştay Dergisi, Sayı 81, 114

yazılı olarak cevap vermek durumundadır. Olumsuz cevap verilmesi durumunda, başvuru talebinin neden reddedildiğine dair gerekçeler ve başvurunun reddedilmesi üzerine başvurulabilecek kanun yollarının da yazılı olarak bildirilmesi zorunludur³²⁴.

Diğer tüm haklarda olduğu gibi, bilgi edinme hakkının da hak sahibi tarafından hiçbir sınırlamaya tabi olmaksızın kullanılması mümkün olmayacaktır. Bu hakkın kullanılmasında kamu menfaati ile kişisel menfaatler dikkate alınarak, adil bir dengenin sağlanması gerekmektedir. Aksi durumda hak ve özgürlüklerin kullanılmasında çatışma, bunun neticesinde de bu hak ve özgürlük ihlalleri meydana gelecektir³²⁵. Hak ihlallerinin önlenmesine yönelik BEHK'nun *Bilgi Edinme Hakkının Sınırları* başlıklı dördüncü bölümü altında, hakkın kullanılmasının sınırları düzenlenmiştir.

3.3.2.2. Kişisel Verilerin Korunması İle İlişkisi

Teknolojik gelişmeler ve buna paralel olarak her alanda bilgiye olan talep artarak ilerlemektedir. İdare, yönetim fonksiyonu çerçevesinde pek çok bilgi toplar³²⁶. İdarenin, özellikle kamu hizmetlerini sağlıklı ve verimli yürütebilmesi için, kişisel nitelikteki bilgilere fazlasıyla ihtiyacı vardır. Ancak bu durum bireylerin, kişisel nitelikteki verilerinin dolayısıyla da özel hayatlarının gizliliğini ve güvenliğini tehdit etmektedir. Bu nedenle her ne sebeple olursa olsun elde edilmiş bilgilerin, ilgili bireylerin özel hayatlarına zarar vermeyecek şekilde kullanılmaları gerekmektedir. Burada yasa koyuculara düşen görev, bu tehditlerin, gerek hukuki düzenlemelerin yapılarak, gerekse teknolojik önlemlerin alınarak hak ihlallerinin önlenmesini ve bireylerin temel hak ve özgürlüklerini kullanmalarına müsait ortamları oluşturmaktır³²⁷.

Bu bağlamda, kişisel verilerin korunması hakkı ile bilgi edinme hakkı, birbirlerini yakından ilgilendiren haklardır. Gerçekten de bilgi edinme hakkı ile kişisel verilerin korunması hakkı, birbirlerine ters iki amaca yönelmiş iki hak görünümündedir. Her ikisi de bireye ait temel hak olmakla birlikte, biri bilgiye ulaşmayı ya da bilgiyi öğrenmeyi amaçlarken, diğeri bilgiye erişimi veya bilgiyi öğrenmeyi engellemeye yöneliktir. Bilgi edinme hakkının kullanılması kapsamında edinilmek istenen bilginin, diğer bir kişiye ait

³²⁴ BEHK m. 12

³²⁵ Nusret İlker Çolak, *Bilgi Edinme Hakkının Sınırları ve Sınırlama Ölçütleri*, Parg. 2, Erişim Tarihi: 29.06.2014, <http://www.e-akademi.org/makaleler/nicolak-1.htm>.

³²⁶ Çolak, Parg. 7

³²⁷ Tortop, 2

kişisel veri niteliğinde bir bilgi olma ihtimali göz önünde bulundurulduğunda, bu iki hakkın birbirleri ile ne derece yakından ilgili olduğu anlaşılmaktadır. Bu iki hakkın birbirleri ile çatışan haklar olması münasebeti ile hangisinin öncelikli hak olduğunun belirlenmesi, hak ve özgürlüklerin gereği gibi bireylerce kullanılması açısından ayrıca bir öneme sahiptir. Aksi takdirde hak ve özgürlüklerin karşı karşıya gelmesi durumunda nasıl hareket edileceğinin bilinmemesi, bu hak ve özgürlüklerin gereği gibi kullanılamamasına ve ortadan kalkmasına neden olabilecektir³²⁸.

Bilgi edinme hakkı ile kişisel verilerin korunması hakkının ilişkili olduğu diğer bir durum da, bilgi edinme hakkına getirilen sınırlamalardan özel hayatın gizliliği ve haberleşmenin gizliliği içerisinde kişisel nitelikteki verilerin de var olabilmesidir³²⁹. BEHK m. 21' e göre kişinin sağlık bilgilerine, özel ve aile hayatına, şeref ve haysiyetine, mesleki ve ekonomik değerlerine dair bilgi ve belgelerin, bu kanunun kapsamı dışında tutulmuştur. Madde metninde özel hayat olarak düzenlenmiş bulunan alanlara ait bilgi ve belgelerin, Veri Koruma Hukuku kapsamında kişisel veri olarak kabul edilecek veriler oldukları açıktır. Ayrıca önceki başlıklarımız altında da ifade ettiğimiz gibi kişisel veriler, kişinin özel hayatının bir parçasıdır (2.3.1.1. 1982 Anayasası başlığı). Bu bağlamda, bilgi edinme hakkının BEHK kapsamında sınırlarından birinin kişisel nitelikteki veriler olması, bu iki hak arasındaki münasebetin diğer bir göstergesidir.

³²⁸ Çolak, . Parg. 2

³²⁹ Dinç, 23

SONUÇ

Yaklaşık son otuz yıllık süreçte ve özellikle de bu sürenin son dönemlerinde teknolojik ilerleme, takip edilemeyecek hızda gelişmiş ve gelişmeye de devam etmektedir. Bu hızlı gelişmenin insan hayatını kolaylaştırdığı da bir gerçektir. Bu kolaylığın başında da insanoğlunun ihtiyaç duyduğu bilgiye rahatlıkla ulaşması gelmektedir. Ancak her nimetin bir de külfeti olduğu da göz önünde bulundurulmalıdır. Kolaylıkla ulaşılan bu bilgilerin şüphesiz ki bir paylaşıcı bir de sahibi vardır. İşte bu noktada bilginin ait olduğu kişilerin, bu hızlı bilgi trafiği içerisinde özellikle temel hak ve özgürlükler noktasındaki pozisyonunun da korunması gerekliliği ön plana çıkmaktadır.

Diğer yandan özel sektörde ve kamu sektöründe faaliyetlerin daha etkin ve verimli olarak sürdürülebilmesi için bireylere ait bilgilere yani kişisel verilere ihtiyaç duyulmaktadır. Her iki sektördeki aktörlerin, faaliyetlerini sürdürmede rakiplerine karşı ayakta kalmaları, onların güçlü olmaları ile yakından ilgilidir. Günümüz dünyasında gücün simgesi de bilgi olarak yerini almıştır. Bu aktörler bu anlamda güçlü olabilmek ve güçlü kalabilmek için başta kişisel veriler olmak üzere hızlı bir şekilde bilgi depolama çabası içerisindeyler.

Gelinen noktada bireyin kişisel verilerinin korunması, bu suretle de modern hukuk anlayışının temeli olarak kişi temel hak ve özgürlüklerinin korunması ihtiyacı daha bir önemli ve elzem hale gelmiştir.

Veri korumaya yönelik uluslararası alanda bazı hukuki düzenlemeler yapılmıştır. Bu düzenlemeler, ulusal düzeydeki düzenlemelere yol göstermesi veya örnek teşkil etmeleri açısından önemli düzenlemelerdir. Özellikle de Avrupa'da yeknesak bir veri koruma sistemi oluşturulma çabası, bu düzenlemelere öncülük etmiştir. Bu doğrultuda Avrupa Konseyi'nin 108 sayılı Sözleşmesi, örnek olması yanında Konsey üyesi devletler açısından bağlayıcılığı olan bir düzenleme olması nedeniyle ayrı bir öneme sahiptir. Yine Avrupa Birliği tarafında çıkarılan başta 95/46/AT sayılı Direktif olmak üzere 2002/58/AT sayılı ve 2006/24/AT sayılı direktifler de bu alanda yürürlüğe konulmuş uluslararası düzenlemelerdir. Kişisel verilerin korunmasına yönelik diğer bir düzenleme ise Avrupa Birliği Temel Haklar Şartı kapsamında ayrı bir hak olarak kişisel verilerin korunması hakkı eklenmiştir.

Bu düzenlemelerin yegâne amacı, kaçınılmaz şekilde kişisel verilere ulaşabilmenin olduğu bu dönemde, bu verilere ulaşmanın, verileri işlemenin, aktarmanın ve depolamanın, bu alandaki hukuki düzenlemelerde yer alan hükümlere uygun şekilde yapılması suretiyle bireyin kişisel verilerin başkalarının elinde olmasından dolayı mağduriyetinin önlenmesi ve bu yolla temel hak ve özgürlüklerinin korunmasının sağlanmasıdır.

Ülkemizde, kişisel verilerin korunması serüveni 108 sayılı Sözleşmenin imzalanması ile başlamıştır. Ancak diğer Avrupa ülkelerine nazaran sözleşmenin gereklerinin yerine getirilmesi biraz geç olmuştur. Özellikle müstakil bir veri koruma kanununa sahip olunması bir hayli gecikmiş ve AB uyum sürecinde müstakil bir veri koruma kanununa sahip olmamasından dolayı Türkiye sürekli olumsuzluklar yaşamış ve eleştirilmiştir. Nihayet 24 Mart 2016 tarihinde kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu ile müstakil bir veri koruma kanunu Türkiye’de yürürlüğe girmiştir. Çalışmamızın Birinci Bölümünde 6698 sayılı Kanunda tanımlanmış olan kişisel verilerin işlenmesi kavramı, Alman Veri Koruma Kanunu (BDSG)’da yer alan açıklamalar da dikkate alınarak somutlaştırılmaya gayret gösterilmiştir. Bu anlamda kişisel verilerin işlenmesi kavramının, verilerin toplanması, kaydedilmesi, değiştirilmesi, kullanılması ve kullanılmasının engellenmesi, silinmesi kavramları ile yakından ilişkili olduğu ve bu kavramlar ile birlikte daha net anlaşılabilceği kanaatine varılmıştır. Yine kişisel verilerin işlenmesi hususu altında veri işlemenin ancak istisnai hallerde mümkün olabileceği, bu istisnaların başında da ilgili kişinin açık rızasının varlığının gerektiği ulusal ve uluslararası düzenlemelerde hüküm altına alınmıştır. Ulusal mevzuatımızda da veri sorumlusu tarafında kişisel veri işlenebilmesi açık rıza beyanının varlığına bağlanmıştır. Mevzuatımızda *açık rıza* kavramı ile ne kastedildiği belirsiz olsa da bu ifade ile, Kanun’un veri sorumlusuna yüklediği aydınlatma yükümlülüğü ile ilintili olmak üzere açık rızanın aslında aydınlatılmış rıza beyanı olduğu sonucu çıkarılmıştır.

Çalışmamızın İkinci Bölümü altında özellikle 6698 sayılı Kanun’un yürürlüğe girmesinden önceki temel hukuki düzenlemeler ve ülkemiz açısından kişisel verilerin korunması ile ilgili yasal bir düzenlemeye duyulan ihtiyacın nedenleri tespit edilmeye çalışılmıştır. Bu doğrultuda münferit bir veri koruma kanununa ülkemiz açısından ilk olarak kişisel verilerin esasını oluşturan hususların bağımsız bir kanun ile düzenlenmesi,

bu konuya özgü felsefenin ve ilkelerinin ortaya konulması açısından önem arz etmesi gerekçesiyle ihtiyaç duyulduğu, ikinci olarak ise uluslararası üyeliklerin gereklerinin yerine getirilmesi nedeniyle ihtiyaç duyulduğu saptanmıştır.

Çalışmamızın üçüncü ve son bölümünde ilgilinin kişisel verilerin işlenmesi sürecinde karşılaşacağı olumsuz durumlar karşısında sahip olduğu ve olması gereken hakları üzerinde durulmuştur. Ülkemizde toplum nezdinde kişisel veriler ve bu verilerin korunmasının önemi daha yeni yeni anlaşılmaya başlanmıştır. Ayrı bir veri koruma kanunu ile bireylerin bu alana ilişkin düzenlemelerin ve özellikle de hukuka aykırı şekilde kişisel veri işlenmesi karşısında sahip oldukları haklarının neler olduğunu bilmeleri, hem uygulamada hem de teoride oldukça önem arz etmektedir. Zira sadece yasalaşma faaliyetleri, insan haklarının gerçekleştirilmesi açısından yeterli olmayacak, toplumsal farkındalığın da oluşturulması gerekecektir. Bu bağlamda ilgili, başta 6698 sayılı Kanun kapsamında sahip olduğu bilgi edinme hakkına, verilerin düzeltilmesini, silinmesini ve yok edilmesini isteme hakkına, Kanun'da şikâyet ve başvuru olarak düzenlenmiş olan itiraz hakkına sahiptir. Mevzuatımızda kişisel verilerin korunmasına dair 4982 sayılı Kanun'a göre de ilgili kişi bilgi edinme hakkına, yine 6698 sayılı Kanun'un verdiği yetki ile bu Kanun'un uygulanmasından kaynaklanan zararların genel hükümlere göre giderilmesi mümkün olup bu kapsamda, veri sorumlusunun özel hukuk gerçek ya da tüzel kişi olması durumunda 6098 sayılı Kanun kapsamında maddi ve manevi tazminat davası, veri sorumlusunun kamu hukuku tüzel kişisi olması durumunda ise tam yargı davası ile bu zararın giderilmesini isteme hakkına sahiptir. İlgilinin sahip olduğu bu haklar mevzuatımızda yer alan haklar olup ilgili mevzuatta yer almayan ancak kişisel verilerin korunması ile bağlantılı ve sahip olunması gereken bir hak olan unutulama hakkına da sahip olması gerektiği sonucuna varılmıştır.

KAYNAKÇA

- Akgül, Aydın, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, Beta Yayınevi, İstanbul 2014
- Aksoy, Hüseyin Can, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, Çakmak Yayınevi, Ankara 2010
- Aldanmaz, Orhan, “İnsan Onuru Işığında Kişisel Özerklik ve Yerellik İlkesi”, *EÜHFD*, XIV(1-2), 2010.
- Atak, Songül, “Avrupa Konseyi’nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler”, *TBB Dergisi*, sayı 87, yıl 2010
- Atak, Songül, “Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri”, *Bahçeşehir Üniversitesi Hukuk Fakültesi Kazancı Hakemli Hukuk Dergisi*, sayı 59-60, yıl 2009
- Başalp, Nilgün, *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınevi, Ankara 2004
- Bilici, Nurettin, *Avrupa Birliği ve Türkiye*, Seçkin Yayıncılık, Ankara 2010
- Bulut, Nihat, “Eski Yunan’dan Aydınlanma Çağına İnsan Onuru Kavramının Gelişimine Genel Bir Bakış”, *EÜHFD*, XII(3-4), 2008.
- Blechta, Gabor P., (Ed: Maurer – Lambrou Blechta), *Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz*, 3. Auflage, Helbing Lichtenhahn Verlag, 2014 Basel
- Bozkurt, Aslıhan, *Sanal Ortamda “Unutulmak” Bir Hak mı?*, Erişim Tarihi: 24.06.2014, http://www.bilisimdergisi.org/s161/pages/s161_web.pdf.
- Büyük Türkçe Sözlük*, Erişim Tarihi: 29.10.2015, http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.563f0b98be0390.80067468.
- Çakmak, Haydar, *Türkiye Avrupa Birliği İlişkileri*, 3. Baskı, Ankara 2011

- Çelik, Halil, Türkiye'nin "Kişisel Verileri Koruma" Serüveni, Erişim Tarihi: 01.07.2015, <http://hacehissiyasa.blogspot.com.tr/2014/01/turkiyenin-kisisel-verileri-koruma.html>.
- Çolak, Haluk / Taşkın, Mustafa, *Ceza Muhakemesi Kanunu Şerhi*, Seçkin Yayıncılık, Ankara 2007
- Çolak, Nusret İlker, *Bilgi Edinme Hakkının Sınırları ve Sınırlama Ölçütleri*, Erişim Tarihi: 29.06.2014, <http://www.e-akademi.org/makaleler/nicolak-1.htm>.
- T.C. Cumhurbaşkanlığı Devlet Denetleme Kurumu Denetleme Raporu, Erişim Tarihi: 01.07.2015, <https://www.tccb.gov.tr/assets/dosya/ddk56.pdf>.
- Dinç, Engin, *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye'nin Durumu* (Yayınlanmamış Yüksek Lisans Tezi), Diyarbakır 2006
- Erdoğan, Mustafa, *Küreselleşme, Hukuk ve Türkiye*, Uzun, Turgay / Özen, Serap (Ed.). *Avrupa Birliği Sürecinde Türkiye*, Seçkin Yayıncılık, Ankara 2004
- Eren, Fikret, *Borçlar Hukuku Genel Hükümler*, Beta Yayınevi, Düzeltilmiş 12. Baskı, İstanbul 2010
- Ersoy, Eren, *Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması*, Erişim Tarihi: 05.01.2014, <http://ab.org.tr/ab06/bildiri/6.doc>.
- Ersoy, Uğur, *Bir İnsan Hakkı Olarak Kişisel Verilerin Korunması* (Yayınlanmamış Yüksek Lisans Tezi), Ankara 2009
- Hafızoğulları, Zeki / Özen, Muharrem, "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar", *Ankara Barosu Dergisi*, yıl 67, Sayı:4, Güz 2009
- Giritli, İsmet / Akgüner, Tayfun / Bilgen, Pertev / Berk, Kahraman, *İdare Hukuku*, Der Yayınları, İstanbul 2012
- Glaus, Bruno, "Das Recht auf Vergessen und das Recht auf korrekte Erinnerung" 2004, Heft 4, Erişim Tarihi: 24.06.2014, <http://wifimaku.com/medienrecht-schweiz/files/5669173/Recht+auf+Vergessen+und+das+Recht+auf+korrekte+Erinnerung.pdf>.
- Gözler, Kemal / Kaplan, Gürsel, *İdare Hukuku Dersleri*, Güncelleştirilmiş 15. Baskı, Bursa 2014

- Gözübüyük, Şeref / Gölcüklü, Feyyaz, *Avrupa İnsan Hakları Sözleşmesi ve Uygulaması*, Turhan Kitabevi, 8. Baskı, Ankara 2009
- Gözübüyük, Şeref / Tan, Turgut, *İdare Hukuku Cilt: II İdari: Yargılama Hukuku*, Güncelleştirilmiş 7. Bası, Ankara 2014
- Gülener, Serdar, *Dijital Hafızan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak “Unutulma Hakkı”*, Erişim Tarihi: 24.06.2014, <http://tbbdergisi.barobirlik.org.tr/m2012-102-1218>.
- Günday, Metin, *İdare Hukuku*, İmaj Yayınevi, Ankara 2011
- Karimi, Oldouz / Korkmaz, Adem, *Kişisel Verilerin Korunması*, Erişim Tarihi: 10.08.2016, <http://inet-tr.org.tr/inetconf18/bildiri/63.pdf>.
- Kaya, Cemil, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası Prof. Dr. İl Han Özey’a Armağan*, LXIX(1-2), 2011.
- Kılıçoğlu, Ahmet, *Borçlar Hukuku Genel Hükümler*, Genişletilmiş 17. Bası, Turhan Kitabevi, Ankara 2013
- Kılınç, Doğan, “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, *AÜHFD*, Sayı 61 (3), yıl 2012, 1089-1169
- Korkmaz, İbrahim, *Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme*, Erişim Tarihi: 01.05.2016, <http://tbbdergisi.barobirlik.org.tr/m2016-124-1571>.
- Küçük, Ayhan, “Bilgi Edinme Hakkının Sınırları ve Bu Hakkın İhlalinde İdare ve Kamu Görevlilerinin Sorumluluğu”, *Sayıştay Dergisi*, Sayı 81.
- Küzeci, Elif, *Kişisel Verilerin Korunması*, Turhan Yayınevi, Ankara 2010
- Mahmutoğlu, Fatih Selami, *Beden Muayenesi ve Vücuttan Örnek Alınması*, Erişim Tarihi: 15.08.2016, <http://fsmahmutoglu.av.tr/pdf/76b00da1de336791f454b4977f6319d9cdf4656d7818071225.pdf>.
- Maurer, Ustr – Blechta, Lambrou / Kunz, Simon, (Ed: Maurer – Lambrou Blechta), *Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz*, 3. Auflage, Helbing Lichtenhahn Verlag, 2014 Basel

- Parlar, Ali / Hatipoğlu, Muzaffer, *5237 Sayılı Türk Ceza Kanunu Yorumu*, Seçkin Yayıncılık, Ankara 2010
- Oğuzman, Kemal / Barlas, Nami, *Medeni Hukuk*, 18. Bası, Vedat Kitapçılık, İstanbul 2012
- Oğuzman, Kemal / Öz, Turgut, *Borçlar Hukuku Genel Hükümler*, Cilt 2, Gözden Geçirilmiş 10. Bası, Vedat Kitapçılık, İstanbul 2013
- Okur, Nurdan, *Anayasa Hukuku Açısından Özel Hayatın Gizliliği ve Korunması* (yayınlanmamış doktora tezi), Ankara 2010
- Özbek, Veli Özer, *Yeni Türk Ceza Kanununun Anlamı*, Seçkin Yayıncılık, Ankara 2008
- Özdemir, Hayrunnisa, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, Seçkin Yayınevi, Ankara 2009
- Özdemir, Hayrunnisa, *Haberleşmenin Gizliliği ve Kişisel Veriler*, EÜHFD, C. XIII, s. 1-2, yıl 2009
- Özenç, Köksal, *Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması*, Erişim Tarihi: 05.01.2014, <http://www.iscturkey.org/s/2226/i/2007-26.pdf>.
- Pfister, Christa Stamm, (Ed: Maurer – Lambrou Blechta), *Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz*, 3. Auflage, Helbing Lichtenhahn Verlag, 2014 Basel
- Rienäcker, Cai, “*Mehr Datenschutz im Internet EU fordert "Recht auf Vergessen" im Netz*” Erişim Tarihi: 17.01.2016, <http://www.tagesschau.de/ausland/datenschutz288.html>.
- Selk, Robert, *Datenschutz und Internet*, Der Andere Verlag, München 2002
- Seyidoğlu, Halil, *Ekonomik Terimler*, Geliştirilmiş 3. Baskı, İstanbul 2002
- Tinnefeld, Marie-Theres / Buchner, Benedikt / Petri, Thomas, *Einführung in Das Datenschutzrecht*, Oldenbourg Verlag, München 2012
- Topaloğlu, Mustafa, *Bilişim Hukuku*, Karahan Yayınevi, Adana 2005

- Tortop, Nuri, “Çağımızın Önemli Sorunu: Kişisel Bilgilerin Güvenliği Sorunu”, *Amme İdaresi Dergisi*, 33(3), Eylül 2000.
- Uygun, Murat, *Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması* (Yayınlanmamış Yüksek Lisans Tezi), Ankara 2010
- Weihert, Thilo/ Däubler, Wolfgang/ Klebe, Thomas/ Wedde, Peter, *Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG*, 3. Vollständig neu bearbeitete Auflage, Nördlingen 2010
- Wolff, Heinrich Amadeus, *Das Recht auf Vergessen im Datenschutzrecht-Nationalrechtliche und europarechtliche Begründungen, Forderungen sowie deren Bewertung*, Erişim Tarihi: 24.06.2014, http://www.rewi.europa.uni.de/de/lehrstuhl/or/staatsrecht/_dokumente/arbeiten/Koziolak-SPB3-USP-OeR-HA.pdf.
- Yaşamış, Firuz Demir, *Türkiye Barolar Birliği Bilgi Edinme Paneli*, Türkiye Barolar Birliği Yayınları: 62, Ankara 2004
- Yılmaz, Hasan, *TS ISO / IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi*, Erişim Tarihi: 10.08.2016, <http://kidder.dergipark.gov.tr/download/article-file/208742>.
- Yurtcan, Erdener, *CMK Şerhi*, Cilt I, 7. Baskı, Adalet Yayınevi, Ankara 2015

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Kerim KILIÇ
Doğum Yeri ve Tarihi	Trabzon 29.03.1983
Eğitim Durumu	
Lisans Öğrenimi	Atatürk Üniversitesi Erzincan Hukuk Fakültesi
Y. Lisans Öğrenimi	Atatürk Üniversitesi Sosyal Bilimler Enstitüsü
Bildiği Yabancı Diller	Almanca
Bilimsel Faaliyetleri	
İş Deneyimi	
Stajlar	Avukatlık Stajı (2006 – 2007 Trabzon Adliyesi)
Projeler	
Çalıştığı Kurumlar	Erzincan Üniversitesi (Öğr. Gör.)
İletişim	
E-Posta Adresi	kkilic@erzincan.edu.tr av.kerimkilic@gmail.com
Tarih	31.08.2016