

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI

YÜKSEK LİSANS TEZİ

**AVRUPA BİRLİĞİ VE TÜRK HUKUKUNDA
KİŞİSEL VERİLERİN KORUNMASI
VE
BÜYÜK VERİ**

Şehriban İpek AŞIKOĞLU
2501141480

TEZ DANIŞMANI
Prof. Dr. Mustafa AKSU

İSTANBUL – 2018



T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



YÜKSEK LİSANS
TEZ ONAYI

ÖĞRENCİNİN;

Adı ve Soyadı : ŞEHRİBAN İPEK AŞIKOĞLU Numarası : 2501141480
Anabilim Dalı / Anasanat Dalı / Programı : ÖZEL HUKUK Danışmanı : PROF.DR.MUSTAFA AKSU
Tez Savunma Tarihi : 28.08.2018 Saati : 10:00
Tez Başlığı : AVRUPA BİRLİĞİ VE TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI VE BÜYÜK VERİ

TEZ SAVUNMA SINAVI, İÜ Lisansüstü Eğitim-Öğretim Yönetmeliği'nin 36. Maddesi uyarınca yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin KABULÜNE OYBİRLİĞİ / OYÇOKLUĞUYLA karar verilmiştir.

JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1- PROF.DR. ARSLAN KAYA		
2- PROF.DR.MUSTAFA AKSU		Basarılı / Kabul
3- DR.ÖĞR.ÜYESİ. MESUT SERDAR ÇEKİN		Basarılı / Kabul

YEDEK JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1- DR.ÖĞR.ÜYESİ.R. FATİH AYDOĞAN		Basarılı (Kabul)
2- DR.ÖĞR.ÜYESİ.KORAY DEMİR		

ÖZ

AVRUPA BİRLİĞİ VE TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI VE BÜYÜK VERİ ŞEHRİBAN İPEK AŞIKOĞLU

Günümüzde baş döndürücü teknolojilerin her gün bir yenisi günlük hayatımıza dâhil olurken, artık teknolojiyi yakalamak için gündemi değil geleceği takip etmek elzem bir hale gelmiştir. Sanayi 4.0, üretimden tüketime tedarik zincirinin her aşamasında değişim ve dönüşüm getirmektedir. Bu dönüşümde yer alan akıllı teknolojiler, nesnelerin interneti, sensörler, bulut hizmetleri ve robotlar sürekli veri üretmektedir. Büyük yığınlar halindeki bu veri setleri, günümüzde büyük veri uygulamaları ve teknolojileri ile kısa süre içerisinde işlenebilmektedir. Büyük veri içerisinde kişisel veri önemli bir yer tutmakla birlikte profillemeye ve otomatik karar mekanizmaları sonuçlarından bireyler de doğrudan etkilenmektedir. Kişisel verilerin işlenmesi artık sadece bir özel hayatın gizliliği sorunu olarak ele alınamamaktadır. Geliştirilen algoritmalar ve etkileri kişinin kendini ifade etmesi, geliştirmesi, geleceğini belirleyebilmesi haklarına dokunmaktadır. Kıta Avrupası'nda yarım asırlık bir geçmişi olan kişisel verilerin korunması hukuku, verinin işlenmesi ve akışının yaratmış olduğu değer ile bireylerin menfaatlerini dengelemenin yollarını aramaktadır. Türkiye'de ise yakın zamanda uygulanmaya başlayan Kişisel Verilerin Korunması Kanunu kapsamında yeni teknolojilerin nasıl değerlendirileceği önümüzdeki süreçte şekillenecektir. Bu çalışma kapsamında kişisel verilerin korunmasına ilişkin hukuki yapı anlatılırken büyük veri uygulamalarının yaratmış olduğu ekonomik menfaat ile kişisel verilerin korunması hukukunun ilkeleri arasındaki çatışma ortaya konacaktır. Bir başka deyişle büyük veri uygulamalarının kişisel verilerin korunması hukuku çerçevesinde uygunluk sorunu değerlendirilecektir.

Anahtar Kelimeler: kişisel veri, büyük veri, sanayi 4.0, kişisel verilerin korunması

ABSTRACT

PERSONAL DATA PROTECTION UNDER EUROPEAN UNION AND TURKISH LAW AND BIG DATA ŞEHRİBAN İPEK AŞIKOĞLU

Nowadays, new technologies are becoming a part of our daily life at an unprecedented pace. For catching up with technology, it has become essential to follow the future rather than the present. Industry 4.0 introduces change and transformation at every stage of the supply chain from production to consumption. Smart technologies, internet of things, sensors, cloud services and robots, involved in this transformation produce data constantly. These datasets, which are large masses, can be processed in a short time with big data applications and technologies. Personal data take an important place within big data and individuals are directly affected by the results of profiling and automatic decision-making process. Currently, processing of personal data cannot be considered solely as a problem of privacy. Developed algorithms and their effects touch individuals' right to self-expression, self-determination. In Continental Europe, the protection of personal data, which is a half-century old legal field, is seeking ways to balance the interests of individuals and the value of data. In Turkey, very new Personal Data Protection Law will shape the approach and usage of new technologies in the coming period. In this study, while explaining the legal structure for the protection of personal data, the conflict between the economic interests created by big data applications and the principles of the protection of personal data will be discussed. In other words, the issue of legitimacy of big data applications will be evaluated in the context of the legal framework of data protection.

Keywords: personal data, big data, industry 4.0, personal data protection.

ÖNSÖZ

Kişisel verilerin korunması alanında bu çalışmayı yaparken gerek mevzuat gerekse teknoloji anlamında hep güncel olanı yakalamaya çalıştım. Bilhassa Türk hukuku açısından yeni yeni tartışılmakta olan bu konuyu ele almak benim için oldukça heyecanlıydı. Günümüzde etkisini her alanda hissettiğimiz büyük veri uygulamalarını, kişisel verilerin korunması penceresinden Avrupa Birliği hukuku ve Türk hukuku ile karşılaştırarak anlatmaya çalıştım.

Öncelikle İstanbul Üniversitesi Hukuk Fakültesi Ticaret Hukuku Anabilim Dalı Başkanı ve Dekan sıfatıyla huzurlu bir çalışma ortamı sağladığı için Prof. Dr. Abuzer Kendigelen'e çok teşekkür ederim. Asistanlığını yaptığım ve tez jürimde yer almayı kabul ederek beni onurlandıran Prof. Dr. Arslan Kaya'ya saygılarımı ve teşekkürlerimi sunarım.

Tez çalışmam boyunca beni kısıtlamayan, beni dinleyen ve desteklerini esirgemeyen tez danışmanım Prof. Dr. Mustafa Aksu'ya çok teşekkür ederim.

Tezimle ilgili yapıcı eleştirilerini benimle paylaşarak jürimde yer almayı kabul eden Dr. Mesut Serdar Çekin'e, tezimin okumasını, tahsisini büyük bir titizlikle gerçekleştiren Araş. Gör. F. Pelin Tokcan'a ve bu süreçte bana anlayış gösteren İstanbul Üniversitesi Hukuk Fakültesi Ticaret Anabilim Dalı Hocalarına, Araştırma Görevlilerine çok teşekkür ederim.

Son olarak bu çalışmayı hazırlayabilecek olgunluğa erişmemde başrolü oynayan ve desteklerini esirgemeyen annem Meral Aşıkoğlu ve babam Haydar Aşıkoğlu'na teşekkür ederim. İkinci olarak ise çalışmanın hazırlanması sürecinde yapmış olduğu fedakârlık ve katkılardan dolayı beni sabırla destekleyen ablam Gamze Aşıkoğlu'na minnettar olduğumu belirtmek isterim. Yine bu çalışmanın hazırlanması sırasında değerli görüşlerini ve katkılarını esirgemeyen Turgut Uğurlu, Av. Burak Uzun ve Av. Yasemen Öztürkcan ve kişisel veri kavramı ile beni tanıştıran Av. Yasin Beceni, Av. Tuğrul Sevim, Av. Nilay Erdem ve Av. Çağatay Pekiör'ü teşekkürlerimi sunarım.

ŞEHRİBAN İPEK AŞIKOĞLU

İSTANBUL, 2018

İÇİNDEKİLER

ÖZ	iii
ABSTRACT	iv
ÖNSÖZ	v
İÇİNDEKİLER	vi
KISALTMALAR	x
GİRİŞ	1

BİRİNCİ BÖLÜM

KAVRAMLAR VE TARİHSEL GELİŞİM

1.1. Kişisel Veri ve Büyük Veri Kavramları	5
1.1.1. Genel Olarak Kişisel Veri Kavramı	5
1.1.1.1. Bilgi	6
1.1.1.2. Bilginin Kişiyeye İlişkin Olması	10
1.1.1.3. Kimliği Belirli veya Belirlenebilir Bir Kişi	12
1.1.2. Genel Olarak Büyük Veri Kavramı	19
1.1.2.1. Büyük Verinin Kaynakları	22
1.1.2.2. Büyük Verinin Kapsamı	24
1.2. Kişisel Verilerin Korunması	24
1.2.1. Kişisel Verilerin Korunması Hukukunda Korunan Menfaat	24
1.2.2. Kişisel Verilerin Kişilik Hakkı Olarak Korunması	26
1.2.3. Günümüzde Hızla Gelişen Teknolojiler Işığında Artan Kişisel Verilerin Korunması İhtiyacı	28
1.3. Kişisel Verilerin Korunmasının Tarihsel Gelişimi	31
1.3.1. OECD Rehber İlkeleri	34
1.3.2. Avrupa Konseyi Düzenlemeleri	37
1.3.2.1. 108 sayılı Sözleşme	40
1.3.2.2. 108 sayılı Sözleşme'ye Ek Protokol	42
1.3.2.3. 108 sayılı Sözleşme'ye Değişiklik Protokolü	43
1.3.2.4. Avrupa İnsan Hakları Sözleşmesi	44
1.3.3. Birleşmiş Milletler	49
1.3.4. Amerika Birleşik Devletleri Yaklaşımı	50

İKİNCİ BÖLÜM

AVRUPA BİRLİĞİNDE KİŞİSEL VERİLERİN KORUNMASI

2.1.	Genel Olarak.....	55
2.2.	Avrupa Birliği Veri Koruma Yönergesi	56
2.2.1.	Amaç	58
2.2.2.	Kapsam.....	59
2.2.3.	Yürürlükten Kalkma	60
2.3.	Avrupa Birliği Genel Veri Koruma Tüzüğü.....	61
2.3.1.	Kapsam ve Uygulama Alanı	62
2.3.2.	Genel Kavramlar	64
2.3.2.1.	Kişisel Veri.....	64
2.3.2.2.	Kişisel Verilerin İşlenmesi	67
2.3.2.3.	Veri Sorumlusu.....	67
2.3.2.4.	Veri İşleyen	69
2.3.3.	Veri Sorumlularının Uyması Gereken Temel İlkeler.....	71
2.3.4.	Kişisel Verilerin İşlenmesini Meşru Kılan Hukuka Uygunluk Nedenleri	75
2.3.4.1.	Açık Rıza	76
2.3.4.2.	Sözleşmenin Kurulması veya İfası Kapsamında Gerekli Olma	78
2.3.4.3.	Veri Sorumlusunun Tâbi Olduğu Yasal Yükümlülük	80
2.3.4.4.	Fiili İmkânsızlık Durumunda Yaşamsal Çıkarların Koruması.....	81
2.3.4.5.	Kamu Yararı ya da Resmi Bir Yetki Kullanımı	82
2.3.4.6.	Veri Sorumlusunun Üstün Meşru Menfaati	84
2.3.5.	Avrupa Birliği Genel Veri Koruma Tüzüğü ile Getirilen Yenilikler ...	86

ÜÇÜNCÜ BÖLÜM

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

3.1.	Genel Olarak.....	90
3.1.1.	1982 Anayasası	90
3.1.2.	Türk Medeni Kanunu	93

3.1.3.	Türk Ceza Kanunu	95
3.1.4.	Türkiye’de Kişisel Verilerin Korunmasına Duyulan İhtiyaç	98
3.2.	6698 sayılı Kişisel Verilerin Korunması Kanunu	101
3.2.1.	Amaç ve Kapsam	101
3.2.2.	Genel Kavramlar	102
3.2.2.1.	Kişisel Veri	103
3.2.2.2.	Kişisel Verinin İşlenmesi	104
3.2.2.3.	Veri Sorumlusu	106
3.2.2.4.	Veri İşleyen	107
3.2.3.	Veri Sorumlularının Uyması Gereken Genel İlkeler	108
3.2.4.	Kişisel Verilerin İşlenmesini Meşru Kılan Hukuka Uygunluk Nedenleri	110
3.2.4.1.	Açık Rıza	112
3.2.4.2.	Kanunlarda Açıkça Öngörülmüş Olma	115
3.2.4.3.	Fiili İmkânsızlık Durumunda Yaşamsal Çıkarların Koruması	118
3.2.4.4.	Sözleşmenin Kurulması veya İfası Kapsamında Gerekli Olma	119
3.2.4.5.	Veri Sorumlusunun Hukuki Yükümlülüğü	122
3.2.4.6.	Kişisel Verinin İlgili Kişi Tarafından Alenileştirilmesi	123
3.2.4.7.	Hakkın Tesisi, Kullanılması veya Korunması için Zorunlu Veri İşleme	125
3.2.4.8.	Veri Sorumlusunun Üstün Meşru Menfaati	126

DÖRDÜNCÜ BÖLÜM

BÜYÜK VERİ UYGULAMALARI BAKIMINDAN KİŞİSEL VERİLERİN KORUNMASI

4.1.	Genel Olarak	128
4.1.1.	Büyük Veri Uygulamaları ve İktisadi Menfaat	128
4.1.2.	Büyük Veri Uygulamalarında Yer Alan Algoritmalar	131
4.1.3.	Büyük Veri Uygulama Örnekleri	133
4.2.	Büyük Veri Uygulamaları Kapsamında Kişisel Verilerin İşlenmesi	138
4.2.1.	Otomatik Karar Alma Mekanizmaları	141

4.2.2. Profilleme	142
4.3. Büyük Veri Uygulamalarının Kişisel Verilerin Korunması Hukuku Bakımından Değerlendirilmesi.....	145
4.3.1. Büyük Veri Uygulamaları ve Genel İlkeler Uyumluğu	146
4.3.1.1. Hukuka ve Dürüstlük Kuralına Uygun Olma	147
4.3.1.2. Doğru ve Gerekliğinde Güncel Olma İlkesi	154
4.3.1.3. Belirli, Açık ve Meşru Amaçlar İçin İşlenme İlkesi.....	157
4.3.1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma	161
4.3.1.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre Kadar Muhafaza Edilme	165
4.3.2. Büyük Veri Uygulamaları ve Hukuka Uygunluk Sebepleri	169
4.3.2.1. Açık Rıza	170
4.3.2.2. Sözleşmenin Kurulması veya İfası Kapsamında Gerekli Olma	175
4.3.2.3. Kişisel Verinin İlgili Kişi Tarafından Alenileştirilmesi	179
4.3.2.4. Veri Sorumlusunun Üstün Meşru Menfaati	184
4.3.3. Büyük Veri Uygulamalarına Getirilen Düzenlemeler.....	187
4.3.3.1. Veri Koruma Etki Analizi ve Ön Değerlendirme	189
4.3.3.2. Tasarımdan İtibaren ve Varsayılan Ayarlarla Veri Koruması.....	192
SONUÇ.....	197
KAYNAKÇA.....	201

KISALTMALAR LİSTESİ

108 sayılı Sözleşme	: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
a.e.	: aynı eser
a.g.e.	: adı geçen eser
a.g.m.	: adı geçen makale
a.y.	: aynı yer
Avrupa Birliği Genel Veri Koruma Tüzüğü	: Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC
Avrupa Birliği Veri Koruma Yönergesi	: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data
bkz.	: bakınız
çev.	: çeviren
d.n.	: dipnot
ed.	: editör
haz.	: hazırlayan

m. : madde

OECD : The Organisation for Economic Co-operation and Development

OECD Rehber İlkeleri : Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

par. : paragraf

s. : sayfa

v.d. : ve diğçerleri

vd. : ve devamı

GİRİŞ

1. Konunun Önemi ve Takdimi

Günümüzde akıllı robotlar, büyük veri, nesnelerin interneti, üç boyutlu yazıcılar ve bulut teknolojileri ile tetiklenen dördüncü sanayi devrimi üretimden tüketime tedarik zincirinin her aşamasında etkilerini göstermeye başlamıştır. Bu etkiler kaçınılmaz olarak temel ilkeler üzerine inşa edilmiş hukuk dallarında değişim ve dönüşümü beraberinde getirmiştir. Kişisel veriler, kişiler özelinde ihtiva etmiş olduğu özel hayatın gizliliği ve kişilik haklarına ilişkin öneminin yanında, günümüzde ekonomik anlamda da bir değer olarak tartışılmaktadır. Bu nedenle kişisel verilerin hukuki çerçevesinin çizilerek düzenlenmesi bu dönüşüm içerisinde kaçınılmaz bir hal almıştır. Dünyada 1970'li yıllardan itibaren bilgisayar sistemleriyle işlenen kişisel verilerin korunmasına ilişkin getirilen genel ilkeler, günümüzde büyük veri uygulamaları ile geliştirilen kişisel veri işleme faaliyetleri doğrultusunda tekrardan ve çok daha yoğun şekilde tartışılmaktadır. Teknik ve ekonomik alandaki yeni ve hız kesmeyen gelişmeler, nesnelerin interneti, büyük veri, bulut sistemleri gibi uygulamalar bu tartışmanın yoğunlaşmasının arka planını oluşturmaktadır. Bu güncel gelişme ve kavramlar ile günümüz dünyasında yeni bir ekonomi oluşturulmakta ve kişisel veriler de bu ekonominin bir yapı taşı olarak yer alarak daha da önem kazanmaktadır. Avrupa Birliğinde, yıllar içerisinde geliştirilmiş olan hukuki yaklaşım doğrultusunda, yeni teknolojilerle birlikte yoğunlaşan kişisel veri işleme faaliyetlerini, ekonomik gelişmeleri engellemeden sağlamak üzerine düzenleme çalışmaları yapılmıştır. Türkiye'de ise 2016 yılından itibaren Kişisel Verilerin Korunması Kanunu ile kişisel verilerin korunması konusunda yürütülen çalışmalar artmıştır.

Kişisel verilerin korunması hukuku kapsamında temel prensip, bireylerin kişisel hak ve özgürlükleri ile veri akışı ve kişisel verilerin işlenmesinden elde edilen menfaatin dengelenmesidir. Bu doğrultuda genel olarak pek çok hukuki metinde kabul edilmiş genel ilkeler bu dengenin enstrümanları olarak bir uygunluk testi geliştirmektedir. Yürürlükteki hukuki metinler, kişisel verilerin işlenmesini engellemekten ziyade düzenlemektedir. Devletler kendi kültürel gereksinimleri uyarınca kişisel verilerin

işlenmesine ilişkin hukuka uygunluk sebeplerini iç hukuklarındaki düzenlemeler ile belirlemektedir.

Büyük veri uygulamalarıyla birlikte geliştirilen yeni sistemler ile genel ilkeler arasında bir çatışma olduğu ifade edilmektedir. Bu uygulamalar özellikle bireylerin kişisel verileri üzerindeki kontrolünü kısıtladığı gerekçesiyle eleştirilmektedir. Büyük veriyi, gelişmiş bilgisayar sistemleri ile işlenebilen geniş hacimli veri setleri olarak tanımlamak mümkündür. Günümüzde büyük verinin; hacim, hız ve çeşitlilik unsurları vurgulanmaktadır. Belirtmek gerekir ki büyük veri uygulamaları çok farklı kaynaklardan, çok sayıda elde edilmiş veriyi işleyebilen bilgisayar sistemlerinden oluşmaktadır ve çoğunlukla dijital dünyadan toplanan bu veriler teknik olarak birlerden ve sıfırlardan ibarettir. Büyük veri uygulamaları ile tekil olarak anlam ifade etmeyen veriler birleştirilerek yeni, anlamlı sonuçlar elde edilebilmektedir. Perakende sektörü, sağlık, sigorta hatta politika alanında dahi kullanılan büyük veri uygulamalarının, veri koruma hukukunun genel ilkeleri ve kişisel verilerin işlenmesine ilişkin olarak hukuka uygunluk sebepleri ışığında değerlendirilmesi ihtiyacı doğmaktadır.

2. Çalışmanın Sınırlandırılması

Dördüncü sanayi devriminin ortaya çıkardığı üç boyutlu yazıcı, nesnelerin interneti, büyük veri, yapay zekâ gibi sistemler borçlar hukuku, fikri mülkiyet hukuku, iş hukuku gibi pek çok hukuk dalında benimsenen ilkelerin tekrar değerlendirilmesini gündeme getirmiştir. Bu çalışmada büyük veri uygulamalarının kişisel verilerin korunması hukuku kapsamındaki etkileri, genel ilkeler ve hukuka uygunluk sebepleri ile sınırlı olarak incelenecektir. Büyük veri uygulamalarına temel olarak nesnelerin interneti, yapay zekâ kullanımı gibi teknolojiler ve ürettikleri veriler kaynaklık etmektedir. Sanayi 4.0'ın tartışılan yeniliklerinden olan büyük veri uygulamaları ile sınırlandırılan bu çalışmada yeri geldiğinde nesnelerin interneti yahut yapay zekâ kullanımlarına ve etkilerine büyük veri uygulamalarında kullanıldıkları ölçü ile sınırlı olarak yer verilecektir.

Büyük veri uygulamaları incelenirken büyük verinin barındırdığı veri grupları özelinde bir sınırlama yapmak gerekecektir. Bu bakımdan büyük veri uygulamaları

tarafından toplanan ve belirli bir kiři ya da kiřiler ile baęlantısı olamayan, örneęin ilkim deęiřiklikleri, ekolojik bilgiler, tarımsal ve ekonomik veriler alıřma kapsamına dâhil edilmeyecektir.

Bir kiřiyi belirli ya da belirlenebilir kılan veriler kiřisel veri olarak deęerlendirilerek alıřma kapsamında incelenecektir. Ancak özel nitelikli kiřisel veriler ve hukuka uygunluk kořulları hususi olarak incelenmeyecektir. Bunlara genel nitelikli kiřisel verilerin hukuka uygunluk sebepleri arasında karřılařtırmalı olarak deęinilecektir. Ancak iřbu alıřma büyük veri uygulamalarında saęlık verilerinin kullanılmasını incelememekte, bir bařka deyiřle hususi hükümleri ve yönetmelięi bulunan saęlık verilerinin iřlenmesi, bu alanın kendine özgü sorunları nedeniyle alıřma kapsamı dıřında bırakılmaktadır.

Kiřisel verilerin korunması hukuku kapsamında öngörülen yaptırım mekanizmaları ve sorumluluk rejimi, alıřma alanını genişletmemek amacıyla zorunlu bazı durumlar hari hususi olarak ele alınmamıřtır.

3. alıřmanın Planı

alıřma kapsamında birinci bölümde öncelikle kiřisel veri ve büyük veri kavramları açıklanarak kiřisel verilerin korunması, korunan menfaat ve kiřilik hakkı olarak korunması anlatılacaktır. Kiřisel veri koruma hukukunun temel ilkelerinin yer aldıęı metinler kiřisel verilerin korunması hukukunun tarihesi bařlıęı altında incelenecektir. İkinci ve üçüncü bölümde ise Avrupa Birlięi ve Türk hukukunda genel olarak kiřisel verilerin korunmasına iliřkin düzenlemeler ve düzenlemelerde yer alan kavramlar açıklanacaktır. Daha sonra büyük veri uygulamalarının veri iřleme metotları, kiřisel verilerin korunması hukuku baęlamında incelenecektir.

Günümüzde kiřisel verilerin korunması hukuku bakımından hâkim olan Avrupa Birlięi veri koruma ekolünde, kiřisel verilerin korunması bir kiřilik hakkı olarak düzenlenmekte ve kiřisel veri sahiplerinin menfaatleri üstün tutularak korunmaktadır. Benimsenen prensiplerin, büyük veri uygulamaları ve yarattıęı ekonomik deęer göz önünde bulundurularak incelenmesi gerekmektedir. Bu doęrultuda öncelikle Avrupa Birlięi ve Türk hukukunda veri koruma düzenlemelerinde yer alan hukuka uygunluk

sebepleri açıklanacaktır. Avrupa Birliği'nde 1995 yılından bu yana uygulanmakta olan Avrupa Birliği Veri Korunma Yönergesi, Mayıs 2018 tarihinde uygulanmaya başlanmış olan Avrupa Birliği Genel Veri Koruma Tüzüğü ile yürürlükten kaldırılmıştır. Bu nedenle Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında yer alan hukuka uygunluk nedenleri, Avrupa Birliği Veri Korunma Yönergesi yürürlük dönemi ile karşılaştırmalı olarak açıklanacaktır. Türk hukukunda ise 2016 yılında Resmî Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu henüz yeni yeni yürürlüğe girmiş olsa da içermiş olduğu hukuka uygunluk sebepleri Kanun'un gerekçesi ve Kişisel Verileri Koruma Kurumu tarafından yayımlanmış olan rehberler kapsamında değerlendirilecektir.

Son bölümde ise büyük veri uygulamaları bakımından önem arz eden profillemeye ve otomatik karar mekanizmalarına ilişkin düzenlemelere ve büyük veri uygulamaları kapsamında yürütülen kişisel veri işleme faaliyetlerinin genel ilkeler ve hukuka uygunluk sebepleri perspektifinden değerlendirilmesine yer verilecektir. Büyük veri uygulamaları bakımından uygulanabilecek olan düzenlemeler bu bölümde açıklanacaktır.

BİRİNCİ BÖLÜM

KAVRAMLAR VE TARİHSEL GELİŞİM

1.1. Kişisel Veri ve Büyük Veri Kavramları

1.1.1. Genel Olarak Kişisel Veri Kavramı

Kişisel veri kavramı, pek çok düzenleyici metinde¹ yer alan hali ile “*belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün veriler*” olarak tanımlanmaktadır. Yaygın olan bu tanım ile kişisel veri kapsamını mümkün olduğunca geniş tutmak amaçlanmaktadır. Bu tanım itibari ile kişisel veri, belli bir kimsenin kimliğine, etnik kökenine, dış görünüşüne veya finans, sağlık, öğrenim ve istihdam durumuna ilişkin olabilmektedir. Bununla birlikte bir kişinin bireysel ve toplumsal yaşantısına dair bilgiler ve çevresiyle kurduğu haberleşmeler de kişisel veri niteliği taşımaktadır. Benzer şekilde, bir kimsenin ikamet, iletişim ve banka kartı bilgileri ile kişisel düşünce ve inançları ve hatta internet kullanım alışkanlıklarına ilişkin bilgiler de kişisel veri kapsamında yer alabilmektedir.

¹ Bahsedilen tanımın geçtiği metinlere ve yer alan tanımlara ilişkin olarak:

OECD’nin 1980 yılında yayınlamış olduğu ilkelerin 1/b maddesinde “*“personal data” means any information relating to an identified or identifiable individual (data subject)*”, bkz. OECD, “**Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**”, 23 Temmuz 1980, (Çevrimiçi) http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, 19 Nisan 2018; 108 sayılı Avrupa Konseyi Sözleşmesi’nin 2/a maddesinde, “*“personal data” means any information relating to an identified or identifiable individual (“data subject”)*”, bkz. Avrupa Konseyi, “**Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**”, 28 Ocak 1981, (Çevrimiçi) <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>, 19 Nisan 2018; 95/46/EC sayılı Avrupa Birliği Yönergesi 2/a maddesinde, “*“personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*”, bkz. “**Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data**”, 24 Ekim 1995, (Çevrimiçi) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>, 19 Nisan 2018; 7 Nisan 2016’da Resmi Gazete’de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun tanımlara ilişkin 3/d maddesinde, “*“kişisel veri, kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi”*” olarak tanımlanmıştır.

Üzerinde görüş birliği bulunan kişisel veri tanımından yola çıkarak, kişisel veri kavramının bilgi, kişiye ilişkin olma ve kimliği belirli veya belirlenebilir bir kişi olmak üzere üç temel unsurdan oluştuğunu söylemek mümkündür. Sayılan bu unsurlar, Article 29 Working Party² tarafından yayımlanmış olan kişisel veri kavramına ilişkin belirsizlik ve yaklaşım farklılığını bertaraf etmek amacı taşıyan görüş metninde³ yer almakta ve açıklanmaktadır.

1.1.1.1. Bilgi

Kişisel veri kavramını açıklarken gerek Avrupa Birliği mevzuatı gerekse Kişisel Verilerin Korunması Kanunu kapsamında kullanılan ve Article 29 Working Party tarafından yayımlanan Rapor'da⁴ da belirtilen ilk unsur bilgidir. Ancak bilgi unsuruna değinmeden önce veri, bilgi ve enformasyon kavramlarına ilişkin deyimisel bir açıklama yapmak gerekmektedir. Sayılan kavramlar arasındaki ilişki ve farklılık, sadece veri koruma hukuku bakımında değil, bilgi toplumu süreçlerinin açıklanması bakımından da farklı disiplinlerce tartışılan bir konudur. Doktrinde “veri” (**data**), “enformasyon” (**information**) ve “bilgi” (**knowledge**) sözcükleri arasındaki ilişki ve bunların birbirleri yerine kullanımları tartışmalı bir alan oluşturmaktadır. Bazı yazarlar bu üç terimin birbirlerinin yerine geçiyormuş gibi kullanımının önemli bir hata oluşturduğuna, deyimler arasında farklılık bulunduğuna işaret etmektedir⁵. Veri,

² Article 29 Working Party, 95/46 sayılı Avrupa Birliği Veri Koruma Yönergesi'nin 29. maddesi çerçevesinde kurulan ve veri koruması ile mahremiyet konularında Avrupa Birliği bünyesinde bağımsız danışma organı olarak faaliyet gösteren çalışma grubudur. Article 29 Working Party'nin görevleri 95/46 sayılı Avrupa Birliği Veri Koruma Yönergesi'nin 30. maddesi ve 2002/58 Sayılı Avrupa Birliği Yönergesi'nin 15. maddesi ile belirlenmiştir. Article 29 Working Party, kişisel verilerin işlenmesi konusunda bireylere yönelik korumanın sağlanması, elektronik haberleşme sektöründe temel hak ve özgürlüklerin ve meşru menfaatlerin korunması konularında Avrupa Komisyonu'nun danışma organı konumundadır. Article 29 Working Party görüşleri, teorik olarak bağlayıcı olmasalar da Avrupa Komisyonu ve Avrupa Birliği üye devletleri bünyelerinde düzenleyici resmi kurum olarak görev alan veri koruma otoriteleri tarafından dikkate alınmaktadır. Ancak 25 Mayıs 2018 tarihi itibarı ile Avrupa Birliği Genel Veri Koruma Tüzüğü yürürlüğe girmiş ve Article 29 Working Party yerini Avrupa Veri Koruma Kurumu'na (European Data Protection Board) bırakmıştır.

³ Article 29 Working Party, “Opinion 4/2007 on the Concept of Personal Data”, WP 136, Görüş, 20 Haziran 2007, s. 6.

⁴ a.e.

⁵ Türksel Kaya Bensghir, **Bilgi Teknolojileri ve Örgütsel Değişim**, 1. Baskı, Yayın No: 274, Ankara, TODAİE, Haziran 1996, s.14; Anthony Liew, “Understanding Data, Information, Knowledge and Their Inter-Relationships”, **Journal of Knowledge Management Practice**, Cilt 8, Sayı 2, Haziran 2007, s. 5.

enformasyon ve bilgi arasında, birikim ve algılama yolu ile dönüşüme dayalı bir ilişki olduğu ifade edilmektedir. Veriyi, bilgi işleme sürecinin temel hammaddesi olarak, çeşitli işaretler, harfler, semboller yahut rakamlar ile temsil edilen; ham, işlenmeye hazır, işlenmemiş gerçekler ya da izlenimler olarak tanımlayan yazarlar⁶, enformasyonu ise verilerin, karar alma sürecine destek sunacak şekilde anlamlı bir biçime getirilmek üzere, analiz edilerek işlenmesiyle ulaşılan sonuçlar olarak kabul etmektedirler. Bilgi kavramı ise verilerin çeşitli analiz, sınıflandırma ve gruplama işlemlerinden geçirilerek, ileride özel bir amaç ile kullanmaya yönelik olarak kullanılmaya hazır hale getirilmiş enformasyonu tanımlamak için kullanılmaktadır. Bir başka deyişle, bilgi, *“anlamlı bir biçime sokularak, kullanıcıya güncel ve olası kararların alınmasında yardımcı olan veri”* şeklinde tanımlanmaktadır⁷.

Terimsel anlamda farklılıkların kabulü ile birlikte bu farklılıkların kişisel veri koruma hukukuna, bireylere ilişkin koruma alanını daraltacak şekilde yansıtılması, yasal düzenlemeler bakımından istenmeyen sonuçların ortaya çıkmasına sebep olabilecektir⁸. Bu nedenle söz konusu terimsel farklılıkların kişisel verilerin korunmasına ilişkin bu çalışma kapsamında göz ardı edileceğinin belirtilmesi gerekmektedir.

Kişisel verilerin korunmasına ilişkin düzenleyici metinlerde yer alan kişisel veri tanımı uyarınca içeriğinden bağımsız olarak, bir kişiye ilişkin her türlü veri kişisel veri niteliği taşımaktadır. “Her türlü veri” ifadesi kanun koyucular tarafından bilerek ve kişisel veri kapsamının geniş yorumlanmasına olanak sağlayacak şekilde kasıtlı olarak tercih edilmektedir. Bir verinin kişisel veri kapsamında değerlendirilip değerlendirilmeyeceğine ilişkin tartışmada söz konusu verinin öznel ya da nesnel

⁶ Adem Ögüt, **Bilgi Çağında Yönetim**, Ankara, Nobel Yayın Dağıtım, 2001, s. 11.

⁷ Faruk Çubukçu, **Bilgisayar Terimleri Sözlüğü**, Ankara, V Yayınları, 1987, s. 24; *“Her iki tanım birlikte irdelendiğinde anlaşılacağı üzere bilgi ve veri birbirinden farklı kavramlar olup, en basit anlatımla bilgi bizim algıladığımız temel ve her türlü malumat, bu malumatın bilgisayarın anlayıp işleyebileceği haline de veri denilmektedir. Suyun katı, sıvı ve gaz halinde olduğu gibi tabi ortamda sıvı halde bulunan suyun örneğin buhar makinesinde fonksiyon görebilmesi için gaz haline dönüştürülmesi gerekir. Veri ve bilginin özde her iki hali de aynı olup, aralarında şekil farklılığı bulunmaktadır.”* Levent Kurt, **Açıklamalı- İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara, Seçkin, 2005, s. 38.

⁸ Elif Küzeci, “Kişisel Verilerin Korunması”, **Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku (Genel Kamu Hukuku) Anabilim Dalı Doktora Tezi**, Ankara, 2010, s. 14.

olması herhangi bir önem arz etmemektedir. Bir kişinin kan grubu, TC kimlik numarası, ayakkabı numarası gibi ölçülebilen ya da belirli objektif olguları içeren nesnel bilgiler gibi; kişinin dürüst olması, ahlaklı olması gibi sübjektif değerlendirmeler de kişisel veri niteliği arz etmektedir. Örneğin; bir kişinin işini iyi yapıyor olması, amirince sübjektif olarak değerlendirilebilir ve kendisine bir performans değerlendirme notu atanabilir⁹. Söz konusu performans değerlendirme sonucu bir kişisel veri niteliğindedir. Benzer şekilde kişilerin alışkanlıkları ve bağımlılıklarına ilişkin veriler de kişisel veri niteliğindedir.

Herhangi bir verinin kişisel veri olarak değerlendirilip değerlendirilmeyeceğine ilişkin tartışmada verinin mahiyeti de bir ölçüt değildir. Buna göre bir kimseye ilişkin verinin, kişisel veri kapsamında değerlendirilmesinde söz konusu bilginin herkes tarafından bilinebilir ya da gizli olup olmaması bir başka deyişle, söz konusu verinin medeni hukuk anlamında kişinin, ortak yaşam alanına, dar anlamda özel yaşam alanına ya da sır alanına ait olup olmaması herhangi bir önem taşımamaktadır. Her ne kadar kişisel verilerin korunmasına ilişkin yaklaşımların kişinin özel hayatının ve aile yaşamının korunmasına ilişkin temel bir haktan kaynaklandığının kabulü gerekse de kişinin özel alanı dışında “genel yaşam alanı” olarak da adlandırılan ortak yaşam alanı dış çemberinde de birey korumasız bırakılmamalıdır¹⁰. Kişisel verilerin korunmasına ilişkin temel ilkelere bu alanda da uyulmalıdır. Kişinin kamuya açık yaşam alanında verilerinin toplanması, örneğin video ya da ses kaydının alınması halinde her ne kadar bu verilerin kişinin özel alanından toplanmadığı ileri sürülebilecek olsa da bu verilerin de kişisel veri olarak kabul edilmesi gerekmektedir¹¹.

Bununla beraber verinin gerçeği yansıtıp yansıtmaması da kişisel veri niteliği bakımından önem teşkil etmemektedir. Bu durumun bir yansıması olarak kişisel verilerin korunmasına ilişkin pek çok düzenlemede bireye kendisi hakkında işlenen

⁹ Article 29 Working Party, **a.g.e.**, s. 6.

¹⁰ Küzeci, **a.g.e.**, s. 80.

¹¹ Avrupa Adalet Divanı’nın evinin girişine kamera koyan kişinin kamerayla elde ettiği görüntüler bakımından kamera açısının kamuya açık alana taşması gerekçesiyle tamamen kişisel ya da aile içi kullanımla sınırlı olma istisnası kapsamında değerlendirilemeyeceğine ilişkin açıklamalar için bkz. Mesut Serdar Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu**, 1. Baskı, İstanbul, On İki Levha Yayıncılık, Ocak 2018, s. 26; Avrupa Adalet Divanı, Rynes davası, C-212/13, 11 Aralık 2014.

kişisel verileri düzeltme hakkı tanınmıştır. Bir kişi hakkında işlenen verinin yanlış ya da hatalı olması, güncel olmaması verinin kişisel veri olma niteliğini etkilememektedir¹². Veri sorumlusunun işlediği verileri güncel ve doğruyu yansıtacak şekilde işleme yükümlülüğü bulunmaktadır. Bu yükümlülük hatalı, güncel olmayan ya da yanlış verilerin kişisel veri niteliğini bertaraf etmemekte tam aksine kapsamı doğrulamaktadır. Örneğin; bir futbolcunun sakatlanmış olduğuna ilişkin yapılan asılsız haberin transfer sürecini etkileme ihtimali bulunmaktadır. Benzer şekilde kişilerin özel hayatlarına ilişkin yapılan haberler gerçeği yansıtmıyor olsalar dahi bir kişi ile eşleştirilebilir olmaları sebebi ile kişisel veri niteliği taşımaktadır.

Bir bilginin kişisel veri olup olmadığına ilişkin değerlendirme, o bilginin biçiminden ve saklandığı ortamdan bağımsız olarak yapılmalıdır. Nitekim aranan diğer şartları taşıdığı sürece, bir verinin niteliği itibarıyla alfabetik, sayısal, çizgisel, görsel veya işitsel olması ile kâğıt üzerinde veya bilgisayar ortamında saklanması, o verinin kişisel veri olma özelliğini değiştirmeyecektir¹³. Buna göre, hem Avrupa Birliği kişisel verilerin korunması mevzuatı hem de Türk veri koruma hukuku kapsamında, ses ve görüntü verilerinin de kişisel veri olarak kabul edilmesi gerektiği özel olarak belirtilmiştir¹⁴. Avrupa Birliği Veri Koruma Yönergesi'nde hem giriş bölümünde hem de 33. maddede Avrupa Birliği veri koruma rejiminin, gelişen teknolojinin gerisinde kalmasını engellemek amacıyla ses ve görüntü verilerine özel olarak atıf yapılarak, bu tür verilerin de Yönerge kapsamında ele alınması gerektiği ifade edilmiştir. İlgili hükümde Avrupa Komisyonu'na, özellikle gerçek kişilerin ses ve görüntülerine ilişkin veriler bakımından Avrupa Birliği Veri Koruma Yönergesi'nin uygulama alanının incelenmesi ve bilgi teknolojilerinin gelişimini dikkate alarak gerekli göreceği uygun önerilerin sunulması yükümlülüğü getirilmiştir. Bu hükmün bir yansıması olarak, birçok ülkenin veri koruma yasasında da ses ve görüntü verilerinin kişisel veri niteliği taşıdığına ilişkin hüküm açıkça yer almaktadır. Örneğin; Portekiz ve Lüksemburg veri

¹² Article 29 Working Party, **a.g.e.**, s. 6.

¹³ Article 29 Working Party, **a.g.e.**, s. 7.

¹⁴ “İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, *görüntü ve ses kayıtları*, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilmek özellikleri nedeniyle kişisel verilerdir.” Türkiye Büyük Millet Meclisi, 26. Yasama Dönemi, 1. Yasama Yılı 117 Sıra sayılı “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s.7, (Çevrimiçi) <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>, 22 Mart 2018.

koruma yasalarında “bütün bilgiler” ifadesinin, bilgilerin tutulduğu ortamdan bağımsız olarak, ses ve görüntü verilerini de kapsar şekilde, her türlü bilgiyi ifade ettiği açık olarak belirtilmektedir¹⁵. Benzer şekilde, Fransız veri koruma yasasında da dijital biçimde saklanmaları ve kimliği belirlenebilir bir kimseye ilişkin olmaları şartıyla, ses ve görüntü verilerinin de kişisel veri niteliği taşıdıkları ifade edilmektedir¹⁶. Kişisel Verilerin Korunması Kanunu kapsamında ise bu konuda açık bir hüküm bulunmamasıyla birlikte, tanımlar başlıklı 3. madde gerekçesinde, kişiyi belirlenebilir kılma özellikleri nedeniyle, görüntü ve ses kayıtlarının da kişisel veri olarak kabul edilebileceği belirtilmektedir.

Bilginin kişisel veri olarak kabul edilmesinin yanı sıra, veri korumasına ilişkin düzenlemeler kapsamında korunabilmesi için ayrıca söz konusu kişisel veri niteliğindeki bilgilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi gerekmektedir¹⁷.

1.1.1.2. Bilginin Kişiyeye İlişkin Olması

Kişisel veri kavramının bir diğer unsuru kişisel veri olarak kabul edilecek bilginin kimliği belirli veya belirlenebilir bir kişiye “ilişkin” olmasıdır. Somut bir verinin, tek başına bağlamsız olarak elde edilmiş olması kişisel verilerin korunması bakımından sahipsizlik gerekçesi ile koruma kapsamı dışında bırakılmasına neden olmaktadır. Gerçek bir kişi ile ilişkilendirilemeyen veriler anonim veri olarak

¹⁵ Douwe Korff, “EC Study on Implementation of Data Protection Directive: Comparative Summary of National laws”, **Human Rights Centre**, University of Essex, Cambridge, United Kingdom, Eylül 2002, s. 14, (Çevrimiçi) <http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE> , 19 Nisan 2018.

¹⁶ Ses ve görüntü verilerine ilişkin olarak Avusturya, Belçika, Danimarka, Finlandiya, Fransa, Almanya, Yunanistan, İrlanda, İtalya, Lüksemburg, Hollanda, Portekiz, İspanya, İsveç ve Birleşik Krallık mevzuat ve uygulama hakkında bilgi için bkz. British Institute of International & Comparative Law, “The Implementation of Directive 95/46/EC to the Processing of Sound and Image Data”, Rapor, 16 Mayıs 2003”, (Çevrimiçi) http://ec.europa.eu/justice/data-protection/document/studies/files/lawreport/consultation/biiclstudy-soundimage_en.pdf, 12 Ekim 2016.

¹⁷ Kişisel Verilerin Korunması Kanunu m. 2; 95/46 sayılı Avrupa Birliği Veri Koruma Yönergesi m. 3; Avrupa Birliği Genel Veri Koruma Tüzüğü m. 2; Konuya ilişkin detaylı bilgi 2. ve 3. bölümünde verilecektir.

nitelendirilmektedirler. Anonim veriler hem Avrupa Birliği mevzuatı hem de Kişisel Verilerin Korunması Kanunu tarafından kapsam dışı bırakılmaktadır¹⁸. Örneğin; tek başına “30 yaşında” verisi herhangi bir şey ifade etmezken, “durakta bekleyen 30 yaşındaki kişi” gibi bağlamı belirtilen ve bir kişi ile ilişkilendirilmesine imkân bulunan veriler kişisel veri olarak değerlendirilebilmektedir. Verinin bulunduğu bağlam ile birlikte bir kişi ile ilişkilendirilebiliyor olması önem arz etmektedir. Article 29 Working Party tarafından kişisel veri kavramına dair yayımlanan görüşte¹⁹ örnek olarak bir bölgedeki gayrimenkul fiyatlarının tek başına bir kişisel veri olarak değerlendirilemeyeceği, ancak bölgede yaşayan insanların tespit edilmesi ile birlikte o insanların yıllık ne kadar vergi ödediklerine ilişkin bir veriye ulaştırabileceği belirtilmiştir. Bu nedenle bir eşya, işlem veya olay hakkındaki bir bilginin de söz konusu bilginin kullanım amacı veya kullanımının doğuracağı sonuçlar itibarıyla dolaylı şekilde bir kimseye “ilişkin” olması ile kişisel veri niteliği arz etmesi mümkün olabilecektir.

Başka bir örnekle açıklamak gerekirse, bir süpermarketteki günlük meyve sebze satışlarına ilişkin bilgilerin sadece sipariş girişi ve ciro kontrol amaçlı takip ediliyor olması halinde herhangi bir kişisel veri ihtiva etmezken; bu verilerin manav reyonu sorumlusunun iş performans değerlendirilmesi amacı ile kullanılıyor ya da müşteri alım alışkanlıklarına ilişkin başka veriler ile eşleştirilerek anonim sayılamayacak detayda incelenebiliyor olması halinde söz konusu veriler artık bir kişi ile ilişkilendirilebileceği için kişisel veri niteliğinde kabul edilmektedir. Herhangi bir bilginin, içerik itibarıyla belli bir kişiye ilişkin olması, her türlü amaç ve sonuçtan bağımsız olarak, o bilginin söz konusu kişi “hakkında” olmasını ifade etmektedir.

Bilginin kişiye ilişkin olmasına dair bir başka görüş ise, “ilişkin” kavramının yöneldiği alan meselesine yoğunlaşmaktadır. Bir verinin, hangi halde kimliği belirli veya belirlenebilir bir kimseye ilişkin kabul edileceğine dair tartışma, Avrupa Birliği üye

¹⁸ Kişisel Verilerin Korunması Kanunu genel gerekçesinde de belirtilmiş olduğu üzere gelişen teknolojilerle birlikte anonim veri bir başka deyişle geri dönüştürülemez verilerden bahsetmek güçleşmektedir. Giderek artan sayılarda büyük veri kümelerinin ortaya çıkması ile birlikte herhangi bir “anonimleştirilmiş” veri kümesi arasında bir kişiye ilişkin veriyi tespit etme olasılığı artmaktadır, çünkü başka veri kümeleri ile çaprazlanarak kullanılma olasılığı artmaktadır.

¹⁹ Article 29 Working Party, **a.g.e.**, s. 9.

devletleri tarafından farklı şekilde değerlendirilmektedir. “İlişkin” olmanın ön koşulu olarak bazı ülke hukukları belli bir kimsenin belirlenebilir kılınmasını; bazıları ise, belli bir kimsenin menfaatlerinin etkilenmesini aramaktadır. Bir diğer grup ülkede ise, bir bilginin belli bir kimseye ilişkin olması, söz konusu bilgi vasıtasıyla hem o kişinin kimliğinin belirlenebilmesi hem de menfaatlerinin etkilenmesi birlikte aranmaktadır²⁰. Ancak bu görüşte ilgilinin menfaatinin etkilenip etkilenmediğine ilişkin değerlendirmenin nasıl yapılması gerektiğini tespit edebilmek güçtür. Nitekim ilişkinin kurulmasının yeterli olmayacağı kabulü ile bir menfaat etkilenmesinin beklenilmesi halinde, menfaatin etkilendiğine ilişkin ispat yükü ilgili kişiye geçeceği için bu görüş bireyi koruyan ilkelerle bağdaşmamaktadır. Zira kişisel verilerin korunması hukuku çerçevesinde temel amaç veri sorumlusu karşısında bireyi korumaktır.

1.1.1.3. Kimliği Belirli veya Belirlenebilir Bir Kişi

Kişisel veri olarak kabul edilen bilginin, kimliği belirli veya belirlenebilir bir kişiye ilişkin olması gerektiğinden, kişisel veri kavramının üçüncü ve son unsuru, kimliği belirli veya belirlenebilir bir kişinin²¹ bulunmasıdır.

Medeni Hukukta kişi, hak ehliyetine sahip varlıklara denmektedir²². Kişi kavramı özü itibarıyla hukuk mantığının bir ürünü olup hukuki bir kavramdır. Çünkü hangi varlıkların haklara ve borçlara sahip olabileceğini hukuk düzeni belirlemek zorunda kalmıştır. Bir varlığın kişi olarak nitelendirilmesi, hukuk düzeninin söz konusu varlığı kişi olarak kabul etmesine bağlıdır. Bu sebeple, insanların yanında toplum hayatının gereği olarak hukuk düzeni tarafından öngörülen koşulları yerine getiren insan

²⁰ Karen McCullagh, “Protecting ‘privacy’ through control of ‘personal’ data collection: a flawed approach”, **International Review of Law, Computers & Technology**, Cilt 23, Sayı 1-2, Mart-Temmuz 2009, par. 95.

²¹ Kişisel Verilerin Korunması Kanunu kapsamında kişisel verisi işlenen gerçek kişi “ilgili kişi” olarak; Avrupa Birliği Veri Koruma Yönergesi kapsamında ise “data subject” (“veri konusu”, “veri sahibi”) olarak isimlendirilmektedir.

²² Mustafa Dural, Tufan Ögüz, **Türk Özel Hukuku: Kişiler Hukuku**, İstanbul, Filiz Kitabevi, 2017, Cilt 2, s. 5; Kemal Oğuzman, Özer Seliçi, Saibe Oktay Özdemir, **Kişiler Hukuku (Gerçek ve Tüzel Kişiler)**, Gözden Geçirilmiş ve Yenilenmiş 16. Bası, Filiz Kitabevi, İstanbul, 2016, s. 2; Aydın Zevkliler, M. Beşir Acabey, K. Emre Gökyayla, **Medeni Hukuk: Giriş ve Başlangıç Hükümleri Kişiler hukuku Aile hukuku**, Gözden Geçirilmiş ve Genişletilmiş 6. Baskı, Ankara, Seçkin Yayınevi, 1999, s. 207.

toplulukları ve mal toplulukları da kişi olarak kabul edilmektedir²³. Bir başka deyişle kişi kavramı içinde hem gerçek kişiler, bireyler hem de tüzel kişiler yer almaktadır.

Kişi kavramından farklı olarak kişilik ise, kişi ile birlikte hukukun korumaya değer bulduğu, hukuki ve manevi nitelikteki kavramların tümünü kapsamaktadır²⁴. Çeşitli yazarlar²⁵ kişiliği, bireyin var olması nedeni ile sahip olduğu hak ve fiil ehliyeti ile hayatı, vücut tamlığı, şerefi, haysiyeti, sırları, adı gibi üzerindeki hakların tümü olarak tanımlamaktadır. Diğer bir deyişle kişilik kavramı, kişi kavramından daha geniş olup, hak ve fiil ehliyetlerini, kişisel durumları ve kişilik haklarını da içermektedir. Türk Medeni Kanunu'nda kişiliğin, çocuğun sağ olarak tamamıyla doğduğu anda başlayacağı, hak ehliyetini ise yine sağ doğmak koşuluyla, ana rahmine düştüğü andan itibaren kazanılacağı ifade edilmektedir (m. 28).

Kişisel durumlar, bir kişiyi diğerlerinden ayırmaya yarayan ve hukuk düzeninin kendilerine birtakım sonuçlar bağladığı niteliklerdir. Örneğin; bir kimsenin evli ya da bekâr olması, ergin veya kısıtlı olması kişisel durumlarla ilgilidir. Ancak kişilik hakkı, kişinin maddi, manevi ve ekonomik bütünlüğü ve varlıkları üzerinde sahip bulunduğu mutlak haktır. Örneğin; bir kimsenin, ismi, resmi, sağlığı, vücut bütünlüğü, onuru, şerefi üzerindeki hakları kişilik hakları olarak nitelendirilmektedir.

Kişisel verinin kişiliğin bir parçası olarak yorumlanması gerektiği kabul edilmelidir. Ancak konu itibari ile kişisel veri unsurlarından olan “kişi” kavramının yeri ve kapsamına ilişkin tartışmalar bulunmaktadır. Kişisel verileri korunacak kişi kavramının sadece gerçek kişileri mi yoksa gerçek kişiler ile birlikte tüzel kişileri de mi barındırdığı tartışılmaktadır. Baskın görüş kişisel verilerin korunmasına ilişkin düzenlemeler kapsamında koruma alanının gerçek kişiler ile sınırlandırılması yönünde

²³ Dural, Ögüz, **a.g.e.**, s. 5.

²⁴ Dural, Ögüz, **a.g.e.**, s. 6.

²⁵ Kemal Oğuzman, Özer Seliçi, Saibe Oktay Özdemir, **a.g.e.**, s. 165; Aydın Zevkliler, M. Beşir Acabey, K. Emre Gökyayla, **a.g.e.**, s. 211; Mustafa Dural, Suat Sarı, **Türk Özel Hukuku: Temel Kavramlar ve Medeni Kanunun Başlangıç Hükümleri**, Cilt 1, 10. Baskı, İstanbul, Filiz Kitabevi, 2015, s. 162; Ferit H. Saymen, **Türk Medeni Hukuku: Şahsın Hukuku**, Cilt 2, Yenilenmiş 2. Baskı, İstanbul, Hak Kitabevi, 1960, s. 14-15; Hıfzı Veldet Velidedeoğlu, **Türk Medeni Hukuku: Şahsın Hukuku**, İstanbul Üniversitesi Neşriyatından Sayı 357, Hukuk Fakültesi, Cilt 1, Sayı 81, 3. Baskı, İstanbul, 1963, s. 154, 155.

olsa da bu konuda aksi görüşler Avrupa Birliği üyesi devletler arasında bulunmaktadır. Avrupa Birliği üye ülkelerinden Avusturya, Danimarka, İtalya ve Lüksemburg ile birlik üyesi olmayan İzlanda, Norveç ve İsviçre’de veri koruma yasaları tüzel kişileri de korumaktadır²⁶. 2008 yılında Türkiye Cumhuriyeti Başbakanlığı tarafından Türkiye Büyük Millet Meclis’ine iletilen Kişisel Verilerin Korunması Kanunu Tasarısı’nda “tüzel kişilere ilişkin bütün bilgiler”in de kişisel veri kapsamında değerlendirileceği açıkça belirtilmiştir. Ancak daha sonra iletilen tasarı metinlerinde ve kanunlaşan düzenlemede²⁷ tüzel kişiler kapsam dışında bırakılmıştır. Öğretide, özel hayatın gerçek kişilere ilişkin bir kavram olması ve şirketler bakımından şeffaflık ilkesinin geçerli olması nedeniyle tüzel kişilere ilişkin bilgilerin kişisel veri olarak değil, yalnızca ticari sır olarak kabul edilmesi gerektiği belirtilmektedir²⁸. Belçika, Finlandiya, Fransa, Almanya, Yunanistan, İrlanda, Hollanda, Portekiz, İspanya, İsveç ve Birleşik Krallık’ta yer alan kişisel veri koruma düzenlemelerine göre yalnızca gerçek kişilere ilişkin veriler kişisel veri kabul edilmektedir.

Uluslararası düzenlemeler açısından bakıldığında ise Avrupa İnsan Hakları Sözleşmesi’nde açık bir hüküm bulunmamaktadır. Ancak Avrupa İnsan Hakları Mahkemesi tarafından kişisel verilerin korunmasını isteme hakkının incelendiği olaylarda ve içtihatlarda, konunun Avrupa İnsan Hakları Sözleşmesi’nin 8. maddesi çerçevesinde değerlendirildiği görülmektedir²⁹. Avrupa İnsan Hakları Sözleşmesi’nin 8. maddesinde de Anayasa’nın 20. maddesinde olduğu gibi "herkes" kavramı kullanılmaktadır. Ancak Avrupa İnsan Hakları Mahkemesi kararlarında da belirtildiği üzere Avrupa İnsan Hakları Sözleşmesi’nin 8. maddesinde yer alan temel amaç "bireyi" korumaktır. Avrupa İnsan Hakları Sözleşmesi’nin 8. maddesi kapsamında korunan hakkın bireysel bir nitelik bulundurması sebebi ile özne olarak tercih edilen "herkes" terimi ile yaş, temyiz kudreti, vatandaşlık veya cinsiyet özelinde herhangi bir istisna olmaksızın her bir bireyin bu haktan yararlanabilmesi amaçlanmaktadır. Buna

²⁶ Article 29 Working Party, **a.g.e.**, s. 24.

²⁷ Kişisel Verileri Koruma Kanunu madde 3’te ilgili kişi, kişisel verisi işlenen gerçek kişi olarak tanımlanmıştır.

²⁸ Durmuş Tezcan, “Bilgisayar Karşısında Özel Hayatın Korunması”, **Anayasa Yargısı**, Sayı 8, (Anayasa Mahkemesi’nin 29. Kuruluş Yıldönümü Sempozyumu), Ankara, 25 - 27 Nisan 1991, s. 389.

²⁹ Avrupa İnsan Hakları Sözleşmesi’ne ilişkin detaylı açıklamalara aşağıda yer verilecektir, bkz. “1.3.2.3. Avrupa İnsan Hakları Sözleşmesi”.

karşılık bu hakkın dört alt kategorisinden sadece "konuta saygı hakkının" öznesinin hem gerçek hem de tüzel kişiler olabileceğinin kabulü gerekmektedir. Ancak kişisel verilerin korunması hakkının bağlantılı kabul edildiği "özel yaşama saygı hakkı", "aile yaşamına saygı hakkı" ve "haberleşmeye saygı hakkı" kapsamında ise doğası gereği ancak gerçek kişilerin yararlanabileceği Avrupa İnsan Hakları Mahkemesi içtihatlarında belirtilmektedir³⁰. Kişisel veriler, "özel yaşama saygı hakkı" kapsamında korunan hukuki menfaatler arasında bulunan "bireyin mahremiyetinin korunması hakkı" kapsamında daha geniş bir alanda korunmaktadır. Kamu tüzel kişileri ile özel hukuk tüzel kişilerini kapsayacak şekilde geçen tüzel kişilerin gerek unvanları gerek iletişim bilgileri bakımından "mahremiyet hakkı" söz konusu olamayacağı gibi kuruluşlarının tescil ve ilana bağlı olması ve aleniyet ilkesi sebebi ile kamuya açık olmaları gerekmektedir³¹.

Avrupa Birliği Veri Koruma Yönergesi'nin 2 (a) maddesine göre kişisel veri "belirli ya da belirlenebilir gerçek kişi, veri öznesi" ile ilgili herhangi bir bilgi olarak tanımlanmaktadır. 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkındaki Avrupa Birliği Yönergesi'nde ise elektronik haberleşme sektörüne ilişkin olarak tüzel kişiler de koruma kapsamına dâhil edilmektedir. Ancak 2002/58/EC sayılı Yönerge'nin başlangıç kısmının 12. paragrafında söz konusu genişletmenin sadece elektronik haberleşme sektöründeki "abone" tanımı için olduğu ve üye devletlere Avrupa Birliği Veri Koruma Yönergesi'nin uygulama alanını tüzel kişileri de kapsayacak şekilde genişletme yükümlülüğü getirmediği özel olarak belirtilmektedir.

Bu doğrultuda 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkındaki Avrupa Yönergesi temel alınarak hazırlanan 5809 sayılı Elektronik Haberleşme Kanunu'nda yer alan abone kapsamına gerçek ve tüzel kişilerin dâhil edilmesi kullanıcıyı koruma ve kullanıcı kapsamını

³⁰ Gülay Arslan Öncü, "Özel Yaşama ve Aile Yaşamına Saygı Hakkı", **İnsan Hakları Avrupa Sözleşmesi ve Anayasa, Anayasa Mahkemesine Bireysel Başvuru Kapsamında Bir İnceleme**, ed. Sibel İnceoğlu, İstanbul, Beta, Haziran 2013, s. 301.

³¹ Anayasa Mahkemesi Kararı, Esas Sayısı: 2013/84, Karar Sayısı: 2014/183, Karar Tarihi: 4 Aralık 2014, Resmî Gazete Yayınlanma Tarihi: 13 Mart 2015, Sayısı: 29294.

geniş tutma gayesi ile yapılmıştır ve kişisel veri tanımını genişletmek amacı gütmemektedir.

Gerek Avrupa Birliği'ndeki düzenlemeler gerekse Kişisel Verilerin Korunması Kanunu kapsamında yer alan kişisel verinin tanımına göre, tüzel kişiye ait bir verinin herhangi bir gerçek kişiyi belirlemesi ya da belirlenebilir kılması halinde söz konusu gerçek kişiye ilişkin bir korumanın sağlanması gerekecektir. Ancak burada korunan menfaat yine tüzel kişiye değil, düzenlemenin temellendirdiği öncelik gereği belirlenen ya da belirlenebilecek gerçek kişiye ait olacaktır.

Belirtmek gerekir ki hâlihazırda tüzel kişiler ve tacirler için bir mahremiyetten çok aleniyet prensibi benimsenmektedir. Örneğin; tüzel kişilerden olan Ticaret şirketlerinin, 6102 sayılı Türk Ticaret Kanunu ve 1163 sayılı Kooperatifler Kanunu'na göre Ticaret Siciline tescil ile tüzel kişilik kazanacakları³², merkezleri ile ortaklarının adreslerinin ya da kurucularının Ticaret Sicili Gazetesinde ilân edileceği³³; ayrıca Türk Ticaret Kanununun 39. maddesine göre ticarî işletmeyle ilgili ticari mektuplarda ve ticari defterlere yapılan kayıtların dayandığı belgelerde sicil numarası, ticaret unvanı, işletmenin merkezi ile tescil edilen internet sitesinin adresinin gösterileceği belirtilmektedir. Türk Medenî Kanununun 102. maddesine göre sicile tescil ile tüzel kişilik kazanan vakıfların ilgili tüzük uyarınca yerleşim yeri ile birlikte Resmî Gazete'de ilân edilmesi ve derneklerin de diğer bilgileri ile birlikte ilgili mevzuat uyarınca sicile kaydedilmesi gerekmektedir. Bu doğrultuda şirketlerin adresleri, iletişim bilgileri gibi diğer bilgileri bakımından mahremiyet hakkından söz edilemeyeceği açıktır. Kamu tüzel kişilerinin ise ilgili mevzuat ile görev ve yetkilerinin belirlenmesi ve bu doğrultuda kamu görevlerini yürütecekleri adresleri gibi diğer gerekli bilgilerinin de kamuya açık olması gerekmektedir.

Tüzel kişiler nazarında korunması gereken kamuya açık olmayan ticari sır gibi diğer hususlar hâlihazırda bankacılık düzenlemelerinde yer alan hükümler, rekabet hükümleri ve şirketler arası gizlilik sözleşmeleri ile korunmaktadır. Bu doğrultuda

³² 14 Şubat 2011 tarih ve 27846 sayılı Resmî Gazete'de yayımlanan 6102 sayılı Türk Ticaret Kanunu m. 232, m. 355, m. 588.

³³ 10 Mayıs 1969 tarih ve 13195 sayılı Resmî Gazete'de yayımlanan Kooperatifler Kanunu m. 7.

tüzel kişiler nezdinde kişisel verilerin korunmasına ilişkin düzenlemeler çerçevesinde korunması gereken bir menfaat bulunmamaktadır.

Kişisel veri kavramının son unsuru, kimliği belirli veya belirlenebilir bir kişinin bulunması olduğundan, söz konusu kişi belirsiz bir kişi olmayıp, kimliği belirli veya belirlenebilir bir kişi olmalıdır. Bu çerçevede, bir kişinin kimliğinin belirli olması, o kişinin bir grup insan arasından ayırt edilebilmesini ifade ederken; kimliği belirlenebilir olmak ise, henüz ayırt edilememiş olmakla birlikte bu kişinin diğerlerinden ayırt edilmesinin mümkün olduğu anlamına gelmektedir. Örneğin; “İtalya’da belirli bir bölgede yaşayan Türk öğrenci” ifadesi tek başına doğrudan bir kişinin kimliğini açıklamıyor olsa da bölgede Türk öğrenci sayısının az olması ya da tek olması halinde bahsedilen kişi tespit edilebilir niteliktedir. Söz konusu veriler kişiye ilişkin ad, soyad, TC kimlik numarası gibi doğrudan kişiyi belirleyen nitelikte olmasa bile birbiriyle eşleştirilebilir ve bir kişiye yöneltilebilir veriler grubu olarak kabul edildiği zaman kişisel veri niteliğini taşıyacaktır. Kişisel Verilerin Korunması Kanunu gerekçesinde³⁴ de “Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilmek özellikleri nedeniyle kişisel verilerdir.” ifadesi yer almaktadır. Avrupa Adalet Divanı tarafından verilen 6 Kasım 2003 tarih ve C-101/01 sayılı Lindqvist kararında da benzer şekilde isim ya da isim olmasa bile telefon numaraları, çalışma koşulları veya ilgi alanlarının gerçek bir kişiye ulaştıracak biçimde bir internet sitesinde yer alıyor olması halinde bu verilerin kişisel veri niteliğinde kabul edileceği belirtilmektedir³⁵.

³⁴ Türkiye Büyük Millet Meclisi, 26. Yasama Dönemi, 1. Yasama Yılı 117 Sıra sayılı “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 7.

³⁵ Avrupa Adalet Divanı, Bodil Lindqvist davası, C-101/01, 6 Kasım 2003.

Kişisel veri, yalnızca belirli bir kişiyi doğrudan ya da dolaylı olarak tespit edilebilir kıldığı ölçüde söz konusu unsurlarını tamamlayacağı için bahsi geçen “tespit etme” faaliyetinin, kim tarafından ve hangi ölçüde gösterilecek uğraş sonucunda gerçekleştirilebileceği tartışma konusudur³⁶. Nitekim bu değerlendirme sonucunda elde edilen veriler kullanılarak kişinin kimliğinin tespit edilebileceği kabul ediliyorsa, söz konusu verilerin kişisel verilerin korunması kapsamında değerlendirilmesi gerekmektedir. Bu çerçevede, değerlendirme yapılırken dikkate alınması gereken çeşitli unsurlar bulunmaktadır. Avrupa Birliği Veri Koruma Yönergesi’nin başlangıç bölümünün 26. maddesinde belirtildiği üzere, kişisel verilerin korunması kapsamında bir kimsenin kimliğinin belirlenebilir olup olmadığını tespit etmeye çalışan kişinin, bu amaçla “kullanması makul olan tüm vasıtaları” dikkate alacağı kabul edilmelidir. Diğer bir deyişle, somut olayın tüm özellikleri değerlendirilmeli, kişinin kimliğinin tespitini sağlayabilecek tüm araç ve yöntemlere başvurulacağı varsayılmalıdır. Bu çerçevede, bir kimsenin kimliğinin belirlenebilmesi amacıyla kullanılabilecek resmi siciller gibi makul tüm vasıtalar göz önünde tutulmalıdır. Belirtilmelidir ki teknolojik gelişmeler, veri tabanları ve arama motorlarının kaydettiği veriler günümüzde veri gruplarının bir kişi ile eşleştirilmesini kolaylaştırmakta, bu sayede kişisel veri kapsamına giren veri sayısını gün geçtikçe artırmaktadır.

Alman Federal Mahkemesi tarafından IP³⁷ adreslerinin kişisel veri olup olmadığına ilişkin olarak ön karar için Avrupa Adalet Divanı’na iletilen sorular çerçevesinde Avrupa Adalet Divanı 2016 tarihli kararında³⁸ belirlenebilirlik unsuruna ilişkin olarak görüşünü açıklamıştır. Olayda Patrick Breyer, Almanya Federal Cumhuriyeti’nin pek çok kurumunun işlettikleri internet siteleri aracılığı ile bireylerin internet kullanımlarına ilişkin kayıtları ve IP adreslerini erişim sona erdikten sonra belirli bir süreyle saklamasına karşı dava açmıştır. Karar içermekte olduğu “erişim sağlayıcısından gerekli ek bilgileri sağlama olanağı bulunan hizmet sağlayıcısı bakımından IP adresleri kişisel veri olarak kabul edilebilir mi?” sorusu açısından önem

³⁶ Belirlenebilirlik unsuruna ilişkin olarak mutlak ve nisbi belirlenebilirlik tartışması için bkz. Çekin, **a.g.e.**, s. 35-36.

³⁷ IP adresleri, internet üzerinden iletişimi sağlamak için ağa bağlı bilgisayarlara atanan rakamlar serisidir.

³⁸ Avrupa Adalet Divanı, Breyer davası, C-582/14, Karar Tarihi 19 Ekim 2016.

taşımaktadır³⁹. Avrupa Adalet Divanı önüne gelen olayda, “makul imkânlar” kapsamını geniş yorumlayarak internet erişim sağlayıcıdan gerekli ek bilgilerin talep edilmesi halinde bir IP adresinin bir kişiyi belirlenebilir kılacağı görüşünü benimsemiştir⁴⁰. Kararda, kişinin belirlenebilir olması unsurunun kabulü için, ilgili kişiyi belirlenebilir kılan bütün verilerin, veri sorumlusunun sürekli olarak elinde bulunması gerekmediği belirtilmiştir⁴¹ ancak belirlenebilirlik ölçütünü somut olay bazında değerlendirilmiştir. Üçüncü kişilerden ek bilgilerin talep edilmesi ile elde edilecek verilerin IP adresi ile birleştirilmesi sonucunda bir kişinin belirlenebilir olup olmayacağını araştıran mahkeme, erişilebilir üçüncü kişilerin makul ihtimaller çerçevesinde değerlendirilmesi gerektiğine işaret etmiştir⁴². Somut olay bakımından Avrupa Adalet Divanı, Almanya Federal Cumhuriyeti’nin internet servis sağlayıcılardan elde edebileceği ek bilgiler ile birleştirilmesi halinde IP adreslerinin bir kişiyi belirlenebilir kılacağı savı⁴³ ile IP adreslerinin kişisel veri olarak ele alınması gerektiğine kanaat getirmiştir⁴⁴.

1.1.2. Genel Olarak Büyük Veri Kavramı

İnsanoğlunun bilgi ve biriktirme ihtiyacı doğrultusunda zaman içerisinde kütüphanelerdeki, devlet dairelerindeki yahut herhangi bir dokümantasyon ve arşiv sistemlerinde yer alan bilgi ve belgelerin, teknolojinin de yardımı ile yıllar içerisinde katlanarak büyüdüğü tespit edilmiştir. Büyük veri tanımına ilişkin ilk öngörünün Nikola Tesla’ya ait olduğunu söylemek yanlış olmayacaktır. Nikola Tesla, 1926 yılında vermiş olduğu bir röportajda⁴⁵ kablosuz erişimin mükemmel bir şekilde

³⁹ Avrupa Adalet Divanı, Breyer davası, par. 26.

⁴⁰ Mahkemenin IP adreslerinin kişisel veri olarak kabul ettiği önceki görüşü için bkz. Avrupa Adalet Divanı, Scarlet Extended davası, C-70/10, Karar Tarihi 14 Nisan 2011.

⁴¹ Avrupa Adalet Divanı, Breyer davası, par. 43.

⁴² Avrupa Adalet Divanı, Breyer davası, par. 76.

⁴³ Avrupa Adalet Divanı, Breyer davası, par. 47-49.

⁴⁴ IP adreslerinin kişisel veri sayılması hususunda ayrıntılı bilgi için bkz. Nafiye Yücedağ, “The Protection Of IP Addresses In Peer-To-Peer (P2P) Networks”, 13th International Conference on Internet, Law & Politics, **Managing Risk in the Digital Society**, Barselona, İspanya, 29 Haziran - 30 Eylül 2017, s. 342-357.

⁴⁵ Roportaj John B. Kennedy tarafından yapılmış olup, 30 Ocak 1926 tarihinde Colliers’de yayınlanmıştır. Twenty-First Century Books tarafından ise daha sonrasına tekrar yayınlanmıştır. John B. Kennedy, “An interview with Nikola Tesla”, **Twenty-First Century Books**, (Çevrimiçi) <http://www.tfcbooks.com/tesla/1926-01-30.htm>, 04 Nisan 2018.

işlemesi ile birlikte dünyanın devasa bir beyne dönüşeceğini belirterek bugünkü modern akıllı telefonları tanımlamıştır. Nikola Tesla, insanlar arasında mesafelerden bağımsız olarak anında iletişim sağlanacağından, kilometrelerce uzaklıkta dahi bireylerin mükemmel bir şekilde -sanki yüz yüzeymişçesine- birbirini görüp duyabileceğinden ve bu teknolojinin basit, insanlar tarafından ceplerinde taşınabilecek bir halde olacağından bahsetmiştir.

Yıllar içerisinde katlanarak artan veri büyüklüğünü tanımlamak ve anlamlandırmak için yapılan çeşitli çalışmalar, ortaya atılan tanımlamalar ve kullanımlar içerisinde 2001 yılında Meta Group adına şirketin analisti Douglas Laney tarafından hazırlanan yayında yer alan ve büyük veri bileşenlerini, hız, çeşitlilik ve büyüklük olmak üzere üç boyutlu olarak yani “3V” olarak tanımlayan çalışma dikkat çekici olmuştur⁴⁶. Daha sonrasında ise büyük veri kavramı, Amerikalı medya şirketi O’Reilly Media pazarlama yöneticilerinden Roger Mougals tarafından internet 2.0’ın⁴⁷ yaratılmasını takiben, 2005 yılında⁴⁸ geleneksel iş zekâsı araçlarını kullanarak yönetmenin ve işlemenin neredeyse imkânsız olduğu büyük veri kümelerini açıklamak için kullanılmıştır. 2012 yılında ise Douglas Laney büyük veri tanımını, çok büyük hacim, çok büyük hız ve çok fazla çeşitlilik olarak geliştirmiştir⁴⁹.

⁴⁶ Douglas Laney, “3D Data Management: Controlling Data Volume, Velocity and Variety”, **Application Delivery Strategies**, 6 Şubat 2001, (Çevrimiçi) <https://blogs.gartner.com/douglas-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>, 08 Nisan 2018; Francis X. Diebold, “A Personal Perspective on the Origin(s) and Development of “Big Data”: The Phenomenon, the Term, and the Discipline”, Second Version, **PIER Working Paper**, Sayı 13-003, 26 Kasım 2012, s. 5

⁴⁷ İnternet 2.0, O’Reilly Media tarafından 2004’te kullanılmaya başlayan bir sözcük olup ve ikinci nesil internet hizmetleri olan internet kullanıcılarının ortaklaşa ve paylaşarak içerik yarattığı platformların yer aldığı internet görünümünü tanımlamak için kullanılmaktadır.

⁴⁸ Mark van Rijmenam, “A Short History Of Big Data”, 07 Ocak 2016, (Çevrimiçi) <https://datafloq.com/read/big-data-history/239>, 08 Nisan 2018.

⁴⁹ Douglas Laney, Mark A. Bayer, "The Importance of 'Big Data': A Definition", **Gartner**, 21 Haziran 2012; belirtmek gerekir ki yıllar içerisinde bu tanıma bazı ek unsurlar da eklenmiştir. 2014 yılında, dünyanın önde gelen şirketlerinden birinin sahibi olan ve çeşitli yayınlar (Forbes, HuffPost ve LinkedIn Pulse) için veri ve analitik konusunda çalışmalar yürüten yazar Bernard Marr, hacim, hız ve çeşitliliğe ek olarak doğruluk ve değer unsurlarını tanıma eklemiştir. Yazar, 2016 yılında ise, müşteri satın alma davranışlarını takip etmek ve reklamları yeniden hedeflemek için çalışan birçok ticari büyük veri uygulaması tarafından işlenen kişisel verilerle ilgili artan endişeler nedeniyle altıncı bir unsur olan “**vulnerability**”-“savunmasızlık” kavramını da tanıma eklemiştir (bkz. Daniar Supriyadi, “Personal and

Gerek akademik dünyada gerekse endüstride üzerinde uzlaşmış net bir büyük veri tanımı bulmak pek mümkün gözükmemekle⁵⁰ birlikte çeşitli kaynaklarda büyük veri; genel olarak bilgi, teknoloji, yöntem ve etki kavramları ile ilişkilendirilmektedir. Ayrıca büyük veriyi tanımlayabilmek için kullanılan *hız*, verinin gerçek zamanlı olması; *çeşitlilik*, verinin farklı kaynaklardan elde edilebilir olması; *hacim*, verinin büyük veri kümelerinden oluşması ve *değer* ise kullanımının bir fayda yaratması şeklinde açıklanmaktadır⁵¹.

Gerçekten de gündelik hayatta her gün kullandığımız cep telefonları, akıllı saatler, kredi kartları, üyelikler, sadakat programları, bilgisayarlar, televizyonlar, oyun konsolları ve diğer birçok elektronik cihazlar ve birbirine bağlı sistemler sürekli olarak veri toplamakta ve bu verileri paylaşmaktadır. Böylelikle toplam işlenen veri sayısı tahmin edilemez boyutlara ulaşabilmektedir. Büyük verinin kaynağını sadece internet olarak ifade etmek de doğru değildir. Günümüzde Radyo Frekansı ile Tanımlama (RFID) ve sensör teknolojilerinin gelişmesi, kullanımın artması ile birlikte gündelik hayatın her alanında çeşitli kaynaklardan verilerin toplanması olanaklı hale gelmiştir.

Kirk Bourne tarafından yapılan tespitte insanlık tarihinin başlangıcından 2003 yılına kadar kayıt altına alınmış bütün veri toplamının, 2011 yılının başlangıcında sadece her iki gün içinde, 2013 yılında ise sadece her 10 dakikada üretildiği ifade edilmektedir⁵².

Belirtilen artışın en temel sebebi günümüzde artık her cihazın bir veri üretebiliyor ve hatta geleneksel yöntemlerden farklı olarak çok daha nitelikli veri üretebiliyor olmasıdır. Aralarında artan rekabet sonucunda şirketler, büyük ve yapısal olmayan veri bloklarını analiz ederek sonuçlarının raporlanması ve kullanılabilir hale getirilmesi üzerine çalışmaya başlamışlardır. Büyük ölçekli ve yapısal olmayan verilerin analizi

Non-Personal Data in the Context of Big Data”, **Tilburg Institute for Law, Technology and Society**, Ocak 2017, s. 12-13).

⁵⁰ Andrea De Mauro, Marco Greco, Michele Grimaldi, “What is Big Data? A Consensual Definition and a Review of Key Research Topics”, 4th International Conference on Integrated Information, **AIP Proceedings**, 2015, (Çevrimiçi) <https://aip.scitation.org/doi/abs/10.1063/1.4907823> , 8 Nisan 2018.

⁵¹ Information Commissioner’s Office, “Big data, artificial intelligence, machine learning and data protection”, s. 6, 4 Eylül 2017, (Çevrimiçi) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>, 18 Nisan 2018.

⁵² Kirk Borne, “Big Data, Small World: Kirk Borne at TEDxGeorgeMasonU”, 6 Nisan 2013, (Çevrimiçi) <https://www.youtube.com/watch?v=Zr02fMBfuRA>, 18 Nisan 2018.

için geleneksel veri tabanları ve analiz yöntemleri elverişli olmadığı için yerine bu ölçekte verileri analiz edebilecek büyük veri teknolojileri geliştirilmiştir.

Article 29 Working Party tarafından hazırlanan bildiri uyarınca büyük veri, bazıları iyi tanımlanmış bazıları ise hala belirsiz ve yakın gelecekte geliştirilmesi beklenen çok sayıda veri işleme faaliyetini kapsayan geniş bir terimdir⁵³. Büyük veri teknolojileri akademik çalışmalar, sağlık, sosyal bilimler, ulaşım, ticari iş uygulamalarından suç ile mücadeleye kadar birçok alanda kullanılmaktadır. Sağlık alanında çeşitli tıbbi durumlar ve genetik özellikler arasında bağlantı kurularak bu veriler üzerinden yapılan çalışmalardan geçmişte mümkün olmayan tedavi imkânları geliştirilebilirken aynı zamanda benzer verilerden ilaç sektöründeki pazarlama alanında yahut tedarik zincirine ilişkin iyileştirmeler sağlanmasında ve tasarrufa gidilmesinde yararlanılabilmektedir. Anket şirketleri, müşterilerinin talep ettiği kullanıcılara sosyal medya aracılığı ile çok daha kolay ulaşarak çok daha hızlı ve isabetli sonuçları daha düşük maliyetlere sunabilmektedirler. Temelde büyük veri uygulamaları ile amaçlanan, yığın halinde ve anlamsız olarak bulunan yüksek hacimli veriden anlamlı sonuçlar çıkarmaktır.

1.1.2.1. Büyük Verinin Kaynakları

Büyük verinin diğer veri setlerinden ayrılan en önemli kısmı çok farklı kaynaklardan çok hızlı bir şekilde besleniyor olmasıdır. Temel olarak büyük verinin kaynaklarını **(i)** dolaşan veriler, **(ii)** sosyal medya uygulamaları üzerinden toplanan veriler ve **(iii)** kamuya açık veri tabanları olmak üzere üçe ayırarak ifade etmek mümkündür. Dolaşan veri⁵⁴ ile ifade edilmek istenen, anlık olarak operasyonlar sırasında elde edilen bir ağ ya da formlar üzerinden süreçler içerisinde akan veridir. Veri madenciliğinin⁵⁵ ilgi alanına giren bu

⁵³ Article 29 Working Party, “Statement on Statement of the WP 29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU”, WP 221, Bildiri, 16 Eylül 2014, s. 3.

⁵⁴ Data streaming olarak yabancı kaynaklarda yer alan bu terim dolaşan veri ya da veri akışı olarak isimlendirilmektedir. Anlık olarak geçen veriler ifade edilmek istenmiştir.

⁵⁵ Veri madenciliği veri tabanları içerisindeki değerli bilgileri keşfetmek anlamında kullanılmaktadır. Bilhassa otomatik karar mekanizmaları tarafından veri madenciliğinden yararlanılmaktadır. Konuya ilişkin olarak bkz. Liane Colonna, “Mo’ Data, Mo’ Problems? Personal Data Mining and the Challenge to the Data Minimization Principle”, **Big Data And Privacy Making Ends Meet**, Stanford Law School, The Center

akışlarda genel olarak bir sınıflandırma yolu ile yarar elde edilmektedir. Örneğin, anlık olarak bir internet sitesinin kullanımının konum bazlı olarak sınıflandırılması, bu sınıflandırmanın daraltılıp genişletilmesi veri madenciliği konusudur. Sosyal medya uygulamaları üzerinden ise genellikle pazarlama, satış ve destek hizmetlerinin geliştirilmesi amacı ile sosyal medya etkileşim verileri kullanılmaktadır. Kamuya açık veri tabanları ise genellikle istatistiki olarak bilgi paylaşımı yapan ve belirli bir grup verinin anlamlı bir sonucu olarak sunulmuş veri setleri olarak tanımlanmaktadır. Örneğin, Amerika Birleşik Devletleri yaklaşık 15 farklı kategoride derlediği birçok veri yığını kamuya açık tutmaktadır⁵⁶. Yine Amerika Birleşik Devletleri vatandaşlarının sağlık alanındaki verilerini nüfus, coğrafi ve eğitim tabanlı veri setleri üzerinden kamuya açıklanmaktadır⁵⁷. Benzer kamuya açık veri setleri Avrupa Birliği⁵⁸, Birleşik Krallık⁵⁹ ve Türkiye⁶⁰ tarafından da paylaşılmaktadır. Google⁶¹, Facebook⁶², Amazon, Wikipedia⁶³ gibi teknoloji şirketleri de kamuya açık veri tabanlarını yönetmektedirler⁶⁴.

for Internet And Society, (Çevrimiçi) <https://fpf.org/wp-content/uploads/Big-Data-and-Privacy-Paper-Collection.pdf>, 18 Nisan 2018, s. 20.

⁵⁶ Amerika Birleşik devletleri tarafından oluşturulmuş veri setlerine şu adresten erişilebilir: (Çevrimiçi) <https://www.data.gov/>, 18 Nisan 2018.

⁵⁷ Amerika Birleşik Devletleri vatandaşlarının sağlık alanındaki nüfus, coğrafi ve eğitim tabanlı veri setlerine şu adresten erişilebilir: (Çevrimiçi) <https://www.census.gov/data.html>, 18 Nisan 2018.

⁵⁸ Avrupa Birliği Tarafından oluşturulmuş 20 farklı kategori barındıran veri setlerine şu adresten erişilebilir: (Çevrimiçi) <http://data.europa.eu/euodp/en/home/>, 18 Nisan 2018.

⁵⁹ Birleşik Krallık tarafından oluşturulmuş 12 farklı kategori altında sunulan veri setlerine şu adresten erişilebilir: (Çevrimiçi) <https://data.gov.uk/>, 18 Nisan 2018. Diğer veri tabanlarından farklı olarak 1950 yılından itibaren basılan tüm Birleşik Krallık ulusal yayınların bibliyografyası da veri tabanında yer almaktadır.

⁶⁰ Türkiye İstatistik Kurumu tarafından 17 kategori altında istatistiki veri paylaşımına şu adresten erişilebilir: (Çevrimiçi) www.tuik.gov.tr, 18 Nisan 2018.

⁶¹ Google trends ile ilgili alanlarına ilişkin olarak bölgesel ve tarihsel daraltımlara elverişli sonuçlar elde edilebilmektedir, Google Books Ngrams ise çok fazla sayıda kitap üzerinden arama ve analiz faaliyetleri gerçekleştirilebilmektedir. Google Finance ise son 40 yılda dünya üzerindeki ekonomik hareketleri takip imkânı sunmaktadır.

⁶² Likebutton uygulaması ile ulusal ve uluslararası beğenilen popüler konulara erişim sağlanabilmektedir; herkese açık olarak verilerini paylaşmış ya da izinli olarak oluşturulmuş Facebook kullanıcılarının verilerine erişim sağlayan platforma şu adresten erişilebilir: (Çevrimiçi) <https://developers.facebook.com/docs/graph-api>, 18 Nisan 2018.

⁶³ Wikipedia'nın içerisindeki yapılandırılmış veya yapılandırılmamış çok fazla sayıda veriyi, uygun bir veri tabanı formatına dönüştüren ve kullanıma açan bir proje şu adresten erişilebilir: (Çevrimiçi) <http://wiki.dbpedia.org/>, 18 Nisan 2018.

⁶⁴ Türkiye'de açık veri kullanımına ilişkin olarak ayrıca bkz. Mehmet Bedii Kaya, "Büyük Verinin Hukuki Boyutları", **Büyük Veri ve Açık Veri Analitiği : Yöntemler Ve Uygulamalar**, ed: Prof. Dr. Şeref Sağıroğlu, Dr. Orhan Koç, Grafiker Yayınları, Ankara, 2017, s. 188.

1.1.2.2. Büyük Verinin Kapsamı

Yukarıdaki örneklerden de görülebileceği üzere büyük veri işleyebileceği her türlü veriyi hedefleyerek bünyesine katma amacı taşımaktadır. Bu bakımdan büyük verinin kapsamını öngörebilmek mümkün gözükmemektedir. Büyük veri setleri içerisinde istatistiki veriler, anonim veriler, şirket bilgileri, kamuya açık bilgiler, tüzel kişi bilgileri olabileceği gibi gerçek kişilere ilişkin kişisel verilerin yer alması da kaçınılmaz bir durum olarak gündeme gelmektedir. Büyük veri içerisinde yer alan bir veri, kaynaktan elde edilme anında kişisel veri niteliğinde olabilmektedir. Bununla birlikte söz konusu veri elde edilme anında anonim, istatistiksel yahut anlamsızken, başka bir veri ya da veri seti ile eşleştirilerek büyük veri uygulamaları ile işlendiğinde netice olarak bir kişiye ilişkin bir kişisel veri niteliğine kavuşabilir. Bu bakımdan büyük veri içerisinde yer alan verilerin tanımlanması ya da sonuçların değerlendirilmesi bakımından yukarıda açıklanan kişisel veri kavramı ve unsurları uyarınca bir değerlendirme yapılması gerekmektedir.

1.2. Kişisel Verilerin Korunması

1.2.1. Kişisel Verilerin Korunması Hukukunda Korunan Menfaat

Kişisel verilerin korunması hukuku kapsamında asıl korunan veriler değil, kişisel veri sahibi olan gerçek kişiler olduğunun belirtilmesi gerekmektedir⁶⁵. Kişisel verilerin korunması adına geliştirilmiş ilkeler ve yaklaşımlar ile ilgili kişilerin verilerinin işlenmesinden doğabilecek zararlardan korunması hedeflendiği belirtilmektedir⁶⁶. Bu bakımdan kişisel verilerin korunması kişilik hakkı olarak görülmektedir. Bu görüşü benimseyen Kıta Avrupası ekolünde “sosyal değer” merkezli bir yaklaşım hâkimdir⁶⁷. Bunun yanı sıra Anglo-Amerikan sistemine dâhil ülkelerde ise konu daha ziyade özel hayatın gizliliği ile sınırlandırılmakta ve kişisel verilerin korunmasına Kıta Avrupası’nın aksine ekonomik ve teknolojik olarak yaklaşılmaktadır. Terminolojik

⁶⁵ Küzeci, a.g.e., s. 15.

⁶⁶ a.y.

⁶⁷ a.e., s. 67

olarak da bu farklılıklar “bilgi toplumu” ve “veri ekonomisi” yaklaşımlarını beraberinde getirmektedir.

Amerika Birleşik Devletleri’nde bir değer olarak nitelendirilen verinin ekonomik faydalarından yararlanmak adına kişisel verilerin korunması daha düşük düzeyde iken Kıta Avrupası’nda daha muhafazakâr bir yaklaşım söz konusu olup, kişisel verilerin korunması hakkı bir kişilik hakkı olarak tanınmıştır. Bir başka deyişle kişisel verilerin korunması Avrupa Birliği’nde temel bir insan hakkı olarak kabul edilip kamu tarafından düzenlenirken, Amerika Birleşik Devletleri’nde kişisel verilerin korunmasına ilişkin korumalar şirketlerin kendi düzenlemelerine bırakılmıştır⁶⁸.

Doktrinde kişisel verilerin korunmasına ilişkin olarak ekonomik değer ve sosyal değer ayrımından yola çıkan farklı teoriler bulunmaktadır. Mülkiyet teorisi kapsamında kişisel verilerin mülkiyete konu olması gerektiği görüşünü savunan yazarlar, bireylerin kişisel verilerini sözleşme konusu ederek yarar sağlayabileceklerini, bir başka deyişle bireylerin kişisel verilerini satma ya da bedelsiz olarak açıklama özgürlüğüne sahip olması gerektiğini ifade etmektedir⁶⁹. Diğer bazı yazarlar ise, kişisel verilerin fikrî mülkiyet hakkı kapsamında korunabileceğini savunmaktadırlar. Bu yaklaşımda telif hakkı ile kişisel verilerin korunması hakkının koruma alanı benzetilerek kişisel verilerin fikri mülkiyet tekniğine benzer şekilde korunması gerektiği ifade edilmektedir⁷⁰.

Kıta Avrupası’nda ise kişisel verilerin korunmasının kişilik değerleri ile bir bütün olarak değerlendirilmesi gerektiğinden yola çıkılarak kişisel verilerin korunmasının temel bir insan hakkı olduğu görüşü ağır basmaktadır⁷¹. Nitekim özel hayatın gizliliğinden farklı olarak mahrem niteliği taşımayan, bir başka deyişle bir kişiye ilişkin gizli olmayan verilerin dahi kişisel verilerin korunması hukuku kapsamında korunması gerekmektedir. Bunun nedeni ise bu verilerin işlenmesi ile kişinin kendini

⁶⁸ Serpil Karlıdağ, “Ekonomi Politik Açıdan Kişisel Verilerin Korunması”, **Amme İdaresi Dergisi**, Cilt 46, Sayı 1, Mart 2013, s. 128.

⁶⁹ Lawrence Lessig, “Privacy as Property”, **Social Research**, Cilt 69, Sayı 1, The New School, 2002, s. 261.

⁷⁰ Küzeci, **a.g.e.**, s. 72.

⁷¹ **a.e.**, s. 74.

ifade etme, kendini geliştirme gibi haklarının zarar görebileceği, kişinin manipüle edilebileceği, ayrımcılığa uğrayabileceği endişesidir. Kişisel verilerin korunmasına ilişkin kişilik hakkı merkezli yaklaşımın bir başka endişesi ise kendini sürekli gözetim altında hisseden bireylerin ifade özgürlükleri, hareket ve irade serbestilerinin kısıtlanabileceği düşüncesidir⁷².

Bu doğrultuda gerek Kıta Avrupası'nda gerekse Türk hukukunda kanun koyucu kişisel verilerin korunmasını bir kişilik hakkı⁷³ olarak görerek menfaat dengesini kişisel veri sahibi olan bireyler lehine kurmuştur. Ancak, devlet birey arasındaki dikey ilişkide devletin menfaatlerinin ağır bastığı durumlar bakımından kişisel verilerin korunması hakkının sınırlandırılabilir⁷⁴. Özel hukuk ilişkileri bakımından ise kanun koyucunun kişisel verisi işlenen bireyin üstün tuttuğu menfaati karşısında veri sorumlularının özellikle meşru menfaat, gereklilik ya da zorunluluk gerekçeleri ile veri işleme taleplerinin nasıl dengeleneceği çatışan menfaatler sorununu gündeme getirmektedir.

1.2.2. Kişisel Verilerin Kişilik Hakkı Olarak Korunması

Kişisel verilerin korunmasına ilişkin aşırı korumacı bir yaklaşım olan kişilik hakkı yaklaşımı verinin yaratmış olduğu ekonomik değeri engelleyebileceği düşüncesi yukarıda bahsedilmiş olan eleştirilere konu olabilmektedir. Ancak gerek Kıta Avrupası'nda hâkim olan görüş gerekse Türk kanun koyucunun benimsediği yaklaşım uyarınca kişisel veriler başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini koruma prensibi kapsamında geliştirilmiş koruma yöntemleri bu tez kapsamında incelenerek büyük veri uygulamaları bakımından değerlendirilecektir.

Kişisel verilerin korunması alanında Alman Federal Anayasa Mahkemesi'nin 15 Aralık 1983 tarihli "Nüfus Sayım" kararı⁷⁵ önem taşımaktadır⁷⁶. Karara konu Nüfus

⁷² Çekin, **a.g.e.**, s. 13.

⁷³ Çekin, kişisel verilerin korunmasına ilişkin temel hakkın niteliği itibarı ile kişilik hakkının bir alt kategorisi olarak değerlendirdiğini Alman Federal Mahkemesinin Volkszählungsurteil kararına atıf yaparak vurgulamıştır. Kişisel Verilerin Korunmasının Temel Hak ve Özgürlükler (Anayasal) Boyutu hakkında detaylı bilgi için bkz. Çekin, **a.g.e.**, s. 13.

⁷⁴ Çekin, **a.g.e.**, s. 15-17.

⁷⁵ Kararın önemli bölümlerinin İngilizce tercümesi için bkz. (Çevrimiçi) <https://freiheitsfoo.de/census-act/> 9 Eylül 2018.

⁷⁶ Çekin, **a.g.e.**, s. 6.

Sayım Kanunu’nda Alman Hükümeti bireylerin kişisel, çalışma alanları ve mesleklerine ilişkin bilgiler ile yaşam koşullarına ilişkin bilgilerin bir anket çalışması ile nüfus sayımının yanı sıra toplanmasını öngörmüştür. Kararda Alman Anayasası’nda koruma altına alınan insan onuru ve kişiliğin serbestçe geliştirilmesi hakkı ile bağlantılı olarak kişisel verilerin korunması değerlendirilmiştir⁷⁷. Alman Federal Anayasa Mahkemesi kararında⁷⁸ bu iki hak arasından bireylerin kişisel verilerinin geleceğini tayin etme hakkını⁷⁹ türetmiştir. Kişinin resmi ve ismi üzerindeki hakkı, biyolojik ebeveynlerini bilme hakkı ve muhalif düşünce geliştirme hakkı kişinin kendini serbestçe geliştirebilmesine ilişkin hakkın görünümüleri olarak belirtilmektedir⁸⁰.

Kişisel verilerin korunma yollarını, genel koruma ve özel koruma olmak üzere ikiye ayırarak incelemek mümkündür. Genel koruma kişisel verilerin, kişilik hakkı, mahremiyet ve özel yaşam alanlarına ilişkin genel normlar çerçevesinde korunmasını amaçlamaktadır. Nitekim kişilik hakkı kişilikdeğerlerinin bütünü üzerinde geçerlidir. Bu nedenle kişilik hakkının bir parçası olan kişisel verileri koruyan bazı hükümleri, medeni hukuk kapsamında bulabilmek mümkündür. Ancak genel korumanın eksik kaldığına ilişkin görüşler bulunmaktadır⁸¹. Özellikle teknolojik gelişmelerin hızla arttığı günümüzde kişisel verilerin korunmasına ilişkin hakkın kişilik hakkından bağımsız olarak kişisel verilerin geleceğinin tayin hakkı içerisinde hususi olarak değerlendirilmesi gerektiği savunulmaktadır⁸². Bu görüş kapsamında kişisel verilerin korunmasına ilişkin olarak özel olarak tesis edilmiş temel ilkelerin hüküm altına alındığı, kapsayıcı ve özelleştirilmiş bir düzenlemenin her daim gerekli olduğu belirtilmektedir⁸³.

Kişisel verilerin korunmasının hususiyet arz eden usul ve esaslar doğrultusunda

⁷⁷ Küzeci, **a.g.e.**, s. 75.

⁷⁸ Karar hakkında daha geniş bilgi için bkz. Elif Küzeci, “İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı”, **İnsan Hakları Yıllığı**, Cilt 32, 2014, s. 53, 54.

⁷⁹ Alm. “Informationelles Selbstbestimmungsrecht”, İng. “Self-Determinasyon”

⁸⁰ Furkan Güven Taştan, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, 2. Baskı, İstanbul, On İki Levha Yayıncılık, Kasım 2017, s. 67.

⁸¹ Küzeci, **a.g.e.**, s. 289.

⁸² Taştan, **a.g.e.**, s. 68.

⁸³ Küzeci, **a.g.e.**, s. 289.

birtakım ulusal ve uluslararası hukuk normlarıyla sağlanması özel korumayı ifade etmektedir. Bu doğrultuda bu korumadan beklenen, doğrudan doğruya ve özel olarak kişisel verilerin korunması alanının düzenlenmesidir.

Pek çok devlet, genel kanunlarında yer alan kişilik haklarına dair düzenlemelerin yanı sıra kişisel verilerin korunmasına ilişkin özel düzenlemelere iç hukuklarında ayrıca yer vermektedir. Örnek olarak İsviçre Medeni Kanunu'nda, Türk Medeni Kanunu ile hemen hemen benzer düzenlemelere yer verilmiş olmasına rağmen ayrıca kişisel verilerin korunmasına ilişkin müstakil bir düzenleme yapılmıştır. Almanya, Fransa, İngiltere'de medeni hukuk düzenlemelerinde özel alanının korunmasına yönelik kapsayıcı hükümlere yer verilmiş bulunsa da kişisel verilerin korunmasına ilişkin özel düzenlemeler medeni kanun ile karşılanamayan bir korumayı getirmekte ve bir anlamda genel düzenlenmeleri tamamlamaktadır⁸⁴.

1.2.3. Günümüzde Hızla Gelişen Teknolojiler Işığında Artan Kişisel Verilerin Korunması İhtiyacı

Bilgi depolama, geri getirme ve işleyip yeni bilgiye dönüştürme ihtiyacı en az insanlık tarihi kadar eskidir. İnsanlık her devirde bu amaçlar için çeşitli araçlar ve yöntemler geliştirmiştir. Ancak son yüzyılda teknolojinin hayatın her alanına girmesi, elektronik cihazların günlük yaşamda sıkça kullanılması ile toplanan, işlenen ve kaydedilen veri boyutları tahmin edilemeyecek derecede artmıştır. İşlenen veri ölçeğinde her geçen yıl büyük artışlar yaşanmakta ve insanlık tarihinde örneği yaşanmamış ölçekte veri işlenebilmektedir. 1989'da Avrupa Hukuk Komitesi tarafından yayımlanan raporda verinin yayılma, dağılma ve dolaşım hızının fazla olmasının koruma alanını zorlaştırdığı ifade edilmiştir⁸⁵.

Anlık internet istatistiklerini ölçen "Internet Live Stats" isimli internet sayfasına göre, bu yazının yazıldığı gün içinde ortalama olarak bir saniyede gönderilen mail sayısı 2.600.000, bir saniyede gönderilen tweet sayısı 8,000, bir saniyede yapılan Google

⁸⁴ Küzeci, **a.g.e.**, s. 297-298.

⁸⁵ The European Committee on Legal Co-operation, "New Technologies: A Challenge to Privacy Protection?", Rapor, Fransa, 1989, s.5, (Çevrimiçi) <https://rm.coe.int/1680684607>, 29 Nisan 2018.

araması ise 66.500 adet civarındadır⁸⁶. Her yıl Davos'ta toplanan Dünya Ekonomik Forumu, 2011 yılında Bain & Company ile ortaklaşa hazırladığı raporunda günümüz ekonomisinin yeni bir yapı taşına sahip olduğunu tespit etmektedir. “Kişisel Veri: Yeni Bir Değer Sınıfının Ortaya Çıkışı” başlıklı raporda verinin “*21. Yüzyılda adeta benzin gibi değerli bir kaynak*” haline geldiği savunulmaktadır⁸⁷. 2018 yılında gerçekleşen Dünya Ekonomik Forumunda ise konuşmalar panelinde konuşma yapan tarihçi-yazar Yuval Noah Harari verinin günümüzde en değerli varlık olduğunu belirtip kişisel verinin taşıdığı bir başka öneme dikkat çekerek, verilerin sahipliği kavramının iyi değerlendirilmesi gerektiğinin altını çizmiş ve geleceğin şekillenmesinde veri işleyenlerin aktif rolü olacağını belirtmiştir. Kişisel veri işleyen kurum ve kuruluşların objektif olarak çok fazla kaynaktan veri toplayabilmeleri sebebi ile kişileri, kişinin kendisinden daha iyi tanıyabileceğini belirten Harari, pazarlama, reklamcılık gibi alanlarda bu durumun kullanılabileceğini ve kişilerin manipüle edilebileceğini ifade etmiştir. Bu doğrultuda kişisel verinin ihtiva ettiği manevi değer karşısında ekonomik bir değer arz etmesi ile koruma ihtiyacı daha da artmaktadır⁸⁸.

Günümüzde pek çok şirket kişisel verileri koruyamadığı gerekçesiyle soruşturmalar geçirmekte ve ciddi cezalar almaktadır. Facebook'un, politika alanında çalışmaları olan veri analizi firması Cambridge Analytica ile 2016 Amerika seçimleri sırasında kullanıcılarının verilerini paylaştığı ortaya çıkmıştır. Cambridge Analytica'nın bu şekilde elde ettiği verilerle kısmen oluşturulan psikografik modelleme tekniklerinin Trump seçim kampanyası için yürütülen çalışmaların temelini oluşturduğu iddia edilmektedir. Aynı şekilde Brexit döneminde Birleşik Krallık'ta da benzer bir kampanyanın yürütüldüğü düşünülmektedir. Bu doğrultuda Birleşik Krallık ve Amerika'da şirketin Facebook kanalıyla seçmenlerin verilerini topladığı konusunda

⁸⁶ Internet Live Stats, (Çevrimiçi) <http://www.internetlivestats.com/>, 19 Nisan 2018.

⁸⁷ Açıklamanın orijinali şu şekildedir: “*Personal data will be the new “oil” – a valuable resource of the 21st century*” bkz. World Economic Forum, “Personal Data: The Emergence of a New Asset Class“, Ocak 2011, (Çevrimiçi) http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf, 19 Nisan 2018.

⁸⁸ Yuval Noah Harari, 2018 yılında gerçekleşen Dünya Ekonomik Forumu konuşma videosu, 23 Ocak 2018, (Çevrimiçi), <https://www.weforum.org/events/world-economic-forum-annual-meeting-2018/sessions/will-the-future-be-human>, 19 Nisan 2018.

incelemeler başlatılmıştır⁸⁹. Bu konuda başlatılan soruşturmalar bütün dünyada büyük bir ilgi ile takip edilmiştir.

Günümüzde pek çok uygulamanın ücretsiz olmasının temel sebebi aslında karşılığında kişisel veri talep etmesidir. “*If you’re not paying for the product, you are the product*” ifadesi ile günümüz dijital dünyası tanımlanmaktadır⁹⁰. Büyük oranda doğru olan bu tanım, gerçekten de ücretsiz olan pek çok uygulamanın aslında bireylerden talep ettiği kişisel verileri araştırdıkça belirginleşmektedir. Çevrimiçi davranışsal reklamcılık⁹¹, pek çok pazarlama faaliyeti ve büyük veri uygulamaları doğrudan kişisel verileri kullanmaktadır. Şirketlerin söz konusu bu verileri doğrudan paylaşmasına çoğu zaman gerek olmamaktadır. Google tarafından yaratılan **adwords** ve **adsense** gibi programlar yeni reklamcılık anlayışları markaların kullanıcıların kim olduklarını bilmeden doğru kişiye ulaşmasına olanak sağlamaktadır.

Teknolojinin, tedarik zincirine etkisi ve dijitalleşen dünya ile tetiklenen 4. Sanayi Devrimi’nin getirdiği yenilikler özelinde kişisel verilerin yerinin göz ardı edilmesi mümkün gözükmemektedir⁹². Kişisel verinin, kişiler özelinde ihtiva etmiş olduğu mahremiyet, özel hayatın gizliliği ve kişilik haklarına ilişkin önemin yanında günümüzde ekonomik anlamda da bir değer olarak tartışılması ile birlikte hukuki çerçevesinin çizilerek düzenlenmesi kaçınılmaz bir hal almıştır. Nitekim Kıta Avrupası’nda veri koruma reformu⁹³ ile her ne kadar bu denge göz önünde

⁸⁹ Konuya ilişkin haber için bkz. Foo Yun Chee, “EU lawmakers to investigate alleged misuse of Facebook users’ data”, ed. Alissa de Carbonel, **Reuters**, 19 Mart 2018, (Çevrimiçi), <https://www.reuters.com/article/us-facebook-cambridge-analytica-eu/eu-lawmakers-to-investigate-alleged-misuse-of-facebook-users-data-idUSKBN1GV1A3> , 19 Nisan 2018.

⁹⁰ İnternet kullanıcılarının, kullanımları sırasında bırakmış olduğu elektronik ayak izinin kendilerini ürün haline getirdiğine ilişkin görüş için bkz. Harry Henderson, **Privacy in the Information Age**, Facts of File, Amerika Birleşik Devletleri, 2006, s. 4.

⁹¹ Çevrimiçi davranışsal pazarlama, kullanıcıların çevrimiçi faaliyetleri esas alınarak, bireysel bir profil oluşturarak ve hedeflenmesine olanak sağlayan ve kullanıcılara daha nitelikli ve özelleştirilmiş bir içerikle reklam hizmeti sunulmasını sağlayan bir teknolojidir. Tüketici davranışları üzerindeki etkileri ve kişisel verilerle ilişkisine ilişkin olarak bkz. Leyla Keser Berber, **Çevrimiçi Davranışsal Reklamcılık**, İstanbul, On İki Levha Yayıncılık, 2014.

⁹² Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, “EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies”, **Computer Law & Security Reviews**, Cilt 34, Sayı 1, Şubat 2018, s. 138.

⁹³ Avrupa Komisyonu, “Avrupa Birliği Genel Veri Koruma Tüzüğü Taslağı”, 2012/0011, C7-0025/12, Brüksel 25 Ocak 2012, s. 2, (Çevrimiçi)

bulundurularak bir düzenleme yapılması planlansa da Avrupa Birliği Genel Veri Koruma Tüzüğü'nde bu denge, veri temelli ekonomiden ziyade birey lehine kurularak kişisel verilerin korunmasına ilişkin daha sıkı düzenlemeler getirilmiştir.

Kişisel verilerin taşınmış olduğu ekonomik ve sosyal değer itibari ile iktisadi menfaat ve kişilik hakkı arasında bir çatışma söz konusu olmaktadır. Kıta Avrupası'ndaki kişilik hakkı merkezli yaklaşım, Avrupa merkezli şirketler tarafından teknolojik gelişimi engellediği gerekçesiyle eleştirilere konu edilmektedir. Ancak kabul edilmelidir ki günümüz teknolojileri ile işlenen veriler, bireylerin geleceğini tahmin edebilme ve yönlendirebilme potansiyelini kendi içinde barındırmaktadır. Bu bakımdan bireylerin özgür olarak gelişebilmeleri, kendilerini ifade edebilmeleri ve kişisel verilerini rahatça paylaşabilmeleri için kendilerini güvenli bir ortamda hissetmeleri esas olmalıdır⁹⁴. Bu güvenli ortamı sağlarken ise diğer taraftaki iktisadi menfaati ve teknolojik gelişmeleri engelleyecek kısıtlamalardan mümkün olduğunca kaçınmak, menfaatler arası dengeyi kurabilen, uygulanabilir düzenlemelerin hayata geçirilmesine gayret etmek gerekmektedir.

1.3. Kişisel Verilerin Korunmasının Tarihsel Gelişimi

Kişisel verilerin korunması, teknolojinin gelişimiyle birlikte gittikçe önemi artan bir konu haline gelmiştir. 1950'li ve 1960'lı yıllar çeşitli ve şaşırtıcı imkânlar sağlayan bilgisayarların ortaya çıktığı, hızla geliştiği ve bilgisayar kullanımının giderek yaygınlaşmaya başladığı bir dönemdir⁹⁵. Veri işlemenin, insan eli ile yapıldığı dönemden otomatik olarak bilgisayarlar aracılığı ile gerçekleştirilmeye başladığı döneme geçilmesi ve doğal bir sonuç olarak çok daha fazla verinin çok daha hızlı bir şekilde işlenebilmesi, büyük ölçekte veri kayıt sistemlerinin oluşmasını sağlamıştır. Bu dönemde kişisel verilerin işlenmesi alanında kazanılan hız hem toplumsal hem de

[http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM\(2012\)0011_EN.pdf](http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf), 23 Nisan 2018

⁹⁴ NESSI (the Networked Software and Services Initiative), "Big Data: A New World of Opportunities, White Paper", Aralık 2012, s. 19, (Çevrimiçi) http://www.nessi-europe.com/Files/Private/NESSI_WhitePaper_BigData.pdf, 14 Nisan 2018.

⁹⁵ Çekin, **a.g.e.**, s. 5.

akademik düzeyde temel hak ve özgürlükler açısından endişe ile karşılanmıştır⁹⁶. İkinci Dünya savaşı sırasında kişisel verilerin kötüye kullanımlarından çıkarılan dersler Avrupa Topluluğu’nu bu konuda önlemler almaya sevk etmiştir⁹⁷.

Bu doğrultuda bilgisayarların ve otomatik veri işleme sistemlerinin kullanılmasından dolayı kişilerin temel hak ve özgürlükleri özelinde korumanın sağlanabilmesi adına 1970’li yıllarda ilk hukuki metinler kabul edilmeye başlanmıştır⁹⁸.

İlk olarak 1970 yılında Almanya’nın Hessen eyaletinde kişisel verilerin korunmasına ilişkin eyalet düzeyinde bir yasal düzenleme yapılarak bu ihtiyaç karşılanmaya çalışılmıştır. Düzenlemenin o dönem için kabulündeki en önemli etken, şehir bölge planlama amacı ile ortaya çıkmış ve tartışmalara konu olan “Hessen Planı”dır. Hessen Planı ile 1960’lı yılların sonunda federe düzeyde merkezi bir veri bankasının kurulması tasarlanmıştır⁹⁹. Hessen Planı ile yapılan bu çalışma, kişilerin özel yaşamının gizliliğine ve mahremiyetine ilişkin endişeleri tetikleyerek kişisel verilerin korunmasına yönelik düzenlemelerin yapılmasına ilişkin bir temel hazırlamıştır. Konuya ilişkin devam eden tartışmalar ve Hessen eyaletinin verilerin korunmasına ilişkin yaptığı düzenleme, kısa süre sonra Almanya’da federal düzeyde de bir koruma ihtiyacını gündeme getirmiş ve 1977 yılında Federal Almanya Veri Koruma Yasası kabul edilmiştir.

Devletlerin vatandaşlarını belirlenebilir kılma amacı ile yapmış olduğu çalışmalara ilk örneklerden biri İsveç’in 1947 yılında her vatandaşa cinsiyet ve doğum tarihi bilgilerini içeren, on haneli bir kimlik numarasının verilmesini sağlayan bir sistem oluşturulmasıdır¹⁰⁰. İsveç’te 1960’lı yılların ortalarında ise nüfus sicili ve ayrıca bir

⁹⁶ Cherie L. Givens, **Information Privacy Fundamentals for Librarians and Information Professionals**, United Kingdom, Rowman & Littlefield, 2014, s. 7.

⁹⁷ Steven S. McCarty ve Anne Titus Hilby, “Research Guide to European Data Protection Law“, **Legal Research Series**, Berkley, 2013, s. 11.

⁹⁸ Cherie L. Givens, **a.g.e.**, s. 7.

⁹⁹ 1960’lı yıllarda Almanya’da, devlet kurumları tarafından çeşitli amaçlar doğrultusunda, bilgisayar sistemleri giderek yaygınlaşarak kullanılmaya başlanmıştır. Bu konuda en bilinen ve en çok tartışılmış örneklerden biri; Bavyera eyalet yönetiminin, Münih’te yapılan olimpiyatlar için kurulmuş olan bilgisayar sistemini, daha sonra merkezi Bavyera Mülk Bilgi Sistemi’ne dönüştürmek isteyerek çalışmalar yürütmesidir. Colin J. Bennett, **Regulating Privacy: Data Protection and Public Policy in Europe and the United States**, New York, Cornell University Press, 1992, s. 48.

¹⁰⁰ Colin J. Bennett, **a.g.e.**, s. 49-50.

vergi sicili oluşturmak için çalışmalara başlanmıştır. Almanya’da duyulanlara benzer endişelerin tetiklenmesini sağlayan bu gelişmeler doğrultusunda Federal Almanya Veri Koruma Yasası’nın kabulünden önce İsveç’te 1973 yılında kişisel verilerin korunması alanında Almanya’nın Hessen eyaletindeki düzenlemeden sonra ilk ulusal düzenleme olarak kabul edilen kişisel verilerin korunmasına ilişkin kanun yasalaşmıştır. 1973 yılında yasalaşan İsveç Veri Koruma Kanunu kapsam olarak sadece bilgisayar aracılığı ile kişisel verilerin işlenmesini düzenlemiştir. Kişisel verilerin hangi koşulda, ne zaman işlenebileceğine ve genel veri koruma ilkelerine ilişkin maddi hükümler 1973 yılında yasalaşan İsveç Veri Koruma Kanunu’nda yer almamıştır. Bunun yerine her bir bilgisayarlı kişisel veri kayıt işlemi için veri koruma otoritesinden öncelikle izin alınması gerektiği ve veri koruma otoritesinin her bir kayıt işlemi için ayrı şartlar öngörebileceği düzenlenmiştir¹⁰¹.

Aynı dönemde diğer Avrupa ülkelerinde de kişisel verilerin korunması konusu gündeme gelerek, kısa bir süre içerisinde kişisel verilerin korunmasına ilişkin hukuki metinler Avrupa’da pek çok ülkede yasalaşmıştır. OECD’nin kişisel verilerin korunmasına ilişkin temel ilkelere yer verdiği uluslararası kişisel verilerin korunmasına ilişkin bağlayıcı olmayan ilk metin olarak kabul edilen “Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler”¹⁰²in yayınlandığı 1980 yılında, kişisel verilerin korunmasına ilişkin olarak Avrupa Ekonomik Topluluğu üyelerinden İrlanda, İtalya ve Birleşik Krallık dışındaki bütün üyeler, kişisel verilerin korunmasına ilişkin olarak ya ciddi çalışma ve hazırlıklarını yürütme aşamasında ya da halihazırda gerekli düzenlemeleri tamamlamış bulunmakta idiler.

1980 yılında OECD tarafından belirlenmiş olan kişisel verilerin korunmasına dair birtakım ilkeler uluslararası alandaki ilk çalışmalara örnektir. Rehber niteliğinde olan bu ilkeler hukuken bağlayıcı olmamakla birlikte daha sonra hukuken bağlayıcı pek çok metinde benzer şekilde yer bulmuştur. Avrupa Konseyi, 1981 tarihli ve 108 sayılı

¹⁰¹ Sören Öman ”Implementing Data Protection in Law”, **Scandinavian Studies in Law**, The Stockholm University Law Faculty, Cilt 47, 2004, s. 290.

¹⁰² OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 Eylül 1980.

Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme¹⁰³ ile kişisel verilerin toplanması, işlenmesi, saklanması ve transferi gibi işlemleri birtakım kurallara bağlamıştır. Kişisel verilerin korunması alanında uluslararası düzlemde bağlayıcı ilk metin olma niteliğini haiz bu sözleşmeye Avrupa Konseyi üyesi 47 devlet ve üye olmayan 6 devlet taraftır¹⁰⁴. 1990 yılında Birleşmiş Milletler Genel Kurulu tarafından kabul edilen “Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler” adını taşıyan belgede kişisel veri dosyalarının bilgisayar aracılığıyla işlenmesine ilişkin genel ilkeler öngörülmüştür. Avrupa Birliği ise 24 Ekim 1995 tarihinde veri koruma hukukunun temelini oluşturan 95/46 sayılı “Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımına Dair Yönerge” ile kişisel veri tanımını yapmış ve Avrupa Birliği dâhilinde yeknesak bir veri koruma hukuku anlayışının temelini oluşturmuştur.

1.3.1. OECD Rehber İlkeleri

OECD, İkinci Dünya Savaşı’nda zarar gören ve tahrip edilen Avrupa’nın yeniden inşası için 1948 yılında kurulan ve 1960 yılında Kanada ve Amerika Birleşik Devletleri’nin de katılımıyla küresel çapta bir işlerlik kazanan Avrupa Ekonomik İşbirliği Örgütü’nün devamı niteliğinde olup 1961 yılında kurulmuştur. 35 üyesi¹⁰⁵ bulunan OECD, ekonomik büyümeyi desteklemek, iş alanlarını arttırmak, yaşam standardını yükseltmek, finansal dengeyi korumak, başka devletlerin ekonomik gelişimine yardımcı olmak, küresel ticaretin büyümesine katkı sağlamak ile demokrasiye ve pazar ekonomisine bağlı devletleri bir araya getirmek amacı taşıyan çalışmalar yürütmektedir. OECD kararları, tavsiye niteliğinde olup üye ülkeler için herhangi bir bağlayıcılık taşımamaktadır. Ancak kurulan ilişkiler gereği üye devletler, OECD tarafından belirlenen ilke ve kurallara riayet etmeye özen göstermektedir. Esasen serbest piyasa ekonomilerinin gelişimini amaçlayan OECD, kişisel verilerin

¹⁰³ Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 Ocak 1981.

¹⁰⁴ Sözleşmeyi imzalayan ve kabul eden ülke bilgileri için bkz. Chart of signatures and ratifications of Treaty 108, 19 Nisan 2018, (Çevrimiçi) <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures>, 19 Nisan 2018.

¹⁰⁵ Üye ülkelerin listesi için bkz. List of OECD Member Countries - Ratification of the Convention on the OECD, (Çevrimiçi) <http://www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm>, 19 Nisan 2018.

korunması ile ilgili çalışmalara 1969 yılında oluşturduğu Veri Bankaları Paneli isimli bir çalıştay ile başlamıştır¹⁰⁶. 1977 yılında bu çalıştay tarafından Viyana’da organize edilen sempozyumda hükümetler, sanayi, uluslararası veri iletişim kullanıcıları, işletmeciler ve hükümetler arası kuruluşların dâhil olduğu paydaşlardan görüş ve deneyimleri toplanmıştır. Sempozyum sonucunda uluslararası veri aktarımlarının önemli olduğu ancak ülkelerin güvenlik ve kamu düzeni çerçevesinde çıkarlarının korunması gerektiği belirtilmiştir. Bununla birlikte bilginin ekonomik bir değer ihtiva ettiği, gerekli güvenlik önlemlerinin ve tedbirlerin alınması gerektiği, ülkelerin kişisel verilerin korunması için birtakım temel ilkelere bağlı kalması gerektiğine ilişkin tespitlerde bulunulmuştur. 1978 yılında oluşturulan yeni bir çalışma grubuna ise uluslararası veri aktarımlarına ve kişisel verilerin korunmasına ilişkin olarak temel ilkeleri hazırlama görevi verilmiştir. Çalışmalar Avrupa Topluluğu ve Avrupa Konseyi’nin işbirliği ile birlikte 1 Temmuz 1979 tarihinde tamamlanmıştır.

1980 yılında OECD Rehber İlkeleri’nin¹⁰⁷ OECD tarafından kabul edilmesi kişisel verilerin korunması meselesinin ekonomik anlamının altını çizmektedir. OECD Rehber İlkeleri ile verinin serbest dolaşımı ve ilgili kişinin kişisel verisinin korunmasına ilişkin menfaatlerinin dengelenmesi gerektiği vurgulanmıştır. OECD, genel olarak üye devletlere kişisel verilerin korunması ve bireysel özgürlüklerle ilgili kabul edilen ilkeleri, iç hukuklarında yapacakları yasal düzenlemelerde göz önünde bulundurarak uluslararası veri akışının ölçüsüz olarak engellenmemesini, mevcut engellerin kaldırılmasını, bu ilkelerin uygulanabilir kılınması için işbirliği yapılmasını tavsiye etmektedir. OECD Rehber İlkeleri, kişisel verilerin korunmasına ilişkin yaklaşımların belirlenmesi ve yasal düzenlemelerin yapılmasında temel alınacak olan 8 ilkeyi belirlemektedir. Bu ilkeler, “veri toplamanın sınırlı olması ilkesi”¹⁰⁸, “verilerin

¹⁰⁶ OECD, kamu sektöründe bilgisayar kullanımlarından yararlanılarak gerçekleştirilen uluslararası veri aktarımlarına ilişkin olarak çalışmalar programlamıştır. Bir grup uzman, dijital veri, kamu yönetimi ve uluslararası ver aktarımı gibi faaliyetlerin mahremiyete etkisine ilişkin farklı incelemelerde bulunmak üzere çalışmalar yürütmüştür. OECD, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, **OECD**, Fransa, 2001, s. 27.

¹⁰⁷ OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 Eylül 1980, (çevirimiçi) http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html, 19 Nisan 2018.

¹⁰⁸ OECD Rehber İlkeleri, m. 7.

belirli bir niteliği karşılaması (veri kalitesi) ilkesi”¹⁰⁹, “amacın belirliliği ilkesi”¹¹⁰, “kullanımın sınırlı olması ilkesi”¹¹¹, “veri güvenliği ilkesi”¹¹², “açıklık ilkesi”¹¹³, “bireyin katılımı ilkesi”¹¹⁴ ve “hesap verilebilirlik ilkesi”¹¹⁵ olarak metinde yer almaktadır.

Her ne kadar metnin üye ülkeler açısından bir bağlayıcılığı olmasa ve üye ülkelerin söz konusu düzenlemeleri iç hukuklarına aktarmaları gibi bir zorunluluğu bulunmasa da OECD Rehber İlkeleri ilerleyen zamanda yapılan ulusal ve uluslararası birçok hukuki metinde dikkate alınmış ve yol gösterici olmuştur¹¹⁶. Birçok ulusal ve uluslararası düzenlemenin gerekçelerinde OECD Rehber İlkelerine atıf görmek mümkündür¹¹⁷. Belirtmek gerekir ki OECD Rehber İlkelerinin hazırlanma sürecinde çalışma grubu Avrupa Konseyi ile yakın temas halinde çalışmıştır. Bunun nedeni iki kurum arasında hazırlanacak olan metinler arasındaki gereksiz farklılıklardan kaçınmak ve benzer temel ilkeleri baz alabilmektir¹¹⁸. Ancak OECD temel ilkeleri, kişisel verilerin işlenmesinde kullanılan metot ya da araçlara bakılmaksızın temel olarak mahremiyet ve bireysel özgürlüklere yönelik olması sebebi ile daha sonraki yıllarda Avrupa Konseyi tarafından hazırlanan sözleşme metninden ayrılmaktadır.

OECD rehber ilkelerinin bir diğer önemi ise OECD üyelerinin sadece Avrupa Birliği üyeleri ile sınırlı kalmamaları sebebi¹¹⁹ ile çok daha geniş bir kapsamda farklı kültür

¹⁰⁹ OECD Rehber İlkeleri, m. 8.

¹¹⁰ OECD Rehber İlkeleri, m. 9.

¹¹¹ OECD Rehber İlkeleri, m. 10.

¹¹² OECD Rehber İlkeleri, m. 11.

¹¹³ OECD Rehber İlkeleri, m. 12.

¹¹⁴ OECD Rehber İlkeleri, m. 13.

¹¹⁵ OECD Rehber İlkeleri, m. 14.

¹¹⁶ Hayrunnisa Özdemir, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, 1. Baskı, Ankara, Seçkin Yayıncılık, 2009, s. 23.

¹¹⁷ 108 sayılı Sözleşme ve Kişisel Verilerin Korunması Kanunu örnek olarak verilebilecektir.

¹¹⁸ OECD, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, s. 28.

¹¹⁹ Pek çok Avrupa ülkesi OECD üyesidir. Avrupa dışındaki üye devletlerden bazıları, ABD, Avustralya, Kanada, Japonya, Kore, Meksika, Yeni Zelanda’dır. Üye ülkelerin tamamı için bkz. “List of OECD Member countries”, (çevirimiçi) <http://www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm>, 12 Nisan 2018.

ve hukuk düzenlerinin sentezi sonucu oluşmuş ve üzerinde uzlaşmış bir metin olmasıdır.

OECD, kişisel verilerin korunması alanına ilişkin çalışmalarına sonraki dönemlerde de teknolojinin getirdiği yenilikler ve ihtiyaçlar doğrultusunda devam etmiştir¹²⁰, 2000 yılında kurumlara gizlilik politikalarının oluşturulmasında yardımcı çevrimiçi eğitim programı oluşturmuş¹²¹, siber güvenlik¹²², çocukların çevrimiçi korunması¹²³ ve dijital güvenlik ve risk yönetimine¹²⁴ ilişkin olarak sürekli olarak güncellenen raporlar yayınlamıştır.

1.3.2. Avrupa Konseyi Düzenlemeleri

İkinci Dünya Savaşı'nın hemen ardından 10 Avrupa ülkesi¹²⁵ tarafından kurulan Avrupa Konseyi'nin hedefi, 5 Mayıs 1949'da imzaya açılan ve 3 Ağustos 1949'da yürürlüğe giren Avrupa Konseyi Statüsü'nün¹²⁶ başlangıç bölümünde belirtildiği şekli ile aşağıdaki gibidir:

¹²⁰ 11 Nisan 1985'de "Uluslararası Veri Aktarımı Deklarasyonu" üye devletlerin hükümetlerince kabul edilmiştir. **"Declaration on Transborder Data Flows"**, (Çevrimiçi) <http://www.oecd.org/sti/ieconomy/declarationontransborderdataflows.htm> , 19 Nisan 2018.

¹²¹ "OECD Privacy Statement Generator", (Çevrimiçi) <http://www.oecd.org/sti/ieconomy/oecdprivacystatementgenerator.htm>, 12 Nisan 2018.

¹²² OECD'nin devletlerin siber güvenlik stratejilerine ilişkin olarak 10 OECD üye ülkesi arasında yaptığı araştırma sonucunda ülkelerin siber güvenlik yaklaşımları ve stratejilerine ilişkin analizlerin yer aldığı rapor 16 Kasım 2012'de yayımlanmıştır. (Çevrimiçi) [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg\(2011\)12/final&doclanguage=en](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2011)12/final&doclanguage=en) , 12 Nisan 2018.

¹²³ Çocukların günlük çevrimiçi kullanımının artmasıyla beraber internet kullanımının yararlarının yanı sıra yarattığı risk alanlarına da dikkat çeken OECD konuyu önemli bir mesele olarak ele alarak rapor yayınlamıştır. Bkz. "The Protection Of Children Online- Risks faced by children online and policies to protect them", 2 Mayıs 2011, (Çevrimiçi) https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf , 12 Nisan 2018.

¹²⁴ "Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document", 2015, (Çevrimiçi) <http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf> , 12 Nisan 2018.

¹²⁵ İlk onaylayan ülkeler, Belçika, Birleşik Krallık, Danimarka, Fransa, Hollanda, İrlanda, İsveç, İtalya, Lüksemburg ve Norveç olmuştur. Almanya, Yunanistan, İzlanda 1949-1950 yılları içerisinde; Avusturya 1956'da, Kıbrıs 1961'de; Malta 1965 yılında katılmıştır.

¹²⁶ Avrupa Konseyi'nin Statüsü'ne Dair Sözleşme 5 Mayıs 1949 tarihinde Londra'da imzaya açılmış ve 42. maddeye uygun olarak 3 Ağustos 1949 tarihinde yürürlüğe girmiştir. Türkiye Sözleşme'yi 12 Aralık 1949 tarihinde onaylamış ve 13 Nisan 1950 tarihinde katılmıştır. 5456 sayılı Onay Kanunu 17 Aralık 1949 gün ve 7382 Sayılı Resmi Gazete 'de yayımlanmıştır. Statute of the Council of Europe, Antlaşma

“(...)halklarının ortak mirası olan ve tüm gerçek demokrasilerin temelindeki bireysel özgürlük, siyasal özgürlük ve hukuk düzeni ilkelerinin gerçek kaynağını oluşturan manevi ve ahlaki değerlere derin bağlılıklarını yeniden belirterek (...) halklarının bu konudaki açık beklentilerine karşılık olmak üzere Avrupa devletlerini daha yakın bir birliğe kavuşturacak bir örgüt kurmanın ivedi gereğini göz önüne alarak (...) bu amaçla aşağıdaki Statüyü benimsemiştir.”

Avrupa Konseyi kişisel verilerin korunmasının da dâhil olduğu pek çok konuda Avrupa Birliği kurumları ile ortak çalışmalar yürütmektedir. Avrupa Birliği organı olmayan Avrupa Konseyi’ne Avrupa Birliği üyesi devletlerin tamamı üyedir. Bölgesel bir kuruluş olan Avrupa Konseyi’nin amaçlarının başında insan haklarının korunması ve geliştirilmesi gelmektedir¹²⁷. Avrupa Konseyi insan haklarının korunması alanındaki çalışmalarını çeşitli hukuksal metinlerin kabulü ve bu alandaki çalışmaların devamlılığı ile yürütmektedir. Konsey’in Kurulduğu yıl olan 1949 yılı içerisinde Avrupa İnsan Hakları Sözleşmesi tasarısı üzerinde çalışmalar başlamıştır. Bu doğrultuda İnsan Hakları Bildirisi’nde bulunan hakları topluca güvence altına almak üzere 4 Kasım 1950’de Roma’da “İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi” imzalanmış ve sözleşme 10 devletin onaylama sürecini tamamlaması ile 3 Eylül 1953’te yürürlüğe girmiştir¹²⁸.

Avrupa Konseyi Danışma Kurulu, Nisan 1967’de Hukuk Komitesini iki konuda çalışma yapmak üzere görevlendirmiştir. Bunlardan ilki modern bilim ve teknolojik

sayısı: 002, imza tarihi: 5 Mayıs 1949, yürürlük tarihi: 3 Ağustos 1949, Türkçe metni için bkz. Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonu tarafından çevirilen metin, “Avrupa Konseyi Statüsü”, (Çevrimiçi) <http://www.ombudsman.gov.tr/contents/files/771a1--Avrupa-Konseyi-Statüsü.pdf>, 2 Nisan 2018.

¹²⁷ Şeref Gözübüyük, Feyyaz Gölcüklü, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması: Avrupa İnsan Hakları Mahkemesi İncelemesi ve Yargılama Yöntemi**, 11. Ek Protokola Göre Hazırlanıp Genişletilmiş 11. Bası, Ankara, Turhan Kitabevi, Ocak 2016, s. 8.

¹²⁸ Türkiye Avrupa İnsan Hakları Sözleşmesini ilk imzalayan devletlerden biridir. Ancak onaylama süreci 18 Mayıs 1954’te tamamlanmıştır. Bu tarihten itibaren Türkiye’nin Sözleşme’ye taraf olmaktan kaynaklı yükümlülükleri işlerlik kazanmıştır. 28 Ocak 1987’de de bireysel başvuru hakkını tanımıştır. Mahkemenin zorunlu yargı yetkisini ise 28 Ocak 1990’da kabul etmiştir. Avrupa İnsan Hakları Sözleşmesi’nin kurduğu sisteme ilişkin ayrıntılı bilgi için bkz. Mehmet Semih Gemalmaz, **Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş**, 7. Baskı, İstanbul, Legal Yayıncılık, 2010, s. 965.

gelişmelerin insan haklarına etkisine dair çözüm üretmek diğeri ise ağırlıklı olarak hızla yayılan teknolojik cihazların mahremiyet hakkına müdahalesine ilişkin söz konusu cihazların hukuki olarak nasıl düzenlenebileceği hakkında önerge hazırlamaktır. Bu çalışmalar sonucunda kişisel verilerin korunması ilkesine dair yaklaşımlar, Avrupa Konseyi'nin 1968 yılında kabul ettiği, "Modern Bilimsel ve Teknolojik Gelişmeler ve İnsan Hakları Hakkında 509 sayılı Tavsiye Kararı"¹²⁹ ile ortaya çıkmıştır. 509 sayılı Tavsiye Kararı'nda, modern bilim ve teknolojik gelişmelerin bireylerin temel hak ve özgürlüklerine ciddi tehdit oluşturduğu¹³⁰, üye devletlerin çoğunluğundaki yasaların mahremiyet hakkına yönelik bu tür tehditlere karşı yeterli koruma sağlamadığı ve bunun sonucunda Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin ihlal edilebileceğine dair endişe bulunduğu¹³¹ belirtilmiştir. Ayrıca üye ülkelere, modern bilim ve teknolojik gelişmeler ışığında söz konusu olabilecek ihlallere karşı özel hayatın gizliliği hakkının ulusal mevzuatlarında yeterince korunup korunmadığına ilişkin inceleme yapmaları önerilmiştir¹³².

1969 yılında tartışılarak kabul edilen Yerel Kamu Kurumlarında Bilgisayarların Kullanılması Hakkında 557 Sayılı Tavsiye Kararı'nda¹³³ ise kamusal hizmetlerin görülebilmesi için özel sektörde halihazırda kullanılan modern araçların tercih edilmesi gerektiği¹³⁴, bilgisayarlardan kamu hizmetlerinde yararlanmasının Avrupa toplumunun evriminde belirleyici bir aşama oluşturduğu¹³⁵, özel kişilerin elindeki bilgi yoğunluğunun ciddi riskler içerdiği¹³⁶, ancak ülkelerin kötüye kullanımına ilişkin gerekli yasal önlemleri almaları gerektiği¹³⁷ belirtilmiştir.

¹²⁹ Avrupa Konseyi, 509 sayılı Tavsiye Kararı, Avrupa Konseyi Parlamenter Meclisi tarafından 31 Ocak 1968'de tartışılarak kabul edilmiştir. "Human rights and modern scientific and technological developments", (Çevrimiçi), <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en>, 12 Nisan 2018.

¹³⁰ Avrupa Konseyi, Tavsiye kararı 509, 1968, m. 2.

¹³¹ Avrupa Konseyi, Tavsiye kararı 509, 1968, m. 4.

¹³² Avrupa Konseyi, Tavsiye kararı 509, 1968, m. 8/1.

¹³³ Avrupa Konseyi Parlamenter Meclisi tarafından 14 Mayıs 1969'da tartışılarak kabul edilmiştir. "Use of Computers in Local Government", (Çevrimiçi), <http://www.assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14593&lang=en>, 12 Nisan 2018.

¹³⁴ Avrupa Konseyi, Tavsiye Kararı 557, 1969, m. 2.

¹³⁵ Avrupa Konseyi, Tavsiye Kararı 557, 1969, m. 5.

¹³⁶ Avrupa Konseyi, Tavsiye Kararı 557, 1969, m. 6.

¹³⁷ Avrupa Konseyi, Tavsiye Kararı 557, 1969, m. 16.b.

1970’li yılların başında yürütülen kişisel verilerin korunmasına ilişkin öneri ve çözüm metinlerinin oluşturulmasına ilişkin çalışmalar sonucunda Avrupa Konseyi hem özel sektör¹³⁸ hem de kamu alanında¹³⁹ kişisel verilerin korunmasına ilişkin tavsiye kararları yayımlamıştır.

Kişisel verilerin korunması alanında Avrupa Konseyi tarafından yapılan en önemli çalışma 1981 yılında kabul edilen 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme’dir¹⁴⁰. OECD Rehber İlkeleri’nden sonra kişisel verilerin korunmasına ilişkin uluslararası alanda hissedilen hukuken bağlayıcı bir metin ihtiyacı Avrupa Konseyi çalışmaları ile nihayetlenmiştir. 108 sayılı Sözleşme kişisel verilerin korunması alanında hukuksal bağlayıcılığı olan ilk uluslararası belgedir.

1.3.2.1. 108 sayılı Sözleşme

1976 yılında uluslararası veri trafiğini de kapsayacak şekilde kişisel verilerin korunması alanında uluslararası sözleşme hazırlanması için Avrupa Konseyi tarafından görevlendirilen uzmanlar komitesi 1979 yılında bir tasarı hazırlayarak Bakanlar Komitesine sunmuştur. Bu tasarı Bakanlar Komitesi tarafından kabul

¹³⁸ Avrupa Konseyi, 73 (22) sayılı “Özel Sektördeki Elektronik Veri Bankaları Karşısında Kişilerin Özel Hayatlarının Korunması Hakkında Tavsiye Kararı” Avrupa Konseyi Bakanlar Komitesi tarafından 26 Eylül 1973’te tartışılarak kabul edilmiştir. “On the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in the Private Sector”, (Çevrimiçi), <https://rm.coe.int/1680502830>, 12 Nisan 2018. Ancak bu tavsiye kararı ve ekindeki ilkeler; uygulanması öngörülen ilkelere ilişkin somut bir rehber sunmadığı, yeterince açık olmadığı ve özel sektörde elektronik veri bankalarının kullanımının sınırlı olması sebebi ile uygulama alanı darlığı gerekçeleriyle eleştirilmiştir. Jeremy Warner, “The Right to Oblivion: Data Retention From Canada to Europe in Three Backward Steps”, **University of Ottawa Law and Technology Journal**, Sayı 2, 2005, s. 82.

¹³⁹ Avrupa Konseyi, 73 (22) sayılı tavsiye kararına gelen eleştiriler üzerine, uygulamayı kamu sektörünü de içerecek genişletmek üzere 74 (29) sayılı “Kamu Sektöründeki Elektronik Veri Bankaları Karşısında Kişilerin Özel Hayatlarının Korunması Hakkında Tavsiye Kararı” yayınlamıştır. “On the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in the Public Sector”, 20 Eylül 1974, (Çevrimiçi), <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51>, 12 Nisan 2018. Bu kararda kişilerin özel hayatlarının gizliliğinin korunması için gerekli önlemlerin alınması şartıyla istatistiki, bilimsel veya tarihsel çalışmalar gibi amaçlarla verilerin belirsiz bir süre ile saklanabileceğini de belirtmiştir.

¹⁴⁰ Avrupa Konseyi, “Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data”, 28 Ocak 1981, (Çevrimiçi) <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>, 12 Nisan 2018.

edilerek 28 Ocak 1981 tarihinde imzaya açılmıştır. 1 Ekim 1985 tarihinde yürürlüğe giren 108 sayılı Sözleşme'nin uluslararası alanda ilk düzenlenme olmasının yanı sıra bir başka büyük önemi, yalnızca üye devletlere değil Avrupa Konseyi üyesi olmayan devletlerin de imzasına açık olmasıdır¹⁴¹.

108 sayılı Sözleşme'ye taraf devletlerin, ülkelerinde bulunan herkes için geçerli olacak şekilde metinde yer alan ilkeleri iç hukuklarına aktarmaları gerekmektedir. Bağlayıcı bir metin olması dolayısıyla OECD Rehber İlkeleri'nin aksine öneri niteliğinde değildir. 108 sayılı Sözleşme'nin ihtiva etmiş olduğu düzenlemeleri iç hukuklarında uygulamaya koymak taraf devletler için bir yükümlülük arz etmektedir. 108 sayılı Sözleşme uyarınca her bir taraf devletin, en geç sözleşme kendi iç hukukundaki kurallar doğrultusunda yürürlüğe girinceye kadar söz konusu ilkeleri uygulanabilir kılmak için kendi ulusal hukukunda gerekli düzenlemeleri yapması gerekmektedir¹⁴². Belirtmek gerekir ki 108 sayılı Sözleşme uygulama alanı bakımından OECD Rehber İlkeleri'nden ayrı olarak sadece otomatik olarak işlenen kişisel veriler bakımından bir düzenleme getirmektedir¹⁴³.

108 sayılı Sözleşme ile ülkeler tarafından iç hukuklarında uygulanması gereken kişisel verilerin korunmasına yönelik asgari gereklilikler belirlenmiştir. OECD Rehber İlkeleri'ne paralel şekilde 108 sayılı Sözleşme ile belirlenen temel ilkeler, verilerin belirli bir nitelikte olması (m. 5), hassas kişisel verilerin özel olarak korunması (m. 6), veri güvenliği (m. 7), ilgili kişinin bilgi alma, verilere ulaşma ve gerektiğinde onları düzeltme hakkı tanınması (m. 8) olarak belirtilmiştir. 108 sayılı Sözleşme uyarınca taraf devletler, kişisel verilerin korunması amacı ile belirlenmiş temel ilkeleri ve ilgili kişilerin haklarını ancak kanunlarla ve demokratik bir toplumda gerekli bir önlem

¹⁴¹ 108 sayılı Sözleşme'yi imzalayan ve onaylayan ülkelerin listesi için bkz. "Members of Council of Europe", (Çevrimiçi), <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures>, 12 Nisan 2018.

¹⁴² Türkiye tarafından 108 sayılı Sözleşme 28 Ocak 1981 tarihinde imzalamış olmasına karşın, iç hukukta gerekli düzenlemeler uzun süre yapılmadığı için uygun bulma kanunu uzun süre çıkarılmamıştır. Türkiye 108 sayılı Sözleşmeyi ancak 2 Mayıs 2016'da onaylamış ve bu nedenle 108 sayılı Sözleşme'nin Türkiye için yürürlük tarihi 1 Eylül 2016 olmuştur.

¹⁴³ 108 sayılı Sözleşme, giriş bölümünde "...taking account of the increasing flow across frontiers of personal data undergoing automatic processing" ifadesi yer almaktadır.

niteliğinde olması şartıyla istisnai olarak sınırlandırılabileceklerdir¹⁴⁴. Bu istisnai haller, devletin veya kamunun güvenliğinin veya devletin önemli malî çıkarlarının korunması ya da suçun önlenmesi ve verileri işlenen kişilerin yahut başkalarının hak ve özgürlüklerinin korunması şeklinde belirtilmiştir (m. 9).

Bununla beraber 108 sayılı Sözleşme ayrıca uluslararası alanda kişisel verilerin serbest dolaşımı prensibini benimsemekte bir başka deyişle devletlerin özel yaşamın gizliliğinin korunması gerekçesiyle veri aktarımı yasaklamasını ya da özel bir izne tabi tutmasını onaylamamaktadır¹⁴⁵. Ancak söz konusu düzenlemeye ilişkin devletlerin veri akışını yasaklayabilecekleri iki istisna belirtilmiştir. 108 sayılı Sözleşme uyarınca belirli veri kategorileri için özel bir koruma getirilmiş olması ve aktarımın yapılacağı akit devlette eşdeğer korumanın bulunmaması durumunda ya da aktarımın Sözleşme'nin tarafı olmayan üçüncü bir devlet aracılığıyla yapılacak olması halinde ülkenin veri akışına izin vermeme hakkı bulunmaktadır¹⁴⁶.

1.3.2.2. 108 sayılı Sözleşme'ye Ek Protokol

8 Kasım 2001'de imzaya açılmış olan 181 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol¹⁴⁷ ile 108 sayılı Sözleşme'deki önemli bir eksikliği gidermek üzere kişisel veri işleme etkinliklerini denetleyecek bağımsız bir organ öngörülmüştür. Ayrıca uluslararası veri transferine ilişkin olarak 108 sayılı Sözleşme'de yer alan hükümlerin kapsamı genişletilerek, yeterli düzeyde

¹⁴⁴ Burada Avrupa İnsan Hakları Sözleşmesi'nin özel yaşamın gizliliği hakkını düzenleyen 8. maddesinin 2. fıkrasındaki sınırlamalara paralel bir düzenleme getirildiği görülmektedir. Küzeci, **a.g.e.**, s. 159.

¹⁴⁵ 108 sayılı Sözleşme, m. 12/1, 2. Söz konusu madde ile gizliliğin korunması amacı dışında gizli ticari kısıtlamalar gibi başka nedenlere dayanılarak veri aktarımını engellemek isteyen devlet uygulamalarının önüne geçmek amaçlanmıştır. Avrupa Komisyonu, "Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", Açıklayıcı Rapor, Strazburg, 21 Ocak 1981, par. 67. (Çevrimiçi) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434>, 12 Nisan 2018

¹⁴⁶ 108 sayılı Sözleşme, m. 12/3.

¹⁴⁷ "Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows", 8 Kasım 2001, (Çevrimiçi) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181>, 12 Nisan 2018.

koruma sağlayamayan üçüncü ülkelere kişisel verilerin aktarımı yasaklanmıştır. 181 sayılı Ek Protokol 8 Kasım 2001’de imzaya açılarak 5 taraf devletin onaylaması ile 1 Temmuz 2004’te yürürlüğe girmiştir. 3 Şubat 2018 itibariyle aralarında Türkiye’nin¹⁴⁸ de bulunduğu 40 devlet tarafından onaylanmış, 7 devlet ise ek protokolü imzalamış ancak onaylama sürecini henüz tamamlamamıştır.

181 sayılı Ek Protokol ile taraf devletlere, 108 sayılı Sözleşme ve Protokol’de belirtilen ilkeleri uygulamaya koyan, iç hukuktaki önlemlere uyulmasını sağlamakla yükümlü ve bağımsız bir ya da daha fazla yetkili makam belirleme yükümlülüğü getirilmiştir. Denetleyici makam kararlarının şikayetlere yol açması halinde bu kararlara karşı yargı yolunun açık olması gerektiği belirtilmiştir. Uluslararası veri aktarımlarına ilişkin olarak ise taraf devletlere, 108 sayılı Sözleşme’ye taraf olmayan bir devlet ya da kuruluşun yetki alanında bulunan bir alıcıya kişisel veri aktarımının, söz konusu devlet ya da kuruluşun yeterli seviyede koruması taahhüdünü arama yükümlülüğü getirilmiştir.

1.3.2.3. 108 sayılı Sözleşme’ye Değişiklik Protokolü

108 sayılı Sözleşme’yi yenileyen Değişiklik Protokolü¹⁴⁹, 18 Mayıs 2018’de Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilmiş ve 25 Haziran 2018 tarihinde imzaya açılmıştır. Değişiklik Protokolü’ne ilişkin ihtiyaç ilk olarak 19 Kasım 2012’de Brüksel’de 108 sayılı Sözleşme’nin güncellenmesi, modernize edilmesine ilişkin önerinin kabul edilmesi ile kabul edilmiştir¹⁵⁰. Toplantıya ilişkin olarak kamuoyu ile paylaşılan bilgi notunda açık bir şekilde Avrupa’nın dünyanın sayılı güçlü veri koruma düzenlemelerinden birine sahip olduğu vurgulanırken, düzenlemelerin tüketici haklarını dijital dünyaya da taşımak adına hızla gelişen teknolojiler ve küreselleşme

¹⁴⁸ Türkiye, işbu protokolü 8 Kasım 2001 tarihinde imzalamış olmasına rağmen söz konusu protokol uzunca bir süre denetleyici bir makam kurulamamış olması sebebi ile ancak 20 Nisan 2016 tarihinde Türkiye Büyük Millet Meclisi’nde kabul edilip 5 Mayıs 2016 tarihli 29703 sayılı Resmî Gazete’de yayımlanarak iç hukuka dâhil edilmiştir.

¹⁴⁹ Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (Çevrimiçi) <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> 9 Eylül 2018.

¹⁵⁰ Avrupa Komisyonu, “Commission to renegotiate Council of Europe Data Protection Convention on behalf of EU”, Bilgi Notu, 19 Kasım 2012, Brüksel, (Çevrimiçi) http://europa.eu/rapid/press-release_MEMO-12-877_en.htm?locale=en 9 Eylül 2018.

eğiliminin göz önünde bulundurularak güncellenmesi gerektiği belirtilmiştir. Bilgi notunda ayrıca 25 Ocak 2012’de Avrupa Komisyonu tarafından kamuoyu ile paylaşılan reform paketine¹⁵¹ atıf yapılmıştır.

Değişiklik Protokolü’nün açıklayıcı raporunda¹⁵², Sözleşme’nin imzaya açılmasından itibaren geçen 35 yıl içerisinde uluslararası veri koruma hukuku bakımından Avrupa Birliği sınırlarını aşarak büyük önem ihtiva ettiği belirtilmiştir. Bununla beraber özellikle insan hakları ve temel haklara yönelik müdahalelerin yeni bilgi teknolojileri ve iletişim teknolojilerinin kullanımının artması ve veri işleme operasyonlarının küresel bir hal alması ile beraber göstermiş olduğu artışın 108 sayılı Sözleşme’nin yenilenmesi ihtiyacını doğurduğu belirtilmiştir. 108 sayılı Sözleşmenin bilgi işlenmesi ve kişisel verilerin korunmasına ilişkin getirmiş olduğu kısıtlamaların farklı menfaatler, temel hak ve özgürlükler arasındaki dengenin dikkatli bir şekilde kurulması amacı taşıdığı belirtilerek, kişisel verilerin korunmasına ilişkin hakkın mutlak bir hak olmadığı tekrardan belirtilmiştir. uluslararası veri akışının modern toplumlar için bir gereklilik olduğu vurgulanırken bu akışın bireylerin temel hak ve özgürlüklerine saygı çerçevesinde yapılması gerektiği belirtilmiştir.

1.3.2.4. Avrupa İnsan Hakları Sözleşmesi

Birleşmiş Milletler Genel Kurul’unda 10 Aralık 1948 günü kabul ve ilan edilen, insanlık tarihinin kilometre taşlarından biri niteliğinde olan “İnsan Hakları Evrensel Beyannamesi” ile insan hakları ve temel özgürlükleri teker teker belirlenmiştir. Ancak İnsan Hakları Evrensel Beyannamesi, devletler bakımından hukuki yönden bağlayıcı olmadığı için, bu bildiride sayılan temel hak ve özgürlükleri tanıyan devletlere kural olarak herhangi bir yükümlülük getirmemektedir¹⁵³. Söz konusu eksikliğin, benzer hak

¹⁵¹ Avrupa Birliği Genel Veri Koruma Tüzüğü’nün oluşturulmasına ilişkin olarak teknolojik gelişmeler ve çevrim içi daha güçlü gizlilik hakkına dair vurgu barındıran reform paketine ilişkin detaylı bilgi için bkz. Aşağıda 1.1. Avrupa Birliği Genel Veri Koruma Tüzüğü.

¹⁵² Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, s. 15.

¹⁵³ İnsan Hakları Evrensel Beyannamesi, Birleşmiş Milletler Genel Kurulunca, oylama sonucunda kabul edilmiş bir karar olup, teknik hukuk anlamında "tavsiye" niteliğindedir; "bağlayıcı" bir etkisi yoktur, bu konuda bkz. Rona Aybay, **Açıklamalı İnsan Hakları Evrensel Bildirisi**, Türkiye Barolar Birliği İnsan Hakları Uygulama ve Araştırma Merkezi, Türkiye Barolar Birliği Yayınları: 113, TBB IHAUM Dizisi: 7, 1. Baskı, Ankara, Aralık 2006, s. 6.

ve özgürlükleri daha da geliştirerek düzenleyen Avrupa İnsan Hakları Sözleşmesi'yle giderilmesi hedeflenmiştir. 20 Mart 1950'de Roma'da imzalanan Avrupa İnsan Hakları Sözleşmesi, 3 Eylül 1953'de 10 devletin onaylama sürecini tamamlaması ile yürürlüğe girmiştir. Türkiye Avrupa İnsan Hakları Sözleşmesi'ni ilk imzalayan devletlerden biridir. Ancak onaylama süreci 18 Mayıs 1954'te tamamlanmıştır.

Öncelikle belirtmek gerekir ki Avrupa İnsan Hakları Sözleşmesi'nde kişisel verilerin korunması müstakil bir hak alanı olarak düzenlenmemiştir. Ancak Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde¹⁵⁴ özel yaşamın gizliliği hakkı düzenlenmiştir. Avrupa İnsan Hakları Sözleşmesi'nde, Birleşmiş Milletler İnsan Hakları Bildirgesi'nde¹⁵⁵ olduğu gibi doğrudan gizlilik (**Privacy**)¹⁵⁶ atfı bulunmamaktadır. Avrupa İnsan Hakları Sözleşmesi'nde “özel hayat ve aile yaşamı” deyimini tercih edilmiştir. Avrupa İnsan Hakları Sözleşmesi'nin ilk taslaklarında 8. madde “**privacy**”

¹⁵⁴ Avrupa İnsan Hakları Sözleşmesi'nin kişinin (i) özel yaşamı, (ii) aile yaşamı, (iii) evi ve (iv) haberleşmesi olmak üzere dört alanda koruma getiren madde 8 hükmü: “1. Her kişi, özel yaşamına ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir. 2. Bu hakkın kullanımına, bir kamu makamı tarafından, ulusal güvenlik, kamu emniyeti ya da ülkenin ekonomik refahı/(esenliği) yararı için, düzensizliğin ya da suçun/suç işlenmesinin önlenmesi için, sağlığın ya da ahlakın korunması için yahut başkalarının haklarının ve özgürlüklerinin korunması için, yasaya uygun olarak getirilen ve bir demokratik toplumda gerekli olanlar dışında/(hariç), hiçbir müdahalede bulunulmayacaktır.” “İnsan Haklarını ve Temel Özgürlükleri Koruma Sözleşmesi” (No.005, “Convention for the Protection of Human Rights and Fundamental Freedoms”), Türkçe çevirisi ve İngilizce metni için bkz. Mehmet Semih Gemalmaz, **İnsan Hakları Belgeleri/Human Rights Instruments**, Cilt 1, 2003, s. 35-59 (Türkçe), s. 299-321 (İngilizce). Daha yakın tarihli olarak, yürürlükteki metnin Türkçe çevirisi ve İngilizce metni için bkz. Mehmet Semih Gemalmaz, **Ulusalüstü İnsan Hakları Usul Hukuku Mevzuatı: Avrupa Konseyi Belgeleri & Avrupa İnsan Hakları Mahkemesi Kuralları Şerhi**, İstanbul, Legal Yayıncılık, Nisan 2006, s. 25-41 (Türkçe), s. 879-896 (İngilizce).

¹⁵⁵ Birleşmiş Milletler İnsan Hakları Bildirgesi m. 12 de “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” ifadesine yer verilmiştir.

¹⁵⁶ “**Privacy**” kelimesinden bundan sonra karşılığı olan “gizlilik” olarak bahsedilecektir. Öğretide “privacy” kelimesinin karşılığı olarak kimi metinlerde “özel yaşamın (ya da hayatın) gizliliği”nin kimilerinde ise “mahremiyet”in kullanıldığı görülmektedir. Mahremiyet, “kişinin herkesle paylaşmayacağı veya herhangi bir kimse ile paylaşmama hakkının bulunduğu olay, inanç ve duygularının, isteği üzerine o kişiyle paylaşılması” durumunu ifade eden “**intimacy**” kelimesine karşılık gelmektedir, bu konuda bkz. Oya Araslı, **Özel Yaşamın Gizliliği Hakkı ve TC Anayasasında Düzenlenişi**, Ankara 1979, (yayınlanmamış doçentlik tezi), s. 6, d.n. 12.; ancak “**privacy**” kavramı ile korunmak istenen değer, bireyin yalnızca mahrem alanını değil mahrem olmayan kamuya açık alanının da içerdiğinden bahisle “**privacy**”nin karşılığı olarak “özel yaşamın gizliliği”nin kullanılması gerektiğine ilişkin görüş de bulunmaktadır, bkz. Küzeci, **a.g.e.**, s. 16.

değişini içermektedir. Ancak 1950 yılına gelindiğinde ise sözleşme taslağında “**privacy**” ifadesi özel hayat anlamına gelen “**private life**” deyişi ile değiştirilmiş ve metin bu hali ile kabul edilmiştir¹⁵⁷. Özel hayata ve aile yaşamına saygı hakkı ile kişisel verilerin korunması hakkı arasındaki ayrımın öneminin yalnızca teoride kaldığı öğretide ifade edilmektedir. Özel hayata ve aile yaşamına saygı hakkı birey merkezli yaklaşımı yansıtmakla birlikte bireyi korumaya yönelik statik bir hak olması nedeni ile negatif koruma¹⁵⁸ gerektirmektedir. Ancak kişisel verilerin korunması ile yüksek oranda dinamik bir koruma öngörmektedir¹⁵⁹.

Avrupa İnsan Hakları Mahkemesi, özellikle 1980’li yılların ortalarından itibaren artan teknolojik gelişmelerin ve konudaki başvuruların etkisi ile gittikçe artan bir yoğunlukta kişisel verilerin korunmasını, Avrupa İnsan Hakları Sözleşmesi’nin sağladığı güvenceler kapsamında ele almaktadır. Avrupa İnsan Hakları Mahkemesi’ne göre Avrupa İnsan Hakları Sözleşmesi, “*güncel koşullar ışığında yorumlanması gereken yaşayan bir enstrüman*”dır¹⁶⁰. Bu görevi üstlenen Avrupa İnsan Hakları Mahkemesi, Avrupa İnsan Hakları Sözleşmesi’ni yorumlarken sosyal değişimleri de kararlarına yansıtmaktadır¹⁶¹. Çeşitli kararlarına da yansıdığı üzere Avrupa İnsan Hakları Mahkemesi’ne göre Avrupa İnsan Hakları Sözleşmesi ile hakların, soyut ya da teorik olarak değil, etkili ve uygulanabilir bir şekilde güvence altına alınması hedeflenmiştir. Bu doğrultuda Avrupa İnsan Hakları Sözleşmesi hükümlerinin sınır ve kapsamını, Avrupa İnsan Hakları Mahkemesi karar ve yorumları ile şekillendirmektedir.

¹⁵⁷ Gloria González Fuster, **The Emergence of Personal Data Protection as a Fundamental Right of the EU**, Belgium, Springer Science & Business, 28 Nisan 2014, s. 82.

¹⁵⁸ “*Pozitif yükümlülükleri negatif yükümlülüklerden ayıran şey şudur ki pozitif yükümlülükler devletlerin pozitif müdahalesini gerektirirken, negatif yükümlülükler müdahaleden imtina etmeyi gerektirmektedir.*” Jean-François Akandji-Kombe, **Avrupa İnsan Hakları Sözleşmesi Kapsamında Pozitif Yükümlülükler: Avrupa İnsan Hakları Sözleşmesinin Uygulanmasına İlişkin Kılavuz Kitap**, çev: Özgür Heval Çınar ve Abdulcelil Kaya, Belçika, 1. Baskı, 2008, s. 11.

¹⁵⁹ Küzeci, **a.g.e.**, s. 84.

¹⁶⁰ Avrupa İnsan Hakları Mahkemesi, Tyrer, Birleşik Krallık’a karşı kararı, Başvuru Numarası 5856/72, Karar Tarihi 28 Nisan 1978, par. 31.

¹⁶¹ Avrupa İnsan Hakları Mahkemesi, Cossey, Birleşik Krallık’a karşı kararı, Başvuru Numarası 10843/84, Karar Tarihi 27 Eylül 1990, par. 35.

Avrupa İnsan Hakları Mahkemesi yıllar içinde verdiği pek çok kararda, kişisel verilerin korunması alanında yer alan temel ilkelerin büyük bir bölümünü, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi kapsamında değerlendirerek önüne gelen olaylar kapsamında uygulamıştır. Özellikle 1980'li yılların ortalarından itibaren kişisel verilerin korunmasına ilişkin hak ihlalleri içeren olayları Avrupa İnsan Hakları Sözleşmesi'nin sağladığı güvenceler kapsamında değerlendirmiştir. Avrupa İnsan Hakları Mahkemesi'ne göre bireysel özerklik ve bilgilerin geleceğini belirleme hakkı, Avrupa İnsan Hakları Sözleşmesi 8. maddesi ile getirilen güvencelerin yorumlanmasında önemli bir temel ilkedir¹⁶².

Bu doğrultuda hukukumuzda da tartışmalı olan özel alan kavramı hakkında Avrupa İnsan Hakları Mahkemesi tarafından yapılan değerlendirme önem teşkil etmektedir. Çeşitli kararlar incelendiğinde özel yaşamın yalnızca kişinin mahrem yaşamı ile sınırlandırılmadığı, başkaları ile ilişki kurduğu alanları da kapsar şekilde yorumladığı görülmektedir. Bu yaklaşımın, kişisel verilerin korunması açısından önemli sonuçları bulunmaktadır. Yukarıda da belirtildiği üzere kişisel veri, kişinin sırları ya da mahremi ile sınırlı olmayıp kişiye ilişkin her türlü bilgiyi kapsamaktadır. Avrupa İnsan Hakları Mahkemesi'nin bu yaklaşımı ile örneğin; kişinin özel fotoğrafları kadar kamusal alandaki görüntü kayıtları da Avrupa İnsan Hakları Sözleşmesi 8. maddesi kapsamında korunmaktadır. Avrupa İnsan Hakları Mahkemesi konuya ilişkin önemli ilk kararını, 6 Eylül 1978'de Klass ve diğerlerinin Almanya'ya karşı yaptığı başvuru üzerine vermiştir. Başvurucuların, Mektup, Posta ve Telekomünikasyonun Gizliliğinin Sınırlandırılması Yasası'nın¹⁶³ Avrupa İnsan Hakları Sözleşmesi'ne aykırılığına ilişkin iddiaları doğrultusunda mahkeme gizli telefon dinlemelerini özel yaşam hakkının ihlali kapsamında değerlendirmiş ve başvurucuları potansiyel mağdur olarak

¹⁶² Avrupa İnsan Hakları Mahkemesi, Pretty, Birleşik Krallık'a karşı kararı, Başvuru Numarası 2346/02, Karar Tarihi 29 Temmuz 2002, par. 61.

¹⁶³ İlgili yasanın 10 maddesinde devlet makamlarının, “özgür demokratik anayasal düzeni”, “devletin varlığını veya güvenliğini” veya “askeri kuvvetlerin güvenliğini” tehdit eden “yakın tehlikelere” karşı korumak üzere postaları açıp denetlemelerine ve telefon görüşmelerini dinlemelerine izin vermektedir. Bu konuda bkz. Avrupa İnsan Hakları Mahkemesi, Klass ve diğerleri, Almanya'ya karşı kararı, Başvuru Numarası 5029/71, Karar Tarihi 6 Eylül 1978, par. 17.

kabul etmiştir¹⁶⁴. Bunun yanında Avrupa İnsan Hakları Mahkemesi başvuruları değerlendirirken kişisel verilerin korunmasını “özel yaşam” kapsamında görmüştür. Kişisel verilerin korunması açısından oldukça önemli olan bireylere ilişkin kişisel bilgilerin resmi makamlarca toplanarak arşivlenmesi¹⁶⁵; telefon görüşmelerine ilişkin kayıtların izlenmesi¹⁶⁶; toplanan verilerin toplanma amacı dışında kullanılması¹⁶⁷; sağlık verilerinin gizliliği¹⁶⁸; emniyet güçleri tarafından parmak izi ve fotoğrafların alınması¹⁶⁹; kişisel verilere erişim hakkı¹⁷⁰; kişisel verilerin gerektiğinden uzun süre tutulması¹⁷¹ konularında vermiş olduğu kararlar yıllar içerisinde Mahkemenin konuya ilişkin yaklaşımını ortaya koymuştur.

Avrupa İnsan Hakları Sözleşmesi’nin 8. maddesinde yer alan özel yaşama saygı hakkının sınırları, aynı maddenin 2. fıkrasında düzenlenmektedir. Bu düzenleme mahkeme tarafından özel yaşama saygı hakkına bir müdahale olduğu tespit edildiğinde, müdahalenin meşruiyet sorunu değerlendirmesinde göz önünde bulundurulmaktadır. 2. fıkra da belirlenen koşul ve ölçütlere uygunluk değerlendirme açısından esas alınmaktadır. Avrupa İnsan Hakları Sözleşmesi’nin 8 (2) hükmü uyarınca özel hayat ve aile yaşamına müdahale, **(i)** burada sınırlı sayımla belirtilmiş

¹⁶⁴ Avrupa İnsan Hakları Mahkemesi, Klass ve diğerleri, Almanya’ya karşı kararı, Başvuru Numarası 5029/71, Karar Tarihi 6 Eylül 1978.

¹⁶⁵ Avrupa İnsan Hakları Mahkemesi, Amann İsviçre’ye karşı kararı, Başvuru Numarası 27798/95, Karar Tarihi 16 Şubat 2000; Avrupa İnsan Hakları Mahkemesi, Rotaru Romanya’ya karşı, Başvuru Numarası 28341/95, Karar Tarihi 4 Mayıs 2001.

¹⁶⁶ Avrupa İnsan Hakları Mahkemesi, Malone, Birleşik Krallığa karşı kararı, Başvuru Numarası 8691/79, Karar Tarihi 2 Ağustos 1984; P.G. ve J.H., Avrupa İnsan Hakları Mahkemesi, Birleşik Krallığa karşı kararı, Başvuru Numarası 44787/98, Karar Tarihi 25 Eylül 2001.

¹⁶⁷ Avrupa İnsan Hakları Mahkemesi, Leander, İsviçre’ye karşı kararı, Başvuru Numarası 9248/81, Karar Tarihi 26 Mart 1987.

¹⁶⁸ Avrupa İnsan Hakları Mahkemesi Z., Finlandiya’ya karşı kararı, Başvuru Numarası 22009/93, Karar Tarihi 25 Şubat 1997; Avrupa İnsan Hakları Mahkemesi, M.S., İsveç’e karşı kararı, Başvuru Numarası 20837/92, Karar Tarihi 27 Ağustos 1997.

¹⁶⁹ Avrupa İnsan Hakları Mahkemesi, Murray, Birleşik Krallık’a karşı kararı, Başvuru Numarası 14310/88, Karar Tarihi 28 Ekim 1994.

¹⁷⁰ Avrupa İnsan Hakları Mahkemesi, Gaskin, Birleşik Krallık’a karşı kararı, Başvuru Numarası 10454/83, Karar Tarihi 7 Temmuz 1989.

¹⁷¹ Avrupa İnsan Hakları Mahkemesi, S. ve Marper, Birleşik Krallığa karşı kararı, Başvuru Numarası 30562/04, Karar Tarihi 4 Aralık 2008

amaçlardan¹⁷² bir ya da birkaçına yönelik; **(ii)** yasada öngörölmüş ve **(iii)** aynı zamanda demokratik toplum için gerekli ve öngörölen amaç ile orantılı olması durumunda meşru sayılmaktadır. Belirtmek gerekir ki Avrupa İnsan Hakları Mahkemesi, konuya ilişkin pek çok kararında, madde 8 (1)'in ihlalini 2. fıkra hükümleri uyarınca meşru görmektedir. Bunun nedeni olarak söz konusu meşru amaçların oldukça geniş belirtilmesi gösterilebilir¹⁷³.

Avrupa İnsan Hakları Sözleşmesi kapsamında kişisel verilerin korunmasına ilişkin olarak uygulanabilecek genel ilkeler belirlenmemektedir. Ancak söz konusu ilkelerin uygulama alanı ve kapsamında Avrupa İnsan Hakları Mahkemesi kararları yol gösterici niteliktedir. Avrupa İnsan Hakları Mahkemesi, önüne gelen pek çok başvuruda ilgili kişinin izni ya da icazeti olmaksızın kişisel verilerinin işlenmesi, toplanması, sınırsız ya da gerektiğinden uzun süre tutulması, meşru amacın açık bir şekilde belirtilmemesi ve gereken güvencelerin sağlanması hallerinde ihlalin gerçekleştiğine karar vermektedir. Ancak Avrupa İnsan Hakları Mahkemesi kararları her ne kadar kişisel verilerin korunmasına ilişkin geniş kapsamlı değerlendirme yapıyor ve genel ilkelerin korunmasını hedefliyor olsa da günümüzde özellikle özel sektörde artış gösteren kişisel verilerin işlenmesi faaliyetleri ve neden oldukları ihاللer bakımından Avrupa İnsan Hakları Sözleşmesi'nin yeterli oranda güvence sağlayıp sağlayamayacağı tartışmalıdır¹⁷⁴.

1.3.3. Birleşmiş Milletler

Kişisel verilerin korunması hukukuna ilişkin çalışmaları olan bir diğer uluslararası merci de Birleşmiş Milletler'dir. Bir üst hukuk normu olarak Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi'nin¹⁷⁵ 12. maddesinde, kişilerin mahremiyet, aile ve konut dokunulmazlığı güvence altına alınarak bu haklara gelecek olası saldırılarda kişilerin hukuki korumadan yararlanma hakkı “... *Hiç kimse, özel yaşamına,*

¹⁷² Madde kapsamında bu amaçlar, ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması olarak sayılmıştır.

¹⁷³ Küzeci, **a.g.e.**, s. 154.

¹⁷⁴ **a.e.**, s. 143.

¹⁷⁵ “Evrensel İnsan Hakları Beyannamesi” (“Universal Declaration of Human Rights”), Birleşmiş Milletler Genel Kurulunun 10 Aralık 1948 tarih ve 217 A(III) sayılı kararıyla kabul ve ilan edilmiştir.

ailisine/(aile yaşamına), konutuna ya da haberleşmesine yönelik keyfi müdahalelere ya da onur/(şeref) ve şöhretine yönelik saldırılara maruz bırakılmayacaktır. Herkesin, bu tür müdahale ya da saldırılara karşı kanun ile korunma hakkı vardır...” ifadesiyle¹⁷⁶ hükme bağlanmıştır. Birleşmiş Milletler’in 16 Aralık 1966 tarihli Sivil ve Siyasi Haklar Hakkında Uluslararası Sözleşmesi’nin 17. maddesinde de aynı koruma hükmü yer almaktadır¹⁷⁷.

1990 yılında ise Birleşmiş Milletler, Kişisel Veri Dosyalarının Bilgisayar Aracılığıyla İşlenmesinde Genel Tavsiye İlkeleri yayımlamıştır¹⁷⁸. Bu metin ile getirilen genel ilkeler¹⁷⁹ ile üye ülkelerin, bilgisayarla kişisel veri işleme konusunda yapacakları düzenlemelerde ortak olarak dikkate alınması tavsiye edilen hususlar belirtilmekte, bu ilkelerin uygulama usullerinin belirlenmesi üye ülkelerin inisiyatifine bırakılmaktadır.

1.3.4. Amerika Birleşik Devletleri Yaklaşımı

Günümüzde kişisel verilerin korunmasına ilişkin olarak hukuki metinlerin hazırlanmasında öncü ve yönlendirici rol her ne kadar Kıta Avrupası’nda olsa da kişisel verilerin korunması ve mahremiyet kavramları ilk olarak 1890 yılında, Samuel Warren ve Louis Brandeis isimli hukukçular tarafından Harvard Law Review’de yayınlanan The Right to Privacy¹⁸⁰ başlıklı makalede “yalnız bırakılma hakkı” (**right**

¹⁷⁶ Yararlanılan kaynak ve Türkçe çevirisi ile İngilizce orijinal metni için bkz. Mehmet Semih Gemalmaz, **İnsan Hakları Belgeleri/Human Rights Instruments**, Cilt 4, Birleşmiş Milletler-Birinci Bölüm/United Nations-First Part, İstanbul, Boğaziçi Üniversitesi Yayınevi, 2004, s. 3-23 (Türkçe) ve s. 353-361 (İngilizce).

¹⁷⁷ Birleşmiş Milletler, “International Covenant On Civil And Political Rights”, no: 14668, 16 Aralık 1966.

¹⁷⁸ Birleşmiş Milletler, “Guidelines Concerning Computerized Personal Data Files”, Resolution no: 45/95, 14 Aralık 1990.

¹⁷⁹ Kişisel verilerin korunması konusunda pek çok metin ile paralellik arz edecek şekilde belirlenen ilkeler ile ulusal mevzuatlarda yer alması gereken temel esaslar belirtilmiştir. Bu ilkeler, hukuka uygunluk ve dürüstlük ilkesi (m. 1), verilerin doğruluğu ilkesi (m. 2), amacın belirliliği ilkesi (m. 3), ilgili kişinin erişimi ilkesi (m. 4), ayrımcılık yapılamaması ilkesi (m. 5- m. 6), veri güvenliği ilkesi (m. 7), denetim ve yaptırım ilkesi (m. 8), verilerin sınır ötesi akışı ilkesi (m. 9) olarak 45/95 sayılı Birleşmiş Milletler Kişisel Veri Dosyalarının Bilgisayar Aracılığıyla İşlenmesinde Genel Tavsiye İlkeleri içerisinde yer almaktadır.

¹⁸⁰ Samuel D. Warren, Louis D. Brandeis, “The Right to Privacy”, **Harvard Law Review**, Cilt 4, Sayı 5, Boston, 15 Aralık 1890, s. 1, (Çevrimiçi), http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html, 12 Nisan 2018.

to be let alone) kapsamında tartışılmıştır. Makalede hukukun bireyin haklarına ilişkin getirmiş olduğu koruma alanı mülkiyetten itibaren takip edilerek gelişen teknolojilerle birlikte kişiliğin bir parçası olan gizliliğin bir hak olarak tanımlanmasının gelişmiş modern toplumlar için vazgeçilmez bir unsur olduğu belirtilmektedir. Ancak Amerika Birleşik Devletleri'nde özel yaşamın korunmasına ilişkin atılan bu adımlar, hukuki yapılanmanın ifade özgürlüğü temelinde inşa edilmiş olması sebebi ile kısıtlı kalmıştır.

1970'li yıllara gelindiğinde ise Avrupa'da olduğu gibi Amerika Birleşik Devletleri'nde de kişisel verilerin korunması yönünde bazı düzenleme girişimlerinde bulunulmuştur. Amerika Birleşik Devletleri Kongresi, 1970 yılında Adil Kredi Raporlama Yasası'nı kabul ederek, bireylere kendilerine ilişkin kredi raporlarını görme ve yanlış bilgileri düzelttirme hakkını tanımıştır¹⁸¹. Takip eden yıllarda ise bilgisayarların özel yaşamın gizliliği hakkı üzerindeki etkilerini araştıran bir komisyon kurulmuş ve komisyonun 1973 yılında sunduğu raporda Adil Enformasyon Uygulama Kuralları¹⁸² adı altında beş temel ilke belirlenmiştir. Bu ilkeler uyarınca **(i)** gizlenmiş kişisel veri saklama sistemlerinin olmaması, **(ii)** kişilerin kendileri hakkında hangi verilerin kayıt altına alındığını ve bunların nasıl kullanıldığını öğrenme yolu bulunması, **(iii)** kişilerin kendileri hakkında belirli bir amaç için toplanmış verilerin, rızaları olmaksızın başka amaçlar için kullanılmasını önleme hakları olması, **(iv)** kişilerin kendileri hakkındaki belirlenebilir bilgilerin kayıtlarını düzeltme ya da değiştirme olanakları bulunması, **(v)** kişisel verilerin kayıtlarını oluşturan, muhafaza eden, kullanan ya da yayınlayan kuruluşların, verilerin kendi hedefleri için kullanımındaki güvenliğini sağlama ve kötüye kullanımını önleyemeye yönelik

¹⁸¹ Amerika Birleşik Devletleri'nde kabul edilerek federal düzeyde etki gösteren Adil Kredi Raporlama Yasası'nda banka ve kredi kuruluşlarının müşteri kredi bilgilerini hangi hallerde hukuka uygun olarak kullanabileceği düzenlenmektedir. Bankacılık sisteminin adil ve doğru kredi raporlamasına bağlı olduğu belirtilen Yasa ile konuya ilişkin bir mahkeme emrinin varlığı, ilgili kişinin doğrudan kendisinin bilgileri açıklamış olması ve kredi kartı kullanımı, sigorta, iş ilişkisinin kurulması gibi örneklendirilen meşru ticari amaçlar haricinde kredi raporlarının kullanımı yasaklanmıştır. Ayrıca kredi kuruluşlarının verileri doğrulamak ve düzenlemek için etkin bir çaba göstermesi gerektiği belirtilmiştir. Adil Kredi Raporlama Yasası'nı, Adil Kredi Faturalandırma Yasası, Adil Borç Toplama Uygulamaları Yasası, Borç Toplama Yasası, Telefonda Pazarlama ve Tüketici Dolandırmaları ve İstisnaları Önlenmesi Yasası izlemiştir. Bu konuda bkz. Harry Henderson, **a.g.e.**, s. 52-54.

¹⁸² Department of Health, Education and Welfare of the United States of Amerika, "Code of Fair Information Practices", 1973.

tedbirleri alması gerektiği saptanmıştır. Ancak raporda belirlenen ilkeler Amerika Birleşik Devletleri'nden çok Kıta Avrupası'nda sahiplenilmiş ve tartışma alanı bulmuştur¹⁸³. Rapor tarihinden kısa bir süre içerisinde Avrupa'da pek çok devlet bu temel ilkelere dayanan düzenlemelere iç hukuklarında yer verirken 1974 yılında Amerika Birleşik Devletleri Özel Yaşamın Gizliliği Yasası kabul edilmiş ancak sınırlı bir uygulama alanı bulması nedeni ile eleştirilmiştir¹⁸⁴.

Amerika Birleşik Devletleri'nde kurumsallaşmış bir veri koruma düşüncesi halen uygulamaya geçmemiş olup kişisel verilerin korunması anayasal bir hak olarak da korunmamaktadır. Amerika Birleşik Devletleri'nde ağırlıklı olarak kişisel verilerin korunması hakkı, özel yaşamın gizliliği hakkının özel bir görünümü olarak nitelendirilmektedir.

Amerika Birleşik Devletleri'nde kişisel verilerin korunmasına ilişkin olarak güdülen bu farklı yaklaşım hala süregelmektedir. OECD Rehber İlkeleri, Amerika Birleşik Devletleri tarafından 1981 yılında imzalanmış ancak iç hukuka dâhil edilmemiştir. Amerika Birleşik Devletleri yasaları arasında kişisel verilerin korunmasını özel olarak düzenleyen kapsayıcı bir yasal metin bulunmamaktadır. Buna karşın federal düzeyde sektör bazlı düzenlemeler¹⁸⁵ bulunmaktadır.

¹⁸³ Simson Garfinkel, **Database Nation: The Death of Privacy in the 21st Century**, O'Reilly, Amerika Birleşik Devletleri, Ocak 2000, s. 8.

¹⁸⁴ 1974 Özel Yaşamın Gizliliği Yasası ve Adil Enformasyon Uygulama Kuralları ile belirlenen ilkelerin uygulamaya dönüştürülmesi amaçlanmıştır. Ancak kişisel verilerin kurumların günlük işleri için kullanılması, nüfus müdürlüğü gibi devlet kurumları tarafından kullanılması, tarihi ve istatistikler amaçlar için kullanılması gibi haller için düzenlemelerde istisnalar bulunması ilkelerin etkili bir şekilde uygulanmasına engel oluşturmıştır. Bu durum ise öğretilerde eleştirilmiştir. Eleştiriler için bkz. Harry Henderson, **a.g.e.**, s. 60.

¹⁸⁵ Kişisel verilerin korunmasına ilişkin olarak sektör bazlı yaklaşım ve düzenlemeler içerisinde en çok mali işlemler, telekomünikasyon ve video hizmetleri sektörlerinde dikkat çekmektedir. Düzenlemelere örnek olarak, 1970 tarihinde kabul edilen ve 1996 tarihinde güncellenen Adil Kredi Rapor Etme Hakkındaki Kanun (Fair Credit Reporting Act); 1986 tarihli Elektronik Komünikasyon Mahremiyeti Hakkında Kanun (The Electronic Communications Privacy Act); 1984 yılında kabul edilen Kablolu İletişim Politikası Hakkında Kanun (The Cable Communications Policy Act); video kiralama ve satın alma kayıtlarının ifşasına karşı koruma sağlayan 1988 tarihli Video Mahremiyetini Koruma Kanunu (The Video Privacy Protection Act); 1988 tarihli işverenlerin yalan detektörleri ve bu detektörlerin test sonuçlarını kullanmasına yasak getiren Çalışanların Poligraf Kullanımına Karşı Korunması Hakkındaki Kanun (The Employee Polygraph Protection Act); 1974 tarihli öğrenciler hakkında tutulan kayıtların doğruluk ve gizliliğini düzenleyen Ailenin Eğitim Hakları ve Mahremiyeti Hakkındaki Kanun (The

Temelde yer alan Avrupa Birliği ve Amerika Birleşik Devletleri arasındaki kişisel verilerin korunması hakkına ilişkin yaklaşım farklılıkları özellikle uluslararası veri aktarımları bakımından pek çok problem yaratmaktadır. Avrupa Birliği’nde yer alan kişisel verilerin korunmasına ilişkin muhafazakâr bakış açısı ve sağlanan kapsamlı korumanın kişisel verilerin aktarımı söz konusu olduğunda aktarılabilecek üçüncü ülkede de şart koşuluyla olması düzenlemelerin Avrupa Birliği dışında da etki doğurmasını kaçınılmaz kılmıştır.

Teknoloji ve bilgi kaynakları konusunda öncü bir rol üstlenen Amerika Birleşik Devletleri, kişisel verilere daha ziyade ekonomik bir değer atfederek Avrupa ülkelerinin aksine verinin serbest dolaşımına ilişkin olarak getirilen her türlü sınırlandırmanın ekonomik gelişmeleri engelleyerek küreselleşmeye zarar vereceği endişesini taşımaktadır¹⁸⁶. Bu uyumsuzluk Amerika Birleşik Devletleri’nde yerleşik teknoloji şirketlerin iş süreçlerinde ve operasyonlarında sorun yaratmaktadır. Bu doğrultuda kısmen devlet destekli bir düzenleme türü olan çeşitli mekanizmalar altında Amerika Birleşik Devletleri merkezli şirketler belirli kurallara uymayı taahhüt ederek Avrupa Birliği vatandaşlarının kişisel verilerini Avrupa Birliği Veri Koruma Yönergesi uyarınca Amerika Birleşik Devletleri’ne aktarabilme olanağına sahip olabilmektedirler¹⁸⁷. Ancak Safe Harbor Kararı olarak adlandırılan bu kurallar bütünü altında yapılan uluslararası veri aktarım faaliyetleri 2015 yılında bir kırılma

Family Educational Rights and Privacy Act); 1991 tarihli Telefon Kullanıcılarının Korunması Hakkındaki Kanun (Telephone Consumer Protection Act); 1994 tarihli Şoförlerin Gizliliğinin Korunması Kanunu (Driver’s Privacy Protection Act); 1996 tarihli Telekomünikasyon Kanunu (Telecommunications Act); 1996 tarihli Sağlık Sigortacılığının Taşınabilirliği ve Hesap Verebilirliği Hakkındaki Kanun (The Health Insurance Portability and Accountability Act); 1998 tarihli Çocukların Online Mahremiyetinin Korunması Hakkındaki Kanun (Children’s Online Privacy Protection Act); 1999 tarihli Finansal Hizmetlerin Modernizasyonu Hakkındaki Kanun (The Financial Services Modernization Act).

¹⁸⁶ Alison White, “Control of Transborder Data Flow: Reactions to the European Data Protection Directive”, **International Journal of Law and Information Technology**, Oxford University Press, Cilt 5, Sayı 2, 1997, s. 233.

¹⁸⁷ “Yeterli” düzeyde korumaya ilişkin yoğun tartışmaların akabinde 2000 yılında Amerika Birleşik Devletleri ve Avrupa Birliği arasında **sui generis** bir anlaşmaya varılmıştır. Avrupa Komisyonu’nun “yeterlilik” kararı olan bu uzlaşi “Bağışıklık Sözleşmesi” (Safe Harbor) olarak Türkçe’ye çevrilebilir. Safe Harbor, kişisel verilerin korunması alanında farklı sistemler arasında uzlaşi sağlanmasının önemli bir örneği olarak gösterilmektedir. Bu konuda bkz. Küzeci, **a.g.e.**, s. 194. Bu karar kapsamında Amerika Birleşik Devletleri ve Avrupa Birliği arasında uzlaşılmış olan veri koruma ilkeleri yer almakla birlikte oluşturulacak programın Amerikan Ticaret Bakanlığı yardımıyla yürütülmesi öngörülmüştür.

yaşamıştır¹⁸⁸. Avrupa Birliği’nden, Amerika Birleşik Devletleri’ne aktarılan kişisel verilere Amerika Birleşik Devletleri yetkilileri tarafından erişim sağlanıyor ve verilerin ulusal güvenliğin korunması için kesinlikle gerekli olanın ötesinde ve aktarma amacıyla bağdaşmayan biçimde işleniyor olması gerekçeleri ile Avrupa Birliği Adalet Divanı, Safe Harbor Kararı’nın geçersizliğine hükmetmiştir. Bu karar sonrasında daha kapsamlı bir mekanizma için çalışmalar yürütülmüştür. Çalışmalar sonucunda 12 Temmuz 2016 tarihinde uzmanlarca Safe Harbor’ın üstüne atılmış büyük bir adım olarak ancak Avrupa Birliği standartlarında “yeterli düzeyde” bir veri korumanın üçüncü ülkeler bakımından aranmıyor olması iddiası ile eleştirilen¹⁸⁹ Privacy Shield Kararı¹⁹⁰ kabul edilmiştir. Bu karar altında uluslararası veri aktarım şartlarına ilişkin yeni mekanizma öngörülmüştür.

¹⁸⁸ Avusturyalı bir Facebook kullanıcısı ve hukuk öğrencisi olan Max Schrems, Snowden’ın gizli dinleme faaliyetlerini ifşa etmesinin ardından Facebook’un Avrupa Birliği vatandaşı olan kullanıcıların kişisel verilerini toplamasına karşı şikâyetinde bulunmuş ve bu şikâyet sonucunda Avrupa Adalet Divanı 6 Kasım 2015 tarihli C-362/14 sayılı kararı ile Safe Harbor Kararı’nın geçersizliğine hükmetmiştir. Avrupa Adalet Divanı, Maximillian Schrems, Data Protection Commissioner’a karşı kararı, C-362/14, 6 Ekim 2015, (Çevrimiçi) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>, 13 Nisan 2018.

¹⁸⁹ Article 29 Working Party, “Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision”, WP 238, Görüş, 13 Nisan 2016, s. 33.

¹⁹⁰ Avrupa Birliği ve Amerika Birleşik Devletleri arasındaki ticaretin desteklenmesine ilişkin olarak Avrupa Komisyonu ve Amerika Birleşik Devletleri Ticaret Komitesi tarafından tasarlanan kurallar bütünü olan Privacy Shield 1 Ağustos 2016’da işletilmek üzere 12 Temmuz 2016 tarihinde kabul edilmiştir. Privacy Shield resmi internet sitesi için bkz. (Çevrimiçi) <https://www.privacyshield.gov/welcome>, 21 Nisan 2018.

İKİNCİ BÖLÜM

AVRUPA BİRLİĞİNDE KİŞİSEL VERİLERİN KORUNMASI

2.1. Genel Olarak

1957 yılında imzalanan Roma Antlaşması ile kurulan Avrupa Ekonomik Topluluğu¹ temelde malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımı olmak üzere dört temel düşünce üzerine kurulmuştur. 1985 yılında Avrupa Komisyonu tarafından Konseye yapılan çağrı ve 1986 yılında kabul edilen Avrupa Tek Senedi ile ortak pazar düşüncesinin somutlaşması adına, ortak pazarı engelleyen fiziki, teknik ve mali hususların 1992 yılına kadar kaldırılması öngörülmüştür².

Bu dört temel hedefin yerine getirilmesinde kişisel verilerin toplanması, işlenmesi ve aktarımının devletler arasında gerçekleşmesi doğal bir sonuç olarak ortaya çıkmaktadır. Nitekim arz ettiği değerle beraber korunması gereken kişisel veriler için yeknesak bir yaklaşım zaruri hale gelmiştir. Avrupa Birliği'nde kişisel verilerin korunmasını amaçlayan kurallar, bilgi teknolojilerinin gelişimi ile beraber Avrupa Birliği içinde ortak pazarın gereklerini göz önünde bulundurarak ve serbest veri akışını temel haklara uygun olarak gerçekleştirebilmek amacı ile düzenlenmiştir. Bu kuralların tesisi ile birlikte güdülen temel amaç, Avrupa Birliği üye devletleri arasında veri akışının bireylerin temel hak ve özgürlüklerine zarar vermeden sağlanmasıdır. Başka bir deyişle söz konusu kurallar menfaatler arası bir denge kurmak amacı ile tesis edilmiştir. Zira Avrupa Birliği üye devletleri, Maastricht Antlaşması³ birinci başlıkta 2. maddenin f fıkrasında belirtilen ve 4 Kasım 1950'de Roma'da imzalanan Avrupa

¹ Roma Antlaşması ile kurulan Avrupa Ekonomik Topluluğu, 1992 yılında imzalanan Maastricht Antlaşması ile Avrupa Topluluğu ismini almıştır. Avrupa Birliği'nin üç sütunlu yapısında Avrupa Atom Enerjisi Topluluğu ve Avrupa Kömür ve Çelik Topluluğu ile birlikte ilk sütun olan Topluluklar Sütununu oluşturmakta; ikinci sütununu, "Ortak Dışişleri Güvenlik Politikası"; üçüncü sütununu ise "Adalet ve İçişleri" teşkil etmektedir. Üç sütunlu bir yapıya dayanan hukuki ve siyasal bir varlık olarak Avrupa Birliğine ilk defa bu anlaşma ile değinilmiştir, bkz. Ahmet M. Güneş, **Avrupa Birliği Hukukuna Giriş**, Güncellenmiş 3. Baskı, Ekin Basım Yayın Dağıtım, Ankara, 2017, s. 4.

² Gülören Tekinalp, Ünal Tekinalp, **Avrupa Birliği Hukuku**, 2. Basım, İstanbul, Beta, 2000, s. 12, 13.

³ 1991 yılında imzalanan ve 1 Ocak 1994'te yürürlüğe giren Avrupa Birliği Anlaşması Maastricht'e imzalandığı için bu adla anılmaktadır. Orijinal adı Treaty on European Union olan ve 9 Temmuz 1992'de Avrupa Birliği Resmî Gazetesi'nde yayımlanan metni için bkz. (Çevrimiçi) <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:1992:191:FULL&from=EN>, 4 Nisan 2018.

İnsan Hakları Sözleşmesi'nde garanti altına alınan, üye devletlerin ortak anayasal geleneklerinden kaynaklanan ve topluluk hukukunun genel prensipleri olarak kabul edilen temel haklara saygı göstermeyi taahhüt etmişlerdir. Bu bağlamda Avrupa Birliği'nden dünyaya yayılan veri koruma ekolünün bir önceki bölümde ifade edilen enstrümanlarına ek olarak, üye devletler tarafından benimsenmesi gereken asgari veri koruma ölçütlerinin belirtildiği Avrupa Birliği Veri Koruma Yönergesi'ne ve bu asgari kriterlerin daha kapsamlı bir şekilde düzenlendiği ve doğrudan Avrupa Birliği üye devletlerinin iç hukuklarına etki eden Avrupa Birliği Genel Veri Koruma Tüzüğü'ne ilişkin açıklamalara aşağıda yer verilecektir.

2.2. Avrupa Birliği Veri Koruma Yönergesi

Kişisel verilerin korunmasına ilişkin olarak kilometre taşı niteliğinde önemli metinlerden biri Avrupa Birliği Veri Koruma Yönergesi'dir⁴. Gerek kişisel verilerin korunmasına ilişkin ihtiva ettiği ilkeler gerekse birlik dışı veri aktarımına dair getirdiği düzenlemeler itibariyle Yönerge'nin Avrupa Birliği sınırlarını aşan bir düzenleme olduğunu söylemek mümkündür. Yönerge'nin Avrupa Birliği dışı etkileri ilk olarak Avrupa Birliği üyesi olmayan Avrupa ülkelerinde gözlemlenmiştir. 1999 yılında Liechtenstein, Norveç, İzlanda gibi Avrupa Ekonomik Topluluğu üyesi ülkeler de Yönerge ile bağlı kılınmıştır⁵. Bununla beraber yeterli koruma sağlamayan ülkelere veri aktarımını yasaklayan hüküm nedeniyle Avrupa Birliği dışındaki pek çok ülke de benzer içerikteki düzenlemeleri kabul etmek durumunda kalmıştır.

Avrupa Birliği hukuku kapsamında yönergeler, şekil ve yöntemler açısından yetkiyi ulusal kurumlara bırakarak, devletleri *varılacak sonuçlar* bakımından bağlamaktadır⁶. Bu bakımdan yönergeler, Avrupa Birliği üyesi ülkeler açısından bağlayıcı nitelik taşımakla birlikte doğrudan iç hukuklarına re'sen etki etmemektedirler. Üye devletler,

⁴ Bu bölümden itibaren ilgili yönergeden "Avrupa Birliği Veri Koruma Yönergesi" ya da kısaca "Yönerge" olarak bahsedilecektir.

⁵ Avrupa Ekonomik Topluluğu Ortak Komitesi (EEA Joint Committee), "Decision of the EEA Joint Committee amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement" No. 83/1999, Brüksel, 25 Haziran 1999, yayımlandığı Avrupa Birliği Resmi Gazetesi no: L296, Tarih 23 Kasım 2000.

⁶ Avrupa Birliği'nin İşleyişi Hakkında Antlaşma m. 288/3.

yönergelerde belirlenen amaçlar doğrultusunda ulusal düzeyde bir düzenleme yapma yetkisine sahiptirler⁷.

Avrupa Birliği Veri Koruma Yönergesi'nin hazırlanmaya başlandığı ve kabul edildiği dönemlerde aslında Avrupa Birliği ülkelerinin bazıları hali hazırda iç hukuklarında Avrupa Konseyi'nin 108 sayılı Sözleşmesi ve OECD Rehber İlkeleri doğrultusunda oluşturdukları kişisel verilerin korunmasına ilişkin düzenlemeleri bulundurmakta idi⁸. Ancak Yönerge ile kişisel verilerin korunması alanında üye ülkeler arasında yeknesak bir yaklaşım tesis etme amacı güdülmüştür. Gerçekten de Yönerge öncesi dönemdeki üye ülkeler arası farklı yaklaşımlar 1993 yılında yürürlüğe giren Maastricht Antlaşması'nın getirdiği "tek iç pazar" düşüncesi önünde engel teşkil etmekteydi. Yönerge ile tek iç pazar dairesinde verilerin serbest dolaşımı ve bu transferlerin bireylerin zarar görmeden sağlanması amaçlanmıştır⁹. Bilgi teknolojilerindeki katlanarak artan gelişmeler ile kişisel verilerin toplanması, işlenmesi, saklanması ve dolaşımının bir gereklilik arz etmesi ile birlikte kolaylaşması, diğer yanda Avrupa'da gelişen ekonomik ve sosyal birlikteliğinin birlik ülkeleri arası kişisel veri akışını arttırması kişisel verilerin korunmasına ilişkin ortak bir yaklaşımı elzem kılmıştır¹⁰.

1990 yılında Avrupa Komisyonu kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımı hakkında bir yönerge taslağı hazırlamıştır. Ancak hazırlanan yönerge taslağı kapsamı konusunda uzlaşının sağlanması kolay olmamıştır. Üye devletlerde benimsenen kişisel verilerin korunmasına ilişkin farklı yaklaşım ve koruma seviyeleri, yönerge taslağının olgunlaşma sürecindeki tartışmalarda da etkili olmuştur. Almanya, kendi ülkesinde var olan yüksek düzeydeki korumanın birlik içine sirayet etmesi gerektiği düşüncesini savunurken, Birleşik Krallık, Hollanda, İrlanda ve Danimarka ise 108 sayılı Sözleşme'nin üye devletlerce onaylanmasının zorunlu hale getirilmesinin yeterli olacağını savunmuştur. Bununla birlikte özel sektörden toplanan

⁷ Yönergelerin hukuksal niteliğine ilişkin olarak bkz. Güneş, **a.g.e.**, s. 123-130.

⁸ Andrew Charlesworth, "The Governance of the Internet in Europe", **The Internet, Law and Society**, haz. Yaman Akdeniz, Clive Walker, David Wall, İngiltere, Pearson Education Limited, 2000, s. 63.

⁹ Paul B. Lambert, **Understanding the New European Data Protection Rules**, CRC Press, Amerika Birleşik Devletleri, 2018, s. 84.

¹⁰ Paul M. Schwartz, "The EU-U.S. Privacy Collision: A Turn To Institutions and Procedures", **Harvard Law Review**, Cilt 126, Sayı 7, 2013, s. 1971-1973.

görüşlerde ise bankacılık, tıbbi araştırma, pazarlama gibi alanlarda etkinlik gösteren kurum ve kuruluşlar kişisel verilerin kullanımına getirilecek kısıtlamalara ilişkin endişelerini belirtmişlerdir. Bu doğrultuda 1990 yılında hazırlanan ilk taslağın yoğun eleştiriler alması üzerine 1992 yılında ikinci bir taslak oluşturulmuştur. Nihai metinde belirli bir ulusal sistemin oransız etkisi görülmemektedir¹¹. Üye devletlerden Almanya, Birleşik Krallık, Hollanda ve Fransa’da yürürlükte olan kişisel veri koruma düzenlemelerinin ortak noktalarının yansıtıldığı metin 95/46 sayılı “Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımı Yönergesi” olarak 24 Ekim 1995 tarihinde kabul edilerek 25 Ekim 1998 tarihinde yürürlüğe girmiştir.

2.2.1. Amaç

Avrupa Birliği Veri Koruma Yönergesi’nin giriş bölümünde de belirtildiği üzere kabul edilmesindeki temel amaç Avrupa Birliği ülkeleri arasında veri koruma yaklaşımlarını yeknesaklaştırmak, farklı yaklaşım ve tanımlamaları uyumlulaştırmaktır¹². Yönerge, bu uyumlulaştırmayı yaparken aynı anda hem verinin serbest dolaşımını engellememeyi hem de kişisel verilerin korunmasına dair temel ilkeleri korumayı hedeflemektedir. Diğer bir deyişle, verinin dolaşımının yaratacağı fayda ile kişisel verilerin korunmasına ilişkin bireylerin menfaatleri kapsamında dengenin sağlanması amaçlanmaktadır. Bu amaç Yönerge’nin 1. maddesinde, “*kişisel verilerin işlenmesi bakımından, bireylerin temel hak ve özgürlüklerinin korunması ve üye devletlerce verilerin serbest dolaşımını engelleyecek düzenlemeler yapılmasının önüne geçilmesi*” şeklinde ifade edilmektedir. Bu doğrultuda bütün üye devletlerde geçerli olacak asgari veri koruma ölçütleri Yönerge ile belirlenmektedir¹³.

¹¹ Andrew Charlesworth, “Clash of the Data Titans? US and EU Data Privacy Regulation”, **European Public Law**, Kluwer Law International, Cilt 6, Sayı 2, 2000, s. 256-257; Yönerge’nin kabul edilmesi öncesindeki tartışmalara ilişkin olarak ayrıca bkz. Spiros Simitis, “From the Market to the Polis: The EU Directive on Protection of Personal Data”, **Low Law Review**, University of Iowa Collage of Law, Iowa City, Cilt 80, 1994, s. 445.

¹² Yönerge, Giriş Bölümü, par. 1, par. 4, par. 7 ve par. 8.

¹³ Christopher Kuner, **European Data Protection Law: Corporate Compliance and Regulation**, 2. Baskı, Oxford University Press, Amerika Birleşik Devletleri, 2007, s. 20.

2.2.2. Kapsam

Avrupa Birliđi Veri Koruma Yönergesi'nin kapsamı ve uygulama alanı 3. maddesinde ikili bir ayrıma gidilerek açıklanmaktadır. İlk olarak hangi veri işleme faaliyetlerinin Yönerge kapsamında düzenlendiđi belirtilmektedir. Kişisel verilerin kısmen veya tamamen otomatik araçlarla işlenmesi halinde Yönerge hükümlerinin uygulanacağı ifade edilmektedir¹⁴. Kişisel verilerin otomasyon sistemlerinin kullanıldığı yöntemlerle işlenmesi halinde verilerin otomatik işlenmesinden bahsedilmektedir. Bunun yanında kişisel veriler otomatik araçlarla işlenmese dahi, bu verilerin kişisel verilere kolayca ulaşmaya izin verecek şekilde belli bir kritere göre yapılandırılmış olması, dosyalama sisteminin bir parçasını veya bölümünü oluşturması amacıyla işlenmesi durumunda da Yönerge hükümlerinin uygulanacağı kabul edilmektedir.

Tamamen veya kısmen otomatik olma koşuluna ilişkin olarak faaliyetler bakımından sınırlı ve kesin bir tanım bulunmamaktadır. Bununla birlikte, Yönerge'nin genel amacı doğrultusunda, “tamamen veya kısmen otomatik” olan faaliyetlerin neler olduğu somut olaylar bazında mümkün olduğunca geniş yorumlanmaktadır. Aksi yönde Birleşik Krallık'ta, Durant ile Financial Services Authority arasında görülen davada¹⁵ bir banka tarafından yürütölen el ile dosyalama işlemi tamamen veya kısmen otomatik olan faaliyet kapsamında değerlendirilmemiştir. Söz konusu kararda bir dosyalama sisteminin bilgisayarlı bir dosyalama sistemi ile aynı veya benzer hazır erişilebilirliği sağlamak için yeterli hassaslığa sahip olması gerektiđi belirtilmiştir. Söz konusu karar Birleşik Krallık ile Avrupa Komisyonu arasında kararın Avrupa Birliđi veri koruma hukukuna uygunluğu bakımından tartışmalara sebep olmuştur¹⁶. Zira Avrupa Birliđi veri koruma hukuku açısından bir tekil kimlik numarası, telefon numarası veya başka bir veri vasıtasıyla ya da alfabetik sıralama aracılığıyla çapraz sorgu imkânı sağlayarak verilere erişimin kolaylaştırılması bir dosyalama sistemi tespiti için yeterli sayılmaktadır. Bu doğrultuda Lindqvist ve İsveç arasında görölen dava neticesinde

¹⁴ Yönerge, Giriş Bölümü, par. 15.

¹⁵ Birleşik Krallık Yüksek Mahkemesi, Durant, Financial Services Authority'ye karşı, B2/2002/2636, 8 Aralık 2003 tarihli kararı, karar metni için bkz. <http://www.5rb.com/wp-content/uploads/2013/10/Durant-v-Financial-Services-Authority-CA-8-Dec-2003.pdf>, (Çevrimiçi) 21 Nisan 2018.

¹⁶ Kuner, a.g.e., s. 64-65.

verilen 6 Kasım 2003 tarih ve C-101/01 sayılı Avrupa Birliği Adalet Divanı kararında¹⁷, kilise mensupları hakkında haberlerin yayınlandığı internet sayfasında internet sitesi üzerinden kişilere ait, isim, soyisim, telefon, iş veya hobi gibi bilgilerin yayınlanması, tamamen veya kısmen otomatik yolla veri işleme olarak kabul edilmiştir.

Yönerge'nin uygulama alanına dair diğer sınırlandırmalar ise kişisel verileri işleyen kişiye ve işleme amacına ilişkin olarak da çeşitli konularda getirilmiştir. İlk olarak Yönerge'nin 3. maddesinin 2. fıkrasında sınırları belirlendiği üzere Avrupa Birliği'nin üçüncü sütununda yer alan ve topluluk hukukunun alanına girmeyen, kamu güvenliği, savunma, devlet güvenliği ve ceza hukuku alanındaki üye devlet etkinliklerinde Yönerge hükümlerinin uygulanmayacağı belirtilmiştir. İkinci olarak ise gerçek kişilerce tamamen kişisel ya da ailevi etkinlikler çerçevesinde yapılan veri işleme faaliyetleri Yönerge uygulama alanı dışında bırakılmıştır.

2.2.3. Yürürlükten Kalkma

Avrupa Birliği Genel Veri Koruma Tüzüğü'nde yer alan geçiş hükmü¹⁸ ile birlikte üye devletlere uyum sağlamaları için ve kişisel veri işleme faaliyeti gösteren aktörlerin yeni hükümlere adapte olabilmelerine ve uyum süreçlerini tamamlamalarına ilişkin olarak 2 yıllık bir süre tanınmıştır. Bu doğrultuda Tüzük'ün 25 Mayıs 2018'den itibaren uygulanması öngörülmüştür¹⁹. Bu tarihe kadar Avrupa Birliği Veri Koruma Yönergesi'nin yürürlükte kalması, üye devletlerin herhangi bir gecikmeye mahal vermeksizin gerekli düzenleme ve bildirimleri yapma gerekliliği Tüzük'te tesis edilmiştir. 25 Mayıs 2018 tarihi itibarı ile Avrupa Birliği Veri Koruma Yönergesi ile birlikte Avrupa Birliği üye devletlerinin iç hukuklarında yer alan kişisel verilerin korunması hakkındaki çakışan düzenlemeler yürürlükten kalkmış; tüm üye devletler

¹⁷ Avrupa Birliği Adalet Divanı, Bodil Lindqvist İsveç'e karşı, C-101/01, 6 Kasım 2003, (Çevrimiçi) <http://curia.europa.eu/juris/showPdf.jsf?jsessionid=9ea7d0f130d5c49a1840bda24b8385558b9d436cbd3b.e34KaxiLc3eQc40LaxqMbN4Och4Se0?text=&docid=48382&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=372741>, 21 Nisan 2018

¹⁸ Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 94.

¹⁹ Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 99.

için Avrupa Birliği Genel Veri Koruma Tüzüğü yeknesak bir veri koruma düzenlemesi haline gelerek, aynı şekilde iç hukuklarına sirayet ettirilmiştir.

2.3. Avrupa Birliği Genel Veri Koruma Tüzüğü

Hukukun zaman içerisinde yeni gelişmelere entegre olma gereksiniminin bir görünümü olarak Avrupa Birliği'nde de kişisel verilerin korunması alanında yeni bir düzenleme yapılması ihtiyacı hissedilmiştir. Bu ihtiyaç, bir girişme dönüştürülerek yasal çerçevenin gözden geçirilmesi kapsamında Avrupa Komisyonu tarafından Mayıs 2009'da üst düzey bir konferans düzenlenmiş ve bulut sistemler, global veri akışları, modern iletişim, bilgi teknolojileri ve bununla sınırlı olmamakla birlikte diğer gelişmeler göz önünde bulundurularak yeni ve kapsayıcı bir çalışma yapılması ihtiyacı vurgulanmıştır²⁰. Bu doğrultuda kamu, sivil toplum örgütleri ve devletlerden görüş toplanması kararlaştırılmıştır. Bu görüş alma sürecinde Avrupa Komisyon'u tarafından 9 Temmuz 2009 ile 15 Ocak 2011 tarihleri arasında 401'i bireyler, iş örgütleri ve dernekler ve 43'ü de kamu kurumlarından olmak üzere 473 geri dönüş²¹ alınmıştır. Görüş alışverişinin tamamlanmasının ardından, Avrupa Komisyonu 25 Ocak 2012 tarihinde Avrupa Birliği'nde kişisel verilerin korunmasına dair tesis edilecek olan hukuki çerçeveye ilişkin olarak bir reform paketi taslağı hazırlayarak kamu ile paylaşmıştır. Üye devletlerin²² ve Avrupa Birliği kurumlarının²³ çeşitli görüş bildirilerinin sürdüğü 4 yıllık bir tartışma ve görüş alışverişinin ardından 12 Şubat 2016 tarihinde Avrupa Birliği Konseyi taslağın düzenlenmiş metni üzerinde

²⁰ Avrupa Komisyonu, "Avrupa Birliği Genel Veri Koruma Tüzüğü Taslağı", 2012/0011, C7-0025/12, s. 2.

²¹ a.y.

²² Fransız senatosu 6 Mart 2012 tarihinde reform paketi taslağını kabul etmiş, Fransız Veri Koruma Otoritesi CNIL düzenlemeye ilişkin görüş ve değerlendirmelerini yayınlamıştır. 12 Mart 2012'de İsveç Veri Koruma Otoritesi tarafından düzenlemeye ilişkin görüş yayınlanmıştır. 20 Mart 2012'de Hollanda Parlamentosu, düzenlemede yer alan veri koruma seviyesinin ulusal veri koruma yasasından daha düşük olduğu durumlarda, Hükümeti ilgili maddelere karşı oy kullanmaya çağıran bir kararı kabul etmiştir.

²³ Avrupa Veri Koruma Denetmeni tarafından 7 Mart 2012'de, reform paketine ilişkin 4 bölümden oluşan görüş yayınlanmıştır. Görüş için bkz. Avrupa Veri Koruma Denetmeni, "Opinion of The European Data Protection Supervisor on The Data Protection Reform Package" Brüksel, 7 Mart 2012 (Çevrimiçi) https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf, 13 Nisan 2018; Article 29 Working Party, Veri Koruma Reformu Tasarısına ilişkin olarak 01/2012 sayılı görüşünü yayınlamıştır. Görüş için bkz. Article 29 Working Party, "Opinion 01/2012 on the data protection reform proposals" WP 191, Görüş, 23 Mart 2012.

uzlaşıldığını belirtmiş ve Avrupa Birliği Genel Veri Koruma Tüzüğü, Avrupa Birliği Konseyi'nin 8 Nisan 2016 tarihli toplantısında kabul edilmiştir.

Avrupa Birliği Genel Veri Koruma Tüzüğü 14 Nisan 2016 tarihinde ise Avrupa Birliği Parlamentosu tarafından kabul edilerek, 20 gün sonra yürürlüğe girmek üzere 4 Mayıs 2016 tarihinde Avrupa Birliği Resmî Gazetesi'nde yayımlanmıştır²⁴.

2.3.1. Kapsam ve Uygulama Alanı

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün şekillenmesinde en büyük etken şüphesiz ki 1995'ten bu yana uygulanan Avrupa Birliği Veri Koruma Yönergesi hükümleri ve Yönerge'nin uygulama alanına ilişkin yüksek mahkeme kararlarıdır. 1990'lı yılların ortalarından itibaren teknolojik gelişmelerin ve internetin geldiği nokta itibari ile gündelik hayata etki eden köklü değişimler karşısında sıklıkla eski ve yetersiz olarak eleştirilen Yönerge'nin bu eksikliklerinin giderilmesi hedeflenmiştir²⁵. Yönerge'de yer alan pek çok hususun korunduğu Avrupa Birliği Genel Veri Koruma Tüzüğü, 173 paragraflık giriş bölümü ve 99 maddeden oluşmaktadır. Veri öznesi olan ilgili kişiyi, Yönerge'den daha yüksek seviyede koruyan Avrupa Birliği Genel Veri Koruma Tüzüğü, ilgili kişiye birtakım ek haklar tesis ederken, veri sorumluları ve veri işleyenlere ise çeşitli sorumluluklar getirmektedir²⁶.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün dünyada büyük yankı uyandırmasının temel sebebi ise içerdiği hükümler uyarınca açıkça Avrupa Birliği sınırlarını aşan bir düzenleme olmasıdır. Uygulama alanına ilişkin madde 3'te, Avrupa Birliği sınırları içinde yerleşik veri sorumluları ile veri işleyenler hakkında, bunların faaliyet alanları incelenmeksizin Avrupa Birliği Genel Veri Koruma Tüzüğü kuralları uygulanacağı

²⁴ Bundan sonra Avrupa Birliği Genel Veri Koruma Tüzüğü yahut Tüzük olarak anılacaktır. İngilizce orijinal metin için bkz. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on The Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)", (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>, 13 Nisan 2018.

²⁵ Ayşe Nur Akıncı, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi", **Türkiye Cumhuriyeti Kalkınma Bakanlığı**, Yayın no: 2968, Çalışma Raporu 6, Haziran 2017, s. 11.

²⁶ Paul B. Lambert, **a.g.e.**, s. 42-43, 143-145.

belirtilmektedir. İlgili maddenin 2. fıkrasında ise, Avrupa Birliği’nde yerleşik olmasalar bile Avrupa Birliği’ndeki bireylerin verilerini işleyen veri sorumlusu ve veri işleyenlerin düzenlemeye tabi olacakları ifade edilmektedir. Hükümde, veri sorumlusu ya da veri işleyen tarafından yürütülen kişisel veri işleme faaliyetlerinin, Avrupa Birliği içerisindeki bireylere mal veya hizmet sunulması sırasında gerçekleştirilmesi yahut Avrupa Birliği’nde yerleşik bireylerin davranışlarının takip edilmesine ilişkin olması halinde, işleme faaliyetinin düzenlemeye yer alan hükümlere uygun olması gerektiği belirtilmiştir. Bir başka deyişle, Avrupa Birliği içerisinde faaliyet gösteren²⁷ tüm şirketler yerleşik olduğu yerden ari bir şekilde Avrupa Birliği Genel Veri Koruma Tüzüğü’nün getirmiş olduğu kriterleri sağlamakla yükümlü hale getirilmiştir²⁸.

Bölgesel kapsamın genişletilmesi ile bir şirketin merkezinin Avrupa Birliği ülkelerinden birinde bulunup bulunmadığı değerlendirilmezken; temel olarak aranan şart şirketin Avrupa Birliği sınırları dâhilinde faaliyet göstermesidir. “Bölgesel kapsam” başlıklı 3. madde uyarınca, birlik içerisinde veri sorumlusu yahut veri işleyen konumunda veri işleyen kişilerin yanı sıra, Avrupa Birliği’nde ikamet eden ilgili kişilerin kişisel verilerinin Avrupa Birliği’nde yerleşik olmayan veri sorumluları tarafından mal ve hizmet sunumu ya da davranışlarının takip edilmesi amacı ile işlenmesi halinde Tüzük’ün uygulama alanı bulacağı belirtilmiştir. Söz konusu düzenleme ile Avrupa Birliği Genel Veri Koruma Tüzüğü’nün müdahale alanı birlik sınırlarını aşarak Avrupa Birliği’nde yerleşik olmayan üçüncü taraf ülkelerde yerleşik veri sorumluları bakımından da sonuç doğurur hale gelmiştir²⁹. Avrupa Birliği Genel Veri Koruma Tüzüğü gerekçesinde, bireylerin kendilerine sağlanmış olan korumadan yoksun kalmamalarını teminen Avrupa Birliği içerisinde ikamet eden ilgili kişilere ait kişisel verilerin, Avrupa Birliği’nde yerleşik olmayan bir veri sorumlusu tarafından

²⁷ Burada Avrupa Birliği hukukunda özellikle rekabet hukuku alanında kabul gören “pazar yeri ilkesi” bakımından bir değerlendirme yapılması gerekmekte ve veri işleme yerinden ziyade verisi işlenen ilgili kişi üzerinden değerlendirme yapılması gerekmektedir. Pazar yeri ilkesi ve kişisel verilerin korunması bakımından uygulanmasına ilişkin detaylı bilgi için bkz. Çekin, **a.g.e.**, s. 30-31.

²⁸ Nilgün Başalp, “Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt 21, Sayı 1, İstanbul, 2015, s. 77-106, 88.

²⁹ Paul De Hert, Michael Czerniawski, “Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context”, **International Data Privacy Law**, Cilt 6, Sayı 3, s. 230–243, Oxford University Press, 1 Ağustos 2016, s. 230.

işlenmesi ve bu işleme faaliyetlerinin ilgili kişilere mal veya hizmet sunumunu veya ilgili kişilerin davranışlarının izlenmesini içerdiği hallerde düzenlemeye tabi olacağı belirtilmiştir. Yine gerekçede bir işleme faaliyetinin ilgili kişinin “davranışını izlemek” olarak değerlendirilip değerlendirilemeyeceğinin belirlenebilmesi için, “profil” uygulanmasını³⁰ da içeren veri işleme teknikleri kullanılarak internette kişiye ilişkin kişisel tercihlerin, tutum ve davranışların incelenmesi veya öngörülebilmesi maksadıyla izlenip izlenmediklerinin tespit edilmesi gerektiği ifade edilmiştir. Bu nedenle söz konusu düzenlemenin Google, Facebook gibi Amerikalı şirketlerin veri işleme faaliyetlerini düzenleyebilmek ve sınırlayabilmek amacı ile koyulmuş olduğu açıkça anlaşılmaktadır.

Yolsuzlukla mücadele düzenlemelerinde de olduğu gibi ülkelerin veri koruma mevzuatlarının sıkı bir şekilde yerel olarak sınırlı uygulanması, esasen globalleşen ve sürekli iletişim halinde olan dünyada konuya dair mevzuattan günümüz koşullarında beklenen faydanın elde edilmesinş engelleyebilecektir. Bu doğrultuda bölgesel genişlemeyi, temel olarak evrensel insan hakları kuralları da devletlerin yabancı unsurlu etkiler bakımından vatandaşlarının mahremiyetini koruyor olması nedeni ile desteklemektedir³¹. Günümüzde özellikle internet aracılığı ile sağlanan hizmetler bakımından hizmet sağlayanın nerede olduğunun önemsizleşmesi bu genişlemeyi haklı kılmaktadır.

2.3.2. Genel Kavramlar

2.3.2.1. Kişisel Veri

Avrupa Birliği Genel Veri Koruma Tüzüğü’nde kişisel veri, kimliği belirli veya belirlenebilir gerçek kişilerle ilgili herhangi bir bilgi olarak açıklanmıştır³². İlgili madde hükmünde belirlenebilirlik unsuru Avrupa Birliği Veri Koruma Yönergesi’nden daha geniş bir şekilde yorumlanmaya açık bırakılmaktadır. Tüzük

³⁰ Profil uygulamalarına ilişkin detaylı açıklamalara “3.2.1. Profilleme ve Otomatik Karar Alma Mekanizmaları” başlığında yer verilecektir.

³¹ Brendan Van Alsenoy, “Reconciling the (extra) Territorial Reach of the GDPR with Public International Law”, **Data Protection and Privacy Under Pressure Transatlantic Tensions: EU Surveillance, and Big Data**, ed. Gert Vermeulen, Eva Lievens, Antwerp, Belçika, Maklu, 2017, s. 93.

³² Kişisel verinin tanım ve unsurlarına ilişkin açıklama ve tartışmalara birinci bölümde verilmiştir.

kapsamında isim, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı ya da ilgili kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak bir kişiyi tanımlayan verilerin kişisel veri kapsamında değerlendirileceği belirtilmektedir³³.

Belirtmek gerekir ki Tüzük öncesi dönemde, kişisel veri tanımı kapsamında yer alan “belirlenebilir olma” unsuruna ilişkin Avrupa Birliği üye ülkeleri arasında farklı yaklaşım ve uygulama farklılıkları bulunmaktaydı. Örnek olarak; 78-17 sayılı 6 Ocak 1978 tarihli Fransız Veri Koruma Yasası’nda “nominal veri” kavramı kullanılmaktadır. Bu kavram ile niteliğinden bağımsız şekilde doğrudan veya dolaylı olarak, bir gerçek kişinin kimliğinin belirlenmesine izin veren her türlü veri, düzenleme kapsamına alınmıştır. Ancak 6 Ağustos 2004 tarihinde yapılan değişikliklerle birlikte kişisel veri³⁴, bir kimlik numarasına veya kendisine has bir veya daha fazla faktöre atıfta bulunarak doğrudan veya dolaylı olarak belirlenen veya belirlenebilen gerçek bir kişiyle ilgili herhangi bir bilgi olarak tanımlanmış ve kişinin belirlenebilir olup olmadığının tespiti için, veri sorumlusunun veya herhangi birinin kullandığı yada erişebileceği tüm yolların dikkate alınması gerektiği ifade edilerek sübjektif bir kişisel veri tanımına gidilmiştir.

Birleşik Krallık ise “kişisel veri” ve “veri” arasında şekilsel bir ayrımı tercih etmiştir. Birleşik Krallık veri koruma kanunu olan 16 Temmuz 1998’de kabul edilen Data Protection Act ile bir verinin kişisel veri olarak kabul edilebilmesi için gerçek ve yaşayan bir kişinin veriden yola çıkılarak ya da veri sorumlusunun elinde bulunan yahut bulunması muhtemel veriler aracılığı ile belirlenebilir olması ölçütü benimsenmiştir. Ayrıca bireye ilişkin görüşlerin de bu kapsamda değerlendirilebileceği belirtilmiştir³⁵. Ancak tartışmalara sebep olmakla birlikte

³³ Avrupa Birliği Genel Veri Koruma Tüzüğü m. 4 (1).

³⁴ Fransız Veri Koruma Yasası, Loi Informatique et Libertés, sayı 78-17, 6 Ocak 1978, m. 4.

³⁵ 16 Temmuz 1998 tarihli Birleşik Krallık Veri Koruma Kanunu, Data Protection Act 1998, Part 1 m. 1, “‘personal data’ means data which relate to a living individual who can be identified— (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual”

Birleşik Krallık Temyiz Mahkemesi, Durant Kararı'nda³⁶ kişisel verinin belirlenmesinde bireyin özel yaşamının gizliliğinin önemli ölçüde etkili olmasını arayarak biyografik olarak doğrudan etkileme ve yönelik olma kriterleri altında değerlendirmiştir. Finlandiya hukukunda ise geniş bir kişisel veri tanımlaması tercih edilmiş ve bu tanım uyarınca, kişinin bireysel mahremine, karakterine, koşullarına ilişkin her türlü kendisini ya da ailesini veya evini belirleyebilir kılan her çeşit veri kişisel veri kapsamında sayılmıştır. “Belirlenebilirlik” kavramı bazı üye devletlerce anahtar-veri kuramı üzerinden bir verinin veri sorumlusu tarafından kişiyi belirlenebilir kılmasına yönelik bir kapı açıp açmadığına bakılarak tanımlanmaya çalışılmıştır. Ancak örneğin Belçika veri koruma hukukunda veriyi işleyen kişinin bu bağlantıyı kurup kuramayacağına bakılmaksızın objektif olarak söz konusu verinin bir kişiyi belirleyip belirlemediğine bakılmaktadır³⁷. Alman hukuku bakımından ise belirlenebilirlik ölçütü bakımından, veri sorumlusunun elinde bulunan bilgi, kaynak ve imkânların göz önünde bulundurulduğu “görece ölçüt” yöntemi benimsenmiştir³⁸.

Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında Yönerge ile paralel şekilde kişisel veri altında özellikli birtakım veriler sayılarak belirtilmiştir. Bunlar kişilerin sağlık durumuna veya cinsel yaşama ilişkin verileri, genetik ve biyometrik verileri, sendika üyelik durumu, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan veriler olarak sınırlı sayıda gösterilmiştir³⁹. Söz konusu verilerin işlenme şartları genel nitelikli kişisel verilere nazaran daha dar tutularak özel olarak

³⁶ Kararın orijinalinde “*The first is whether the information is biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised. The second is one of focus.*” ifadesi yer almaktadır.

³⁷ Korff, **a.g.e.**, s. 15.

³⁸ Nafiye Yücedağ, “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt 75, Sayı 2, 2017, s. 767.

³⁹ Yönerge'nin yürürlükte olduğu dönemde üye devletler, Yönerge'de sayılan özel nitelikli kişisel verilere ek olarak başka veri kategorileri ekleyebilmekteydi. Örneğin Finlandiya veri koruma düzenlemesinde ayrıca sosyal üyelikler, tedavi ve sosyal yardım hakları da özel nitelikli kişisel veri olarak kabul edilmiştir. Yunan veri koruma hukukunda sendika dışındaki herhangi bir derneğe üyelik ve sosyal yardımlar da özel nitelikli veri olarak kabul edilirken, Portekiz hukukunda özel konulara ilişkin bilgiler ifadesi kullanılarak kapsama ilişkin herhangi bir açıklamaya yer verilmemiştir. Bazı ülkelerde ise finansal duruma ilişkin veriler özel nitelikli olarak kabul edilmiştir (Korff, **a.g.e.**, s. 86-88).

belirtilmiştir⁴⁰. Tüzük'te ayrıca, genetik veriler, biyometrik veriler veya sağlık ile ilgili verilerin işlenmesine ilişkin olarak üye devletlere ek sınırlama getirme ya da ek koşullar uygulama serbestisi tanınmaktadır.

2.3.2.2. Kişisel Verilerin İşlenmesi

Pek çok kaynakta olduğu gibi hangi faaliyetlerin kişisel veri işleme olarak nitelendirileceği Tüzük'de örnekleme yolu ile belirtilmektedir. Ancak sayılan fiiller veri döngüsünün tamamını içerecek şekildedir. Buna göre kişisel veri ya da kişisel veri setlerinin üzerinde gerçekleştirilen; toplama, kaydetme, organize etme, yapılandırma, depolama, uyarılma, değiştirme, geri alma, üzerinde çalışma, kullanma, iletilmesi suretiyle açığa vurma, yayma veya başka bir şekilde ulaşılabilir hale getirme, sıralama veya birleştirme, engelleme, silme veya imha etme gibi kişisel veriler üzerinde, otomatik olan veya olmayan yollarla gerçekleştirilen herhangi bir işlem veya işlem grubu kişisel verilerin işlenmesi kapsamına girmektedir. Bu tanımla, kişisel verilerin toplanmasından başlayarak, kişisel verilerle ilintili olabilecek her türlü süreci içerecek şekilde, bütün işleme türleri koruma altına alınmaktadır. Bununla birlikte belirtmek gerekir ki kişisel verilerin anonim hale getirilmesi de kişisel veriler üzerinde gerçekleştirilen ayrı bir işlem olarak tanımlanmaktadır. Her ne kadar Tüzük'ün gerekçesinde⁴¹ ilgili kişinin belirlenemeyeceği şekilde anonim hale getirilmiş olan kişisel veriler hakkında koruma ilkelerinin uygulanmayacağı belirtilmişse de mevcut bir kişisel verinin, ilgili kişi ile bağlantı kurulamayacak hale getirilerek anonimleştirilmesi işlemi de bir kişisel veri işleme faaliyeti olarak sayılmalıdır⁴².

2.3.2.3. Veri Sorumlusu

Avrupa Birliği Genel Veri Koruma Tüzüğü'nde “**controller**” olarak geçen kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek ve tüzel kişiler için Türkçe karşılık olarak veri denetçisi, veri kontrolörü ve veri sorumlusu deyimleri kullanılmaktadır. Veri sorumlusunun şirket, kurum ya da bir kuruluş olması halinde,

⁴⁰ Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 9.

⁴¹ Avrupa Birliği Genel Veri Koruma Tüzüğü, Giriş bölümü, par. 26.

⁴² Article 29 Working Party, “Opinion 05/2014 on Anonymisation Techniques”, WP 216, Görüş, 10 Nisan 2014, s. 7.

kişisel verileri işleme konusunda gerçekleştirdiği faaliyetler kapsamında bizzat tüzeli kişiliğin bütünü ile ilgili düzenlemelerde belirtilen hukuki sorumlulukları üstlenmesi gerekmektedir⁴³. Tüzeli kişinin belli bir organının ve/veya veri işleme konusunda ilgili tüzeli kişi nezdinde görevlendirilen bir kişinin veri sorumlusu - **data controller** yükümlülüklerine aykırı davranışı neticesinde hukuka aykırılık ortaya çıksa dahi sorumluluk, veri sorumlusu olan ilgili tüzeli kişi üzerinde doğmaktadır⁴⁴. Üye devletlerin hukuklarındaki genel hükümlerine göre söz konusu tüzeli kişinin bu hukuka aykırılığın ortaya çıkması konusunda irade gösteren kişiye tazminat hukuku bakımından rücu talebinde bulunup bulunamayacağı ayrıca düzenlenmesi gereken bir husustur. Ancak belirtmek gerekir ki Tüzük ile güdülen amaç tüzeli kişinin bizzat kendisinin sorumlu olmasıdır.

Avrupa Birliği Veri Koruma Yönergesi'nin yürürlükte olduğu dönemlerde bazı üye devletler veri sorumlusunun yükümlülüklerini tüzeli kişi için gerektiği şekilde yerine getirebilmesini sağlamak için “veri koruma görevlisi (**personal data protection official**)⁴⁵” istihdam etme zorunluluğunu getirmişlerdir⁴⁶.

Bu zorunluluk, belirtilen veri sorumlusunun yükümlülük ve sorumluluklarına ilişkin olarak temelde bir sapma yaratmamakta; aksine sorumluluk zincirine bir kişiyi daha

⁴³ Article 29 Working Party, “Opinion 1/2010 on the concepts of “controller” and “processor””, WP 169, Rapor, 16 Şubat 2010, s. 15-16f.

⁴⁴ Taştan, **a.g.e.**, s. 70-71. Veri sorumlusu nezdinde bir kişinin neden olmuş olduğu hukuka aykırı bir fiil bakımından sözleşmesel sorumluluk ve haksız fiil sorumluluğu gündeme gelebilecektir. Bu kapsamında Borçlar Hukuku anlamında veri sorumlusuna Türk Borçlar Kanunu madde 66’dan yola çıkarak adam çalıştırmanın sorumluluğu hükümleri kapsamında da gidilebilecektir, Taştan, **a.g.e.**, s. 72.

⁴⁵ Yabancı kaynaklarda, “Data privacy officer” ya da “data protection officer” terimleri kullanılmaktadır. Yönerge’de 18. madde altında “personal data protection official” terimi kullanılmıştır. Terimin Türkçe karşılığı olarak bu çalışma kapsamında “veri koruma görevlisi” ifadesi kullanılacaktır.

⁴⁶ Üye ülkelerden Almanya, Hollanda, İsveç, Lüksemburg ve Fransa ulusal mevzuatlarında veri koruma görevlisi atanmasına ilişkin hususları düzenlemiştir. Almanya’da otomatik veri işleme sistemleri ile kırktan fazla kişinin çalıştığı özel sektör şirketleri için veri koruma görevlisi atama zorunluluğu getirilirken, kamu kurumları açısından hiçbir istisna bulunmaksızın veri koruma görevlisi atama zorunluluğu bulunmaktadır. İsveç’te ise veri koruma görevlisi atama zorunluluğu bulunmamakla birlikte “kişisel veri temsilcisi” terimi tercih edilerek gönüllü uygulama getirmiştir. Hollanda’da ise yine bir zorunluluk olmamakla birlikte veri sorumlularının veri koruma uzmanı (terminolojik olarak, “mahremiyet görevlisi” terimi kullanılmaktadır) seçebileceği; ancak bu kişinin veri sorumlusundan emir ve talimat almamak üzere bağımsız bir konumda olması gerektiği belirtilmiştir. Article 29 Working Party, “Report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union”, WP 106, Rapor, 18 Ocak 2005, s. 15-19.

eklemektedir. Veri koruma görevlisi olarak istihdam edilecek kişiye de veri sorumlusunun yanında ayrıca sorumluluklar yüklenmekte, böylelikle veri sorumlusunun temel sorumlğunun yanında veri koruma görevlisi eliyle veri sorumlusunun faaliyetlerini denetleme, sorumluklarını yerine getirme, bunlara nezaret etme noktasında işlevleri güçlendirmektedir. Veri koruma görevlisinin ilgili kanunlardaki yükümlölükleri yerine getirmemesi sorumlğunu doğurmakla birlikte bu sorumluluk veri sorumlusuna atfedilen hukuki ve cezai sorumluluğı ortadan kaldırmamaktadır.

Avrupa Birliğı Genel Veri Koruma Tüzüğü'nde⁴⁷ veri sorumlusu ve veri işleyenlerin hangi durumlarda veri koruma görevlisi atamaları gerektiğı belirtilmiştir. Büyük oranda özel nitelikli kişisel veri işleyen veri sorumluları ve veri işleyenler ile ana faaliyet konusu bireylerin düzenli, sistematik ve büyük çaplı olarak izlenmesini gerektiren işlerden oluşan veri sorumluları ve veri işleyenler bakımından veri koruma görevlisi atanması bir zorunluluk olarak düzenlenmektedir. Sayılan grubun dışına kalan veri sorumlusu ve veri işleyenler için kendileri adına hareket etmek üzere bir veri koruma görevlisi atamalarının ihtiyari olduğı belirtilmiştir. Veri sorumluları tarafından atanacak olan veri koruma görevlisinin, Tüzük'te sayılan görevlerini yerine getirirken veri sorumlusundan talimat almaması gerekmektedir⁴⁸.

2.3.2.4. Veri İşleyen

Kişisel verileri, veri sorumlusu adına işleyen gerçek veya tüzel kişiler, kamu otoriteleri veya başka herhangi kurum veri işleyen olarak adlandırılmaktadır⁴⁹. Verileri işleyen kavramını kişisel verilerin kaydedilmesi, saklanması, sıralanması ve birleştirilmesi gibi işlemenin teknik yönlerini yürütmek üzere veri sorumlusu tarafından görevlendirilen uzmanlaşmış kişi veya kurum olarak tanımlamak mümkündür. Veri sorumlusu ve veri işleyen arasındaki ilişki ve çizgi taraflar arasında açıkça belirlenebilir olmalıdır. Veri işleyen kullanımı, şirketlerin yan operasyonlarını

⁴⁷ Avrupa Birliğı Genel Veri Koruma Tüzüğü, m. 37.

⁴⁸ Tüzük kapsamında veri koruma görevlisi bulundurma zorunluluğı şartları ve veri koruma görevlisinin konumu, hakları ve yükümlölükleri hakkında daha detaylı bilgi için bkz. Çekin, **a.g.e.**, s. 113-116.

⁴⁹ Avrupa Birliğı Genel Veri Koruma Tüzüğü, m. 4 (8).

yürütmek üzere dış kaynak kullanımlarını tercih etmesi ile birlikte daha sık görülmeye başlanmıştır. Belirtilmelidir ki, veri işleyen veri sorumlusu adına veri işlerken, veri sorumlusunun emir ve talimatları altında hareket etmek zorundadır. Veri sorumlusu tek bir veri grubu için farklı işleme faaliyetleri kapsamında farklı veri işleyenler kullanabilmektedir. Örneğin; bir şirket, müşteri deneyimini geliştirmek için çağrı merkezinden, müşterilerini arayarak anket uygulamasını isteyebilir; bir anket firmasıyla anlaşarak belirli saatler arasında mağazalarına gelen müşteri ve potansiyel müşterileri ile anket yapılmasını isteyebilir; sonuçların başka bir veri analizi firmasından değerlendirmesini isteyebilir; matbu formları başka bir arşiv firmasının deposunda; dijital verileri ise şirket veri tabanında saklamayı isteyebilir. Görülebileceği üzere veri toplama, kullanma, saklama gibi verinin döngüsündeki bütün işleme faaliyetleri şirketin emir ve talimatları ile üçüncü taraf veri işleyenlerce gerçekleştirilebilmektedir. Veri işleyen, sözleşmesel ilişki içerisinde olduğu taraf için veri işleyen sıfatında hareket ederken, onun emir ve talimatlarının dışına çıkmamalıdır. Bu nedenle veri sorumlusu ve veri işleyen arasındaki ilişkinin sınırlarının ve kapsamının belirlenerek taraflar arasında yazılı bir sözleşme yapılması gerekmektedir⁵⁰. Belirtilmelidir ki

Yönerge'den farklı olarak Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında veri işleyenlerin yükümlülükleri genişletilerek veri sorumlusuna yaklaştırılmıştır⁵¹. Veri sorumlusu ile birlikte veri işleyenler de veri güvenliğine ilişkin gerekli tedbirleri almakla yükümlü kılınmış ve veri ihlalleri halinde bildirimde bulunma yükümlülüğü getirilmiştir⁵². Veri sorumlusunun yazılı onayı olmaksızın alt veri işleyen çalıştıramayacağı, işleme faaliyeti ile ilgili hizmetlerin sona ermesi ya da tamamlanmasından sonra tüm kişisel verilerin silinmesi veya sorumlusuna iade edilmesi gerektiği, veri sorumlusu adına gerçekleştirilen veri işleme faaliyetlerine ilişkin olarak kayıt tutması gerektiğine dair yükümlülükler Yönerge'den farklı olarak Tüzük'te düzenlenmiştir.

⁵⁰ Paul B. Lambert, **a.g.e.**, s. 238.

⁵¹ Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında veri sorumlusu ve veri işleyen ayrımı için bkz. Çekin, **a.g.e.**, s. 41, 79.

⁵² Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 32-34; Tikkinen-Piri, Rohunen, Markkula, **a.g.m.**, s. 143.

Verilerin gizliliği ilkesine göre, veri sorumlusu veya veri işleyenin otoritesi altında görev yapan kişiler, veri sorumlusunun talimatı olmadan veriler üzerinde herhangi bir işlem gerçekleştiremeyecektir⁵³.

2.3.3. Veri Sorumlularının Uyması Gereken Temel İlkeler

Avrupa Birliği Genel Veri Koruma Tüzüğü temel olarak veri koruması hakkındaki 1980’li yıllardan bu yana kabul görmüş temel prensipleri değiştirmemekte, yaklaşımını aynen korumaktadır. Yönerge’de, 108 sayılı Sözleşme ve OECD Rehber İlkelerinde belirtilen usul ve esaslara paralel şekilde kişisel verilerin işlenmesine ilişkin ilkelere yer verilmiştir⁵⁴. Bununla beraber, teknolojik gelişmeler ışığında Avrupa Birliği Genel Veri Koruma Tüzüğü’nde bazı yeni kavramlar ayrıca ele alınmıştır. Buna göre kişisel veriler hukuka ve dürüstlük kurallarına uygun olarak şeffaf bir şekilde işlenmeli; belirli, açık ve meşru amaçlar için toplanmalı; toplanma amaçlarıyla ilgili, ölçülü ve yeterli olmalı; doğru ve güncel tutulmalı; gerekli olan süre kadar saklanmalı ve uygun tedbirler aracılığı ile güvenliği sağlanarak işlenmelidir. Kişisel verilerin işlenmesine ilişkin gerek hukuka uygunluk sebeplerinin değerlendirilmesinde gerekse hukuka uygun işleme faaliyetinin sınırlarının belirlenmesinde sayılan ilkeler bir referans noktası olarak değerlendirilmelidir. Kişisel verilerin işlenmesinde veri sorumluları ve veri işleyenlerin her zaman göz önünde bulundurulması gereken birtakım sınırlandırmalarda bu ilkeler yol gösterici olmaktadır.

Hukuka ve dürüstlük kurallarına uygun olarak şeffaf bir şekilde veri işleme ilkesi ile kişisel verilerin var olan yasal düzenlemelere ve diğer hukuksal metinlerde öngörülen koşullara uygun olması gerektiği ifade edilmektedir. Hukuka uygunluk ilkesi uyarınca veri işleme faaliyetinin hem mevcut hukuk enstrümanları olan kanunlara ve diğer düzenlemelere hem de veri koruma hukukuna uygunluğunun beraber sağlanması gerekmektedir⁵⁵. Dürüstlük kuralına uygun olma ilkesi ise genel olarak veri sorumlularının veri işlemedeki hedeflerine ulaşmaya çalışırken, ilgili kişilerin çıkarlarını ve makul beklentilerini her daim göz önünde bulundurmaları gerektiğini

⁵³ Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 27.

⁵⁴ Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 5.

⁵⁵ Lill Taranto, “Data Protection Principles”, **European Privacy: Law and Practice for Data Protection Professionals**, ed. Eduardo Ustaran, IAPP publication, 2012, s. 84.

işaret etmektedir⁵⁶. İşleme faaliyetlerinin ilgili kişi için öngörülebilir ve şeffaf olması, bilgilendirmeye dayanması şartları bu ilkenin bir görünümüdür. Bir diğer ifade ile dürüstlük kuralı uyarınca, kişisel veri işleme faaliyeti ilgili kişilerin, hangi kişisel verilerinin toplandığı ve işlendiğini öğrenmelerine açık olmalıdır⁵⁷.

Belirli, açık ve meşru amaçlar için kişisel verilerin toplanması ilkesi ile verilerin toplanma aşamasında veri sorumlularına hangi verileri hangi amaçla işleyeceğini belirlemiş olma yükümlülüğü getirilmektedir. Bu doğrultuda hangi verilerin işlenip hangilerinin işlenemeyeceğinin sınırının belirlenmesi ve bu belirli bir amaç için toplanan verinin başka amaçlar ile kullanılmaması hedeflenmektedir. Ayrıca başlangıçta belirtilen bu amacın meşru olması gerekmektedir.

Toplanma amaçlarıyla ilgili, ölçülü ve yeterli olma ilkesi uyarınca veri sorumlusu, yürüttüğü yahut yürütmeyi planladığı kişisel veri işleme faaliyeti kapsamında öncelikle amaçlarına ulaşabilmek için kişisel verilerin mutlaka gerekli olup olmadığını saptamalıdır⁵⁸. Veri ekonomisi, veri sadeleştirilmesi, yeterlilik ölçütü gibi şartlar bu ilkenin bir görünümü olarak değerlendirilmektedir. Bu ilke temel olarak veri sorumlularına kişisel veri işleme faaliyetlerine ilişkin bir sınırlandırma getirme amacı gütmektedir⁵⁹.

Ölçülülük ilkesi her ne kadar Yönerge kapsamında da yer almış olsa da Yönerge'nin uygulandığı dönemde söz konusu ilke bakımından üye devletlerde farklı yaklaşımlar görülmektedir. İlkenin yasaklamış olduğu başlangıçtaki amaçla uyumsuz veri işleme faaliyetlerinin kapsamı hakkında üye devletler tarafından farklı değerlendirmeler yapılmıştır. Örneğin; Birleşik Krallık'ta veri toplama anında ilgili kişiye sunulan geniş kapsamlı bildirimler geçerli olarak kabul edilmiş ve sonraki veri işleme faaliyetlerinin uygunluğu daha geniş yorumlanmıştır⁶⁰. Belçika veri koruma hukukunda ise toplanma anında ilgili kişiye bildirilen amaç dışında ikincil bir amaç için yürütülecek veri işleme

⁵⁶ Lee A. Bygrave, **Data Protection Law: Approaching Its Rationale, Logic and Limits**, Kluwer Law International, Hollanda, Amerika Birleşik Devletleri, 2002, s. 58.

⁵⁷ Taranto, **a.g.e.**, s. 83.

⁵⁸ Küzeci, **a.g.e.**, s. 220.

⁵⁹ Taranto, **a.g.e.**, s. 86.

⁶⁰ Korff, **a.g.e.**, s. 63-64.

faaliyetlerinin ilgili kiři tarafından makul düzeyde öngörölüp öngörülemediğini değerlendirilmiştir. Alman veri koruma hukukunda ise menfaatler arası bir test sonucunda işlemenin uygun olup olmadığı tespit edilmiştir⁶¹.

Doğru ve gerektiğinde güncel olma ilkesi ile hem ilgili kişinin hem de veri sorumlusu ve veri işleyenin çıkarları korunmak istenmektedir. Kişisel verilerin ilgili kiři bakımından gerçeği yansıtmıyor olması, hatalı veya eski olması ve bu hali ile veri sorumlusunun herhangi bir kişisel veri işleme faaliyetine konu olması bireyin temel hak ve özgürlüklerini, ekonomik çıkarlarını ve/veya manevi bütünlüğünü etkileyen sonuçlar meydana getirebilecektir. Veri sorumlusu açısından ise kişisel veri işleme faaliyetinden beklenen fayda karşılanamayacaktır. Buna göre doğru ve kaliteli verilerle oluşturulmuş veri tabanları, veri sorumlularının yatırımlarının karşılığını daha iyi almalarını sağlamaktadır⁶². İlgili kişinin kişisel verilerine erişim hakkı, verilerin düzeltilmesini talep hakkı bu ilke kapsamında değerlendirilmektedir. İlkenin getirdiği bir diğer tartışma ise söz konusu güncellik durumunun arşivlenmiş ve yedeklenmiş veriler bakımından nasıl uygulanacağıdır⁶³. Bu noktada zaman damgalı olarak ve arşivleme amacı için oluşturulmuş veri tabanları bakımından güncellik şartının aranmaması gerektiği kabul edilmektedir. Ancak her halükârda somut olay bakımından kullanılan kişisel verilerin etkisine göre güncellik şartının aranıp aranmayacağını değerlendirmek gerekmektedir⁶⁴.

Kişisel verilerin gerekli olduğu süre kadar saklanması ilkesi, verilerin veri sorumlusu tarafından toplanma amaçlarına uygun olarak kullanıldıktan sonra saklama süresine ilişkin bir sınırlandırma getirmektedir. Bu doğrultuda veri sorumlusunun kişisel verilerin işlenmesi ile hedeflenen amacın ortadan kalması, amaca ulaşmak için kişisel verinin işlenmesinin gereksiz olduğunun anlaşılması ya da amaca ulaşıldığı için artık kişisel verinin tutulması gerekliliğinin ortadan kalkması halinde kişisel verilerin artık saklanmaması gerekmektedir. Veri saklama politikası oluşturma yükümlülüğü, kişisel

⁶¹ a.e., s. 64-65.

⁶² Hüseyin Can Aksoy, Kişisel Verilerin Korunması, **Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk (Medeni Hukuk) Anabilim Dalı Yüksek Lisans Tezi**, Ankara, 2008, s. 82.

⁶³ Taranto, a.g.e., s. 90.

⁶⁴ Article 29 Working Party, “Opinion 8/2001 on the processing of personal data in the employment context”, WP 48, Görüş, 13 Eylül 2001, s. 3.

verilerin silinmesini talep hakkı⁶⁵ gibi kavramlar bu ilkenin bir görünümü olarak değerlendirilmektedir. Bu doğrultuda verilerin gerekenden fazla tutulmamasını sağlamak adına veri sorumlusu tarafından silinme veya periyodik gözden geçirme sürelerinin belirlenmesi gerekmektedir⁶⁶.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nde, Yönerge'de yer alan genel ilkeler ve kişisel veri işleme şartları mümkün olduğunca muhafaza edilmeye çalışılmıştır. Genel ilkeler bakımından Tüzük ile birlikte bir değişikliğin olmayacağı, 2012 yılında paylaşılan Tüzük taslağının genel gerekçesinde açıkça ifade edilmektedir⁶⁷. Tüzük, Yönerge'nin uygulanmasından ve yorumlanmasından kaynaklanan bazı sorunları çözebilmek ve teknolojik anlamda tarafsızlığı sağlayacak şekilde mevcut çerçevenin uyarlanmasını sağlamak adına, Article 29 Working Party görüşleri ve Avrupa Adalet Divanı Kararları uyarınca uygulamada benimsenen birtakım eklemeleri yahut daraltmaları getirmiştir. Avrupa Adalet Divanı kararlarında sıklıkla atıfta bulunulan ve mevcut ilkelerin bir görünümü olarak geçen “şeffaflık ilkesi”, “veri sadeleştirilmesi ilkesi” ve “veri sorumlusunun kapsamlı sorumluluk ve hesap verebilirlik prensipleri”⁶⁸ Tüzük ile getirilen yeni ilkeler olarak sayılabilecektir⁶⁹.

Sayılan temel ilkeler uyarınca ilgili kişiye, kişisel veri işleme süreçlerine çeşitli aşamalarda katılma olanağı tanıyan bazı haklar verilmiştir. Kişisel verilere erişim hakkı, silinmesini talep hakkı, verilerin düzeltilmesini isteme hakkı ve bazı durumlarda veri işlemeye itiraz hakkı bu kapsamda yer almaktadır. İlgili kişiye tanınan bu hakların bireye kullandırılması başka bir deyişle, ilgili kişinin kişisel verilerinin

⁶⁵ Tüzük kapsamında bireylere kendilerine ait verinin kullanması için geçerli bir sebep kalmamışsa bu verinin silinmesini talep etme hakkına, genel bir ilke olmanın ötesine geçerek, ayrı bir hüküm olarak yer verilmektedir (Avrupa Birliği Genel Veri Koruma Tüzüğü m.17); özellikle dijital hayatta büyük önem taşıyan ve C-131/12 sayılı, 13 Mayıs 2014 tarihli Google İspanya, Mario Costeja González'e karşı Adalet Divanı kararı ile temelleri atılmış bu hak öğretide **right to be forgotten** olarak geçmektedir. Karar için bkz. “Google Spain SL ve Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González” Adalet Divanı (Grand Chamber)’a karşı, Karar No C-131/1213, Karar Tarihi 13 Mayıs 2014, ECR [2014] 317.

⁶⁶ Avrupa Birliği Genel Veri Koruma Tüzüğü, Giriş Bölümü, par. 39.

⁶⁷ Avrupa Komisyonu, Proposal for General Data Protection Regulation, s. 4.

⁶⁸ Yönerge'nin yürürlük sürecinde Article 29 Working Party tarafından hazırlanmış olan hesapverilebilirlik konulu görüş için bkz. Article 29 Working Party, “Opinion 3/2010 on the principle of accountability”, WP 173, Görüş, 13 Temmuz 2010.

⁶⁹ a.e., s. 8.

işlenme süreçlerine katılımı ve denetimi konusunda gerekli mekanizmaları oluşturmak veri sorumlusunun yükümlülüğüdür. Bu doğrultuda, veri sorumlusunun ilgili kişiyi bilgilendirme yükümlülüğü⁷⁰ ve ilgili kişinin kişisel verilerine erişim hakkı sağlama yükümlülüğü⁷¹ bu kapsamda değerlendirilmektedir.

2.3.4. Kişisel Verilerin İşlenmesini Meşru Kılan Hukuka Uygunluk Nedenleri

Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında kişisel verilerin işlenmesinin meşru olduğu hallere ilişkin olarak veri kategorisi ve kişisel verilerin bir işlenme türü olan aktarma bakımından ayrıca bir sınıflandırma yapılarak söz konusu haller belirlenmiştir. Özel nitelikli kişisel verilerin işlenmesinde yer alan hukuka uygunluk halleri daha dar ve özellikli olarak madde 9’da yer alırken genel nitelikli kişisel verilerin işlenmesinde aranacak hukuka uygunluk sebepleri 6. madde kapsamında sayılmaktadır. 49. madde kapsamında ise kişisel verilerin Avrupa Birliği dışındaki ülkelere aktarılması halinde aranacak hukuka uygunluk sebepleri ve şartları belirtilmektedir. Yönerge’den farklı olarak Tüzük kapsamında ayrıca 16 yaşından küçük çocukların kişisel verilerinin işlenmesi 8. madde kapsamında düzenlenmiştir. Daha geniş bir düzenleme olması sebebi ile 6. madde kapsamında sayılan hukuka uygunluk halleri Tüzük’de yer alan kategorik ayrıma değinilerek aşağıda

⁷⁰ Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 14 hükmü gereği, veri sorumlusunun yahut temsilcisinin ilgili kişiye, zaten bildiği durumlar hariç olmak üzere asgari olarak şu bilgileri sunması gerektiği belirtilmiştir; **i.** veri sorumlusunun veya duruma göre temsilcisinin kimlik ve irtibat bilgileri; **ii.** mevcut olması halinde veri koruma görevlisi irtibat bilgileri; **iii.** veri işleme amacı ve yasal dayanağı; **iv.** kişisel veri kategorileri; **v.** kişisel verilerin aktarılacağı alıcı veya alıcı kategorileri. Bununla birlikte 14. Maddenin 2 fıkrasında ayrıca dürüstlük kuralına uygunluk ve şeffaflık ilkesi uyarınca sunulması gereken bilgiler sayılmıştır. İlginin bilgilendirilmesine ilişkin detaylı bilgi için bkz. Article 29 Working Party, “Guidelines on transparency under Regulation 2016/679” WP 260, Rehber, 29 Kasım 2017; Küzeci, **a.g.e.**, s. 230-231.

⁷¹ Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 15 hükmü gereğince ilgili kişinin veri sorumlusuna başvurarak; **i.** kendisine ilişkin verilerin işlenip işlenmediğini, işlemenin amacını, ilgili veri kategorileri ve verinin açıklandığı alıcıları ya da alıcı kategorilerini ve veri saklama sürelerini öğrenme; **ii.** kişisel verilerin düzeltilmesi veya silinmesini veya söz konusu verilerin işlenmesinin kısıtlanmasını talep etme veya söz konusu işleme faaliyetine itiraz etme; **iii.** bir denetim makamına şikayette bulunma; **iv.** profil çıkarmada Dâhil en azından otomatikleştirilmiş kararlar durumunda, kendisine ilişkin verinin her tür otomatik işlenmesinin temelini içeren bilgi talep etme. İlgili kişinin kişisel verilerine erişim hakkı ve bu kapsamda veri sorumlusunun yükümlülüklerine ilişkin detaylı bilgi için bkz. Küzeci, **a.g.e.**, s. 232-234.

açıklanmaktadır. Bu doğrultuda 6. madde kapsamında kişisel verilerin işlenmesi aşağıda sayılan durumlardan bir ya da birkaçının bulunması ile meşru kabul edilecektir:

- i. İlgili kişinin rızasının bulunması;
- ii. İlgili kişinin taraf olduğu bir sözleşmenin ifa edilmesi ya da ilgili kişinin bir sözleşmenin tarafı olmadan önceki istemleri dolayısıyla işlemenin gerekli olması;
- iii. Veri sorumlusunun tabi olduğu yasal bir yükümlülüğe uymak için işlemenin gerekli olması;
- iv. İlgili kişinin ya da üçüncü bir kişinin yaşamsal çıkarlarının korunması için işlemenin gerekli olması;
- v. İşlemenin kamu yararının bulunduğu bir hizmetin gerçekleştirilmesi ya da veri sorumlusunun veya verinin açıklandığı üçüncü kişinin resmi bir yetkisini kullanması için gerekli olması;
- vi. İlgili kişinin temel hak ve özgürlüklerinden kaynaklı çıkarlarının baskın olduğu durumlar hariç veri sorumlusu veya verinin açıklandığı üçüncü kişinin meşru çıkarlarından kaynaklanan amaçlar için gerekli olması.

Yukarıda sayılan hallerin özel olarak kişisel veri işleme faaliyetinde güdülen amaca yönelik olması ve kişinin bu amaç doğrultusunda bilgilendirilmiş olması önem teşkil etmektedir. Bu bakımdan sayılan hallerin kapsamının doğru olarak değerlendirilmesi önem taşımaktadır.

2.3.4.1. Açık Rıza

Yönerge 7. madde (a) hükmü gereğince genel nitelikteki kişisel verilerin işlenmesinde "rızanın" alınmış olması yeterliyken, özel nitelikli kişisel verilerin işlenmesinde "açık rızanın" alınmış olması şartı aranmaktadır⁷². Bu ikili durum Avrupa Birliği Genel Veri Koruma Tüzüğü ile yeknesaklaştırılarak "açık rıza" koşulu her iki veri kategorisi

⁷² Yönerge m. 8/2 (a).

bakımından genel geçer hale getirilmiştir. Avrupa Birliği Komisyonu ve Avrupa Birliği Parlamentosu bu konuda görüş birliği içerisinde iken Avrupa Birliği Konseyi daha az kesin bir ifadeyi önermiştir. Buna göre, "*tereddüde yer vermeyecek (unambiguous) bir rıza beyanı*" ifadesinin tercih edilmesi önerilmiştir. Yasalaşan metinde ise rıza bir beyan ya da onaylayıcı eylem şeklinde ilgili kişinin, kişisel verilerinin işlenmesi konusunda özgürce, belirli bir amaç doğrultusunda özel olarak bilgilendirilmiş halde ve tereddütte yer vermeyecek şekilde irade açıklaması olarak tanımlanmıştır⁷³. Tüzük'ün giriş bölümünde onaylayıcı eylemin ne şekilde olması gerektiği örneklenerek belirtilmektedir. Buna göre, bir internet sitesinde yer alan ilgili formun ya da bilgilendirmenin kabulü anlamında boş bırakılmış bir kutunun işaretlenmesi aktif bir hareket olarak görülerek rızanın alındığı anlamına gelebilecek iken, dolu kutucuğun işaretinin kaldırılmaması, hareketsiz kalma başka bir deyişle, susma yolu ile rızanın alınmasının mümkün olmayacağı ifade edilmektedir⁷⁴.

Tüzük ile rızanın kapsamı ve geçerliliğine ilişkin getirilen bu düzenleme bir yenilikten ziyade Yönerge'nin uygulanmasına ilişkin görüşlerin⁷⁵ hukuki bir zemine oturtulması olarak değerlendirilebilecektir⁷⁶. Nitekim rıza kavramı ve tanımı Avrupa Birliği veri koruma hukuku bakımından sıklıkla tartışmalara konu olmuştur⁷⁷. 2010 yılında Avrupa Komisyonu, Avrupa Birliği üye devletleri arasındaki veri koruma hukukuna ilişkin yaklaşımları yeknesaklaştırmak adına bir rapor yayınlamıştır⁷⁸. Raporla Avrupa Komisyonu'nun, rıza kurallarını açıklığa kavuşturma ve güçlendirme yollarını ortaya koymak istediği ifade edilmiştir⁷⁹. Nitekim üye devletler arasında rıza

⁷³ Tüzük m. 4/11.

⁷⁴ Tüzük, Giriş Bölümü, par. 32.

⁷⁵ Article 29 Working Party, "Opinion 15/2011 on the definition of consent", WP 187, Görüş, 13 Temmuz 2011.

⁷⁶ Avrupa Birliği Genel Veri Koruma Tüzüğü ile düzenlenen rıza koşulunun şartları ve geçerliliğine ilişkin daha detaylı bilgi için bkz. 10 Nisan 2018 tarihinde güncellenen Article 29 Working Party, "Guidelines on Consent under Regulation 2016/679", WP 259, 28 Kasım 2017.

⁷⁷ Veri koruma hukuku bakımından 2010 yılında ilgili kişinin rızası kavramı Avrupa Birliği'nde tartışmaların merkezi olmuştur. Eleni Kosta, **Consent in European Data Protection Law**, 3. Baskı, Martinus Nijhoff, Leiden-Boston, 2013, s. 1.

⁷⁸ Avrupa Komisyonu, "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive Approach on Personal Data Protection in The European Union", COM (2010) 609 final, Brüksel, 4 Kasım 2010.

⁷⁹ a.e., s. 9.

kavramının nasıl sağlanacağına ilişkin olarak bir uygulama birliği bulunmamakta idi⁸⁰. Üye devletlerin uygulamalarındaki farklılıklar Tüzük hükmü ile yeknesaklaştırılmıştır. Ayrıca 16 yaşından küçük çocukların kişisel verilerinin bilgi toplumu hizmetlerinin sağlanması sırasında işlenmesi, Tüzük kapsamında ayrıca bir madde ile hüküm altına alınmıştır⁸¹. Bu doğrultuda 16 yaşından küçük çocukların kişisel verilerinin işlenmesinin ancak rızanın çocuğun velisi veya vasisi tarafından verilmesi veya onaylanması durumunda ve verildiği veya onaylandığı ölçüde hukuka uygun olacağı belirtilmiştir. Ayrıca 16 yaşından küçük çocukların doğrulanabilir rızasının alınması bakımından veri sorumlusuna mevcut teknolojiyi dikkate alarak makul çaba sarf etme yükümlülüğü getirilmiştir.

Rıza kavramı bireylerin verilerinin geleceğini belirleme hakkı ile birlikte düşünülmelidir. Bu doğrultuda veri sorumlularının, ilgili kişiden kişisel verilerinin işlenmesine ilişkin rızalarını talep ederlerken reddetme hakkını tanımaları ve kişisel verilerinin kontrolünü bireylere vermeleri gerekmektedir⁸².

Geçerli bir rızanın bir diğer önemli unsuru ise açıklık olarak değerlendirilmektedir. Bu doğrultuda veri sorumlusu gerçekleştireceği bilgilendirmeler mümkün olduğunca açık ve anlaşılır olmak durumundadır. Bireyin kişisel verilerinin hangi amaçla, nasıl işlendiğine onay verdiğiğine ilişkin bir şüpheye düşmemesi gerekmektedir⁸³.

2.3.4.2. Sözleşmenin Kurulması veya İfası Kapsamında Gerekli Olma

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 6 (b) maddesi uyarınca, kişisel veriler *“bir sözleşme yapmadan önce ilgili kişinin talebi üzerine önlem almak için ya da ilgili kişinin taraf olduğu bir sözleşmenin yerine getirilmesi amacıyla”* işlenebilmektedir.

⁸⁰ Yönerge'nin uygulandığı dönemde, bazı devletler yazılılık şartını ararken bazı devletler örtülü rızayı kabul etmişlerdir; **a.e.**, s. 8; İsveç ve İspanya iç hukuk düzenlemelerinde rızanın kesinlik şartını güçlendirebilmek için rıza tanımına eklemeler yapmışlardır, Lüksemburg veri koruma hukukunda ise açık ve kesin rıza geçerlilik koşulu olarak aranmaktadır. Avusturya, Almanya ve İtalya veri koruma hukuklarında Yönerge'de yer alan rıza tanımına yakın bir tanıma yer verilmekte ve rızanın özgür, spesifik ve bilgilendirilmeye dayalı olma özellikleri vurgulanmaktadır. İtalyan hukuku bakımından ayrıca rızanın yazılı olma şartı aranmaktadır. Buna karşın Birleşik Krallık veri koruma hukukunda ise rıza tanımı yer almamakla birlikte örtülü rıza geçerli kabul edilmektedir, Korff, **a.g.e.**, s. 26-27.

⁸¹ Tüzük m. 8.

⁸² Article 29 Working Party, “Opinion 15/2011 on the definition of consent”, s. 10.

⁸³ **a.y.**

Bu halde ilgili kişinin kişisel verisinin işlenebilmesi için veri sorumlusu ile bir sözleşme akdetme ya da müzakere aşamasında olması gerekmektedir.

Veri koruması hukukunda, hukuka uygunluk hallerini değerlendirirken genel ilkelerden bağımsız düşünmemek ve her bir hukuka uygunluk halinin kapsam ve amacını genel ilkeler ışığında yorumlamak gerekmektedir. Sözleşmenin ifası ya da kurulması kapsamında kişisel veri işleme hukuka uygunluk nedeni ise gereklilik ve ölçülülük ilkesi ile birlikte düşünülmelidir. Veri işleme faaliyetinin bu kapsamda meşru sayılabilmesi için ilgili kişi tarafından akdedilmiş ya da akdedilmesi muhtemel bir sözleşmenin varlığı ve veri işleme faaliyetinin bu sözleşme kapsamında gerekli olması aranmalıdır. Bunun yanında ayrıca kişisel veri işleme faaliyetinin söz konusu sözleşmenin belirli bir amacına ulaşmak için kullanılıyor olması gerekmektedir⁸⁴.

Belirtmek gerekir ki maddenin lafzı bakımından veri sorumlusunun söz konusu sözleşmeye taraf olma şartı aranmamaktadır⁸⁵. Bunun nedeni ise sözleşmenin ifası kapsamında veri sorumlusunun ifayı tek başına yapmayacağı durumlardaki veri aktarımını ve üçüncü tarafların veri işleme faaliyetlerini meşru bir zemine kavuşturmasıdır. Bu kapsamda mesafeli satış sözleşmesi ile ürün alan bir bireyin adres bilgisinin malın teslimi için taşıma şirketi ile veri işleyen sıfatı ile paylaşılması örnek olarak verilebilir. Bununla birlikte her ne kadar sözleşmenin ifası ile ilgili olsa da veri aktarılan üçüncü kişilerin ilgili kişi ile akdedilmiş olan sözleşmenin tarafı olmayacağı sebebi ile bu hukuka uygunluk sebebine dayanarak veri işleyeceğine ilişkin görüş de mevcuttur⁸⁶.

İlgili kişiye ilişkin olarak toplanan verilerin bu kapsamda değerlendirilebilmesi için söz konusu verilerin kurulmuş ya da kurulması muhtemel sözleşme ile doğrudan ilgili

⁸⁴ Article 29 Working Party, “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”, WP 217, 9 Nisan 2014, s. 16-17; biz sözleşmenin ifası kapsamında veri işlemenin gerekli olması halinde ayrıca rızanın alınmaması gerektiğine ilişkin olarak ayrıca bkz. Article 29 Working Party, “Guidelines on consent under Regulation 2016/679”, s. 7-10; Çekin, **a.g.e.**, s. 67-70.

⁸⁵ Nurullah Tekin, “Kişisel Verilerin Korunması ile İlgili Türkiye’deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi”, **Uyuşmazlık Mahkemesi Dergisi**, Sayı 4, 2014, s. 233.

⁸⁶ Satış sözleşmesi kapsamında müşteri hizmetlerinin üçüncü bir kişi tarafından sunulması ve müşteri verilerinin aktarılması halinde müşterinin açık rızasının gerekeceğine ilişkin bkz. Çekin, **a.g.e.**, 71.

olması, gereklilik ve veri sadeleştirilmesi ilkelerine uygun şekilde işlenmesi önem arz etmektedir. İlke gereğince veri sorumlusunun amacına ulaşabilmek için gerekli olan kişisel veriyi sadece amaca yönelik olarak işlemesi gerekmektedir. Bu bakımdan veri sorumlusunun amacına ulaşmak için söz konusu kişisel verileri işlemesinin şart olup olmadığının sorgulanması, bir başka deyişle, kişisel veri kullanmadan ya da daha az kişisel veri kullanarak söz konusu sözleşmenin kurulması ya da müzakeresi mümkün ise o yolun tercih edilmesi gerektiği kabul edilmektedir⁸⁷.

2.3.4.3. Veri Sorumlusunun Tâbi Olduğu Yasal Yükümlülük

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 6 (c) maddesi uyarınca kişisel verilerin, veri sorumlusunun tâbi olduğu bir yasal yükümlülüğe uyum için gerekli olduğu zaman işlenebileceği belirtilmektedir. Sosyal güvenlik mevzuatı, vergi mevzuatı, finans kuruluşları bakımından kara para aklama ve yolsuzlukla mücadeleye ilişkin düzenlemeler kapsamında veri sorumluları tarafından gerçekleştirilen bildirimler de dâhil olmak üzere bu gibi veri işleme faaliyetleri bu kapsamda örnek verilebilir. Bu hukuka uygunluk hali kapsamında amaçla sınırlı olma ve gereklilik ilkeleri göz önünde bulundurulmalıdır. Bu doğrultuda veri sorumlusunun gerçekten bir kanuni yükümlülüğünün olması şartı aranmalıdır. Veri sorumlusunun kanuni yükümlülüğünü yerine getirebilmek için, örneğin verileri anonim halde paylaşması söz konusu yükümlülüğünü yerine getirmesi için yeterli ise o halde anonimleştirerek verileri paylaşması gerekmektedir. Bireylere ilişkin kişisel verileri olduğu halde paylaşması yahut yükümlülüğünün yerine getirilmesi için gerekenden fazla kişisel veriyi paylaşması bu kapsamda değerlendirilemeyecektir.

Yönerge'nin yürürlük sürecinde veri sorumlusunun Avrupa Birliği içerisinde yerleşik olmaması durumunda Avrupa Birliği dışında bir devletin getirmiş olabileceği yasal yükümlülüklerin nasıl uygulanacağı doktrinde tartışılmıştır⁸⁸. Nitekim Safe Harbor

⁸⁷ Avrupa Veri Koruma Denetmeni, "Opinion of the European Data Protection Supervisor on the Data Protection Reform Package", Par. 114.

⁸⁸ Tekin, **a.g.m.**, s. 233; Article 29 Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", s.19; Kinton John D, "Managing the EU-US Discovery Conflict", Law 360, 2008, (Çevrimiçi) <https://www.law360.com/articles/72082>, 18 Nisan 2018.

Kararı'nın geçersiz sayılmasında Avrupa Birliği dışındaki devletlerin getirmiş olduğu yasal yükümlülüklerin yaratmış olduğu problemler önemli bir rol oynamıştır⁸⁹. Tüzük ile, veri sorumlusunun hangi hukuktan kaynaklanan hukuki yükümlülüklerini yerine getirmesi sırasında, kişisel verilerin bu hukuka uygunluk sebebine dayanarak işleyebileceğine ilişkin tartışmaları sona erdirmek için; ilgili hükme, “*Avrupa Birliği Hukuku ya da Üye Devletler hukuku*” ibaresi eklenmiştir⁹⁰. Bu durum açıkça veri sorumlusunun üçüncü bir ülkenin yerel mevzuatından kaynaklanan nedenlerle kişisel verileri işleyebilmesini ilgili hukuka uygunluk sebebi bakımından kapsam dışı bırakmaktadır.

2.3.4.4. Fiili İmkânsızlık Durumunda Yaşamsal Çıkarların Koruması

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 6 (d) maddesi kapsamında kişisel verilerin ilgili kişinin ya da bir başka gerçek kişinin yaşamsal çıkarlarının korunması amacıyla işlenmesi bir hukuka uygunluk hali olarak yer almaktadır⁹¹. Belirtmek gerekir ki söz konusu düzenleme, Yönerge'de düzenlenen özel nitelikli kişisel verilerin işlenmesi için aranan ilgili hukuka uygunluk sebebine yaklaştırılmıştır. Doktrinde kimi zaman yaşamsal çıkar yerine hayati çıkar deyimi de tercih edilmekte ve korunmak istenen çıkarların kapsamına ilişkin bir belirsizlik olduğu bazı akademik çalışmalarda dile getirilmektedir⁹². Ancak Avrupa Birliği Genel Veri Koruma Tüzüğü'nün giriş bölümü madde 46 kapsamında kişisel verilerin işlenmesinin, ilgili kişinin ya da başka bir gerçek kişinin yaşamı için gerekli olan bir menfaatin korunması amacıyla gerçekleştirilmesi halinde hukuka uygun olarak kabul edilmesi gerektiği

⁸⁹ Avrupa Adalet Divanı'nın, Safe Harbour Kararı'nı geçersiz sayan kararında, Amerika Birleşik Devletleri yetkililerinin Avrupa Birliği'nden Amerika Birleşik Devletleri'ne aktarılan kişisel verilere erişim sağladığını ve verilerin ulusal güvenliğin korunması için kesinlikle gerekli olanın ötesinde ve ilk aktarma amacıyla bağdaşmayan biçimde işlediğini tespit etmiş ve ihlal kararı vermiştir, Avrupa Adalet Divanı, C-362/14, par. 94.

⁹⁰ Tüzük, Giriş Bölümü, par. 45; Tüzük, m. 6/1 (c), 6/3.

⁹¹ Avrupa Birliği Genel Veri Koruma Tüzüğü'nde, “*protect the vital interests of the data subject or of another natural person*” ifadesi yer almaktadır.

⁹² Murat Uygun, Avrupa Birliği 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması, (Yayımlanmamış Yüksek Lisans Tezi), **Gazi Üniversitesi Sosyal Bilimler Enstitüsü**, Ankara, 2010, s. 58.

belirtilmiştir⁹³. Bu bakımdan söz konusu hüküm ile korunmak istenen unsurun kişinin can güvenliğine ilişkin olduğunu söylemek mümkündür. Bu nedenle, yaşamsal çıkarların korunması kapsamında kişisel veri işleme faaliyeti ise sadece acil bir kapsam için söz konusu olabilmektedir.

Article 29 Working Party, yaşamsal çıkarların korunması için kişisel veri işleme faaliyetinin sadece ölüm kalım anlarında ya da ilgili kişinin sağlığına ilişkin bir tehlikenin oluşması şartı ile gerçekleştirilebileceğini belirtmiştir⁹⁴. Söz konusu hukuka uygunluk sebebi, gereklilik ve ölçülülük ilkeleri ile sınırlandırılarak yorumlanmalıdır. Örneğin çığ altında kalmış ya da kaybolmuş birinin konum bilgilerine sadece tehlikenin gerçekleştiği muhtemel zaman dilimi için ulaşılması gerekmektedir. Her ne kadar Tüzük'te hüküm, lafzı itibarı ile muhtemel tehlikenin önlenmesi için bir aciliyet durumu aranmıyor olsa da bu hukuka uygunluk sebebinin uygulanması bakımından kümülatif olarak olası tehlikelerin hepsi için önceden bir veri işleme faaliyetinin yapılması hüküm amacı ile bağdaşmayacaktır.

Article 29 Working Party de hükmün ruhuna uygun olarak kısıtlayıcı bir yorum yapmanın gerekli olduğunu belirtmektedir. Bu sınırlama, geçerli bir rızanın alınabileceği haller bakımından değerlendirilmeli, yaşamsal çıkarlar için kişisel verilerin işlenmesi en son ihtimal olarak, rızasını açıklayamayacak yahut rızasını açıklasa bile buna sonuç bağlayamayacak durumda olan kişiler bakımından kişisel veri işlemenin bir sebebi olarak kullanılmalıdır. İlgili kişinin yaşamsal çıkarları için bir kişisel veri işleme faaliyetinden bahsedebilmek için acil ve sağlığa ilişkin bir durumun söz konusu olması gerekmektedir⁹⁵.

2.3.4.5. Kamu Yararı ya da Resmi Bir Yetki Kullanımı

⁹³ Söz konusu hüküm Avrupa Birliği Veri Koruma Yönergesi'nin Giriş Bölümü, par. 31'de de yer almaktadır.

⁹⁴ Article 29 Working Party, **a.g.e.**, s. 20.

⁹⁵ Lucas Bergkamp, Jan Dhont, "Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web", **The Edi Law Review, Legal Aspects of Paperless Communication**, Cilt 7, Sayı 2-3, Kluwe Law International, 2000, s. 81.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 6 (e) maddesi uyarınca kişisel veriler, kamu menfaati ya da verilerin açıklandığı üçüncü bir şahsın veya veri sorumlusunun sahip olduğu bir resmi bir yetkinin kullanılması için gerekli olması halinde işlenebilecektir. Bir diğer ifade ile kamu menfaati veya kamu düzeni gereği veri sorumlusunun ya da verilerin açıklandığı kişi veya kurumun görevinin ifası amacı ile kişisel veriler işlenebilecektir. İlgili hüküm Avrupa Birliği Veri Koruma Yönergesi'nde de aynı şekilde yer almış ve maddede yer alan kamu menfaati ibaresi belirsiz ve yoruma açık olduğu sebebiyle tartışılmıştır⁹⁶. Ancak ilgili hükmün kamu menfaati gerekçesiyle herhangi bir sınırlama olmaksızın veri işlemlerinde araç olarak kullanılmasını engellemek adına dar yorumlanması gerekmektedir⁹⁷.

Yasal yükümlülüğün yerine getirilmesine ilişkin hukuka uygunluk sebebinde olduğu gibi kamu yararı hukuka uygunluk sebebi bakımından da bir yer sorunu mevcuttur. Üye devletler dışında başka bir devletin getirmiş olduğu yetki kapsamında kişisel verilerin işlenip işlenemeyeceğinin tartışılması gerekmektedir. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün giriş bölümünde⁹⁸ vergi veya gümrük kurumları arasında veya sosyal güvenlik konularında yetkili birimler arasında uluslararası veri aktarımı örnek olarak gösterilmekle birlikte söz konusu hukuka uygunluk sebebinin uygulama alanı bulabilmesi için yalnızca üçüncü ülkenin kamusal yararının bulunmasının yeterli olmadığı, Avrupa Birliği üyesi devletin de somut olayda kamusal bir çıkarının bulunması gerektiği ifade edilmektedir⁹⁹.

Önemle belirtmek gerekir ki söz konusu hukuka uygunluk sebebinin unsurları bakımından gereklilik ve ölçülülük prensipleri mümkün mertebe dikkate alınmalı ve bu hukuka uygunluk sebebi dar yorumlanmalıdır. Kamu yararı ve yetki kullanımı kavramlarının üye devletlerin mevzuatlarda tanımlı olması ve bu tanımlı aşan şekilde kişisel veri işleme faaliyetlerinin yürütülmemesi gerekmektedir. Bu doğrultuda hukuksal taleplerin yerine getirilmesi her ne kadar bu hukuka uygunluk sebebi ile

⁹⁶ Tekin, **a.g.e.**, s. 234.

⁹⁷ Küzeci, **a.g.e.**, s.189.

⁹⁸ Tüzük, Giriş Bölümü, par. 112; benzer düzenleme için bkz. Yönerge, Giriş Bölümü, par. 58.

⁹⁹ Article 29 Working Party, "Working Document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995", WP 114, 25 Kasım 2005, s. 15.

bağdaşacak olsa da ölçülülük ilkesinin her zaman göz önünde bulundurulması gerekmektedir. Örneğin, Avrupa Birliği dışında yerleşik bir şirket ile Avrupa Birliği vatandaşı arasındaki uyuşmazlık yüzünden ilgili kişinin bilgileri yetkili mercilerin talebi doğrultusunda aktarılabilecektir ancak ilgili kişi dışındaki üçüncü kişilerin de dosyalarının kümülatif olarak gelecekteki olası uyuşmazlıklar adı altında paylaşılması ölçülülük ilkesi gereğince hukuka uygun olmayacaktır.

2.3.4.6. Veri Sorumlusunun Üstün Meşru Menfaati

Öğretide¹⁰⁰ pek çok tartışmaya konu olan meşru menfaat hukuka uygunluk sebebine ilişkin Yönerge’de aranan menfaat dengesi, Avrupa Birliği Genel Veri Koruma Tüzüğü’nde yer almaktadır. Buna göre veri sorumlusunun meşru menfaatlerinin ilgili kişinin menfaat veya temel hak ve özgürlüklerinin ağır basmaması kaydıyla kişisel veri işleme açısından hukuki dayanak teşkil edebileceği belirtilmektedir. Öncelikle belirtmek gerekir ki Tüzük kapsamında “meşru menfaat” ibaresiyle ne ifade edilmek istendiği açık bir şekilde tanımlanmamaktadır. Bu kavram, *“hukuk düzeni içerisinde cevaz verilen her türlü hukuki, iktisadi ya da kişisel menfaat”* olarak tanımlanmaktadır¹⁰¹. Avrupa Birliği Veri Koruma Yönergesi’nin giriş bölümünde ise *“şirketlerin ve diğer organların meşru olağan etkinlikleri”* ifadesi yer almaktadır¹⁰². Doktrinde bu ifadenin “meşru ticari çıkarlar” olarak algılanabileceği belirtilmektedir¹⁰³. Bazı yazarlar doğrudan pazarlama faaliyetlerinin veri sorumlusunun meşru çıkarları kapsamında değerlendirileceğini ve ilgili kişinin gizlilik çıkarlarının veri sorumlusunun iş çıkarlarını geçersiz kılmadığını savunmaktadırlar¹⁰⁴. Tüzük’ün giriş bölümünde ilgili kişinin müşteri, veri sorumlusunun ise hizmet sağlayan konumunda bulunduğu hallerde meşru menfaat kapsamında veri işleme faaliyetlerinin hukuka uygun olabileceği ama her halükarda gereklilik ve ölçülülük bakımından somut olay şartları ışında bir değerlendirme yapılması gerektiği belirtilmektedir. Yine herhangi bir dolandırıcılığın önlenmesi için ölçülü ve gerekli veri işleme faaliyetinin meşru menfaat kapsamında değerlendirilmesi gerekeceği giriş

¹⁰⁰ Kuner, **a.g.e.**, s. 76; Çekin, **a.g.e.**, s. 72.

¹⁰¹ Çekin, **a.g.e.**, s. 72.

¹⁰² Avrupa Birliği Veri Koruma Yönergesi, Giriş Bölümü, par. 30.

¹⁰³ Küzeci, **a.g.e.**, s. 217.

¹⁰⁴ Lucas Bergkamp, Jan Dhont, **a.g.e.**, s. 81-82.

bölümünde ifade edilmektedir.¹⁰⁵. Ayrıca Kişisel Verileri Koruma Kurulu tarafından verilmiş güncel bir karar¹⁰⁶ aksine, Tüzük'ün Giriş Bölümü'nde grup şirketler arası müşteri ve çalışan verilerinin aktarılmasının meşru menfaat kapsamında değerlendirilebileceği belirtilmektedir¹⁰⁷.

Yönerge'nin uygulandığı dönemde hazırlanan ve büyük ölçüde Tüzük döneminde de uygulama alanı bulacak olan görüşler ve mahkeme kararları doğrultusunda, söz konusu hukuka uygunluk sebebinin uygulanabilmesi için yarışan menfaatler doğrultusunda bir değerlendirme yapmak gerekmektedir¹⁰⁸. Mevzu bahis yarışan menfaatler madde kapsamında da belirtilen veri sorumlusunun menfaati ile ilgili kişinin temel hak ve özgürlükleridir. Veri sorumlusunun menfaati ile ilgili kişinin temel hak ve özgürlükleri kapsamlı bir şekilde değerlendirildikten sonra ve iki menfaat arasındaki denge gözetilerek kişisel veriler işlenebilecektir. Bu değerlendirme bir uygunluk testi olarak veri sorumlusu ve ilgili kişi arasındaki ilişkiyi, veri işlemenin olası sonuçları ve etkilerini, ilgili kişinin makul beklentilerini göz önünde bulundurmaktadır.

Özellikle ilgili kişinin söz konusu veri işleme faaliyetini makul şartlar altında öngöremeyeceği kanaatine varılması halinde veri sorumlusunun meşru menfaatinin varlığına dayanamayacağı kabul edilmektedir¹⁰⁹. Bununla birlikte pazarlama faaliyetlerinin veri sorumlusunun meşru menfaati kapsamında değerlendirilip değerlendirilemeyeceğine ilişkin olarak da Tüzük giriş bölümünde doğrudan pazarlama faaliyetlerinin veri sorumlusunun meşru menfaati kapsamında değerlendirilebileceği belirtilmektedir. Ayrıca grup şirket yapısı içerisinde yer alan veri sorumlularının yönetim yapıları gereğince müşteri ve çalışan verilerini grup

¹⁰⁵ Tüzük, Giriş Bölümü, par. 47.

¹⁰⁶ Kurum internet sitesinde paylaşılan karar özetinde “[b]ir şirketler topluluğu bünyesinde yer alan birden çok veri sorumlusu şirketler arasında veri aktarımı gerçekleştirilmesinin, üçüncü kişiye veri aktarımı olarak değerlendirildiği, ... İş başvurusunda bulunan bir adayın açık rızası olmadan kişisel verilerinin bir şirketler topluluğu altında yer alan veri sorumluları arasında aynı veri tabanını kullanmak suretiyle paylaşılmasının Kanunun 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil etmesi..” ifadesi yer almaktadır.

¹⁰⁷ Tüzük, Giriş Bölümü, par. 48.

¹⁰⁸ Article 29 Working Party, “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”, s. 19; Avrupa Adalet Divanı, Rîgas Davası, C-13/16, 4 Mayıs 2017.

¹⁰⁹ Tüzük, Giriş Bölümü, par. 47.

şirketleri arasında aktarabilmesinin meşru menfaat kapsamında görülebileceği belirtilmektedir¹¹⁰.

İlgili kişinin kendi özel durumları çerçevesinde ve ücretsiz olarak kişisel veri işleme faaliyetine itiraz hakkına sahip olması gerektiği ifade edilmektedir¹¹¹. Şeffaflık sağlamak açısından veri sorumlusu, kişisel verisi işlenen ilgili kişiyi dayanmakta olduğu meşru menfaatler ve veri işlemenin konusu olmaya itiraz hakkı kapsamında açıkça bilgilendirmek ve bu meşru menfaatleri belgelemekle yükümlü kılınmaktadır.

Yönerge'den farklı olarak Tüzük kapsamında çocukların hususi olarak korunması gerektiği göz önünde bulundurularak özellikle ilgili kişinin bir çocuk olduğu durumlarda daha hassas bir değerlendirme yapılması gerektiği belirtilmektedir. Yine Yönerge'de yer almamakla birlikte kamu makamlarının meşru menfaat hukuka uygunluk sebebine dayanarak kişisel veri işleme faaliyetlerinde bulunmaması gerektiği açık bir şekilde düzenlemiştir.

2.3.5. Avrupa Birliği Genel Veri Koruma Tüzüğü ile Getirilen Yenilikler

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün en önemli etkisi ve getirdiği değişiklik yukarıda da belirtilmiş olduğu üzere etki alanının birlik sınırlarını aşacak şekilde düzenlenmiş olmasıdır. Avrupa Birliği sınırları içerisinde faaliyet gösteren tüm şirketlerin düzenlemenin getirmiş olduğu şartlara uyum sağlaması beklenmektedir. Bunun yanı sıra Avrupa Birliği Genel Veri Koruma Tüzüğü'nde yer alan tanımlar büyük ölçüde Yönerge'de yer alan tanımlar ile paralellik arz ederken, veri işlemenin kısıtlanması, profillemeye, psödosomasyon, genetik veri, biyometrik veri, sağlık verisi, yerleşim yeri, bağlayıcı şirket kuralları gibi Yönerge'nin uygulanma süreci içerisinde Avrupa Birliği Adalet Divanı tarafından verilen kararlar kapsamında açıklanan tanımlara yer verilmektedir.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün getirdiği yenilikler aşağıda kısaca özetlenmiştir:

¹¹⁰ Tüzük, Giriş Bölümü, par. 48.

¹¹¹ Tüzük, Giriş Bölümü, par. 47.

- a. Avrupa Birliği genelinde merkezi bir veri koruma kurumunun kurulması kararlaştırılıp ve bu sayede Avrupa Birliği vatandaşlarına merkezi veri koruma kurumu veya kendi ülkelerinde yer alan veri koruma otoritesine başvuru imkânı tanınmaktadır¹¹².
- b. Bireylere kendilerine ait verinin kullanması için geçerli bir sebep kalmamışsa bu verinin silinmesini talep etme hakkı, genel bir ilke olmanın yanı sıra, ayrı bir hüküm olarak yer da almaktadır¹¹³.
- c. Birlik içerisinde satılacak ürün ve hizmetlerin mahremiyet hakkına saygı çerçevesinde tasarlanması ve üretilmesine ilişkin “**Privacy by Design**” ve baştan itibaren mahremiyetin öne çıkarılmasına ilişkin olarak “**Privacy by Default**” ilkesi yer almaktadır¹¹⁴.
- d. Tanımlar bölümü, teknolojik gelişmeler de dikkate alınarak güncellenmiştir¹¹⁵.
- e. Veri koruması ihlallerinin bildirilmesi için yeni bildirim usulleri düzenlenmektedir¹¹⁶.
- f. Veri koruması politikasında çocukların korunması ile ilgili özel hükümler öngörülmektedir¹¹⁷.

¹¹² "One-Stop Shop" ilkesi olarak ifade edilen bu düzenleme veri sorumlularının tek bir Veri Koruması Ulusal Denetim Otoritesi ile muhatap olması sonucunu doğurmaktadır. Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 56.

¹¹³ Avrupa Birliği Genel Veri Koruma Tüzüğü m. 17.

¹¹⁴ Avrupa Birliği Genel Veri Koruma Tüzüğü m. 25; Literatürde ilgili kavramlar “Tasarımla Veri Koruma” ve “Varsayılan Ayarlarla Veri Koruma” olarak tercüme edilmektedir, bkz. Başalp, **a.g.m.**, s. 92; Çekin, **a.g.e.**, s. 53; Taştan, s. 18-19. Ayrıca “Tasarımdan İtibaren Veri Koruma” ve “Başlangıçtan İtibaren Veri Koruma” olarak de çevrilmiştir, bkz. Akıncı, **a.g.m.**, s. 18. “Tasarımdan itibaren veri koruma” ve “varsayılan ayarlarla veri koruma” ilkeleri uyarınca teknolojik gelişmelerin etkisi ile çeşitlenen veri işleme faaliyetleri bakımından veri sorumlularına veri işleme faaliyetinin, bireylerin hak ve özgürlükleri açısından oluşturabileceği çeşitli sıkıntılar ve riskler uyarınca hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında veri koruma ilkelerinin etkili bir şekilde uygulanması özel ve olağan olarak sağlama yükümlülüğü getirilmektedir. Paul B. Lambert, **a.g.e.**, s. 329-339.

¹¹⁵ Avrupa Birliği Genel Veri Koruma Tüzüğü m. 4.

¹¹⁶ Avrupa Birliği Genel Veri Koruma Tüzüğü m. 33-34, veri sorumlularına veri korumasına ilişkin ihlalinin meydana gelmesinden itibaren mümkün olan en kısa sürede ve her halükârda en geç 72 saat içerisinde veri koruma otoritesine bildirim zorunluluğu getirilmiştir. Ayrıca veri sorumlusu, ilgili kişiye de bildirimde bulunmakla yükümlü kılınmıştır.

¹¹⁷ Avrupa Birliği Genel Veri Koruma Tüzüğü m. 8, özellikle bilgi toplumu hizmetleri kapsamında kişisel verileri işlenen çocuklar bakımından geçerli rıza koşulları ayrıca düzenlenmiştir. Bunun yanı sıra, madde 6’da yer alan meşru menfaat istisnası ve madde 57’deki denetleyici kurumların faaliyetlerine yönelik olarak çocukların kişisel verilerine ilişkin özel düzenlemeler bulunmaktadır.

- g. Veri koruması görevlisi atama yükümlülüğü düzenlenerek yer almaktadır¹¹⁸.
- h. Veri koruması ihlali hallerinde uygulanacak cezalar arttırılmıştır¹¹⁹.
- i. İlgili kişinin rızasının alınması hususunda daha yüksek bir standart öngörülmektedir¹²⁰.
- j. Riskli veri koruması işleme faaliyetleri öncesinde veri koruması etki analizi gerçekleştirilmesi zorunluluğu getirilmektedir¹²¹.
- k. "Veri sadeleştirilmesi" ilkesi lafzi olarak da Avrupa Birliği Genel Veri Koruma Tüzüğü metni içinde hüküm altına alınmıştır¹²².
- l. Kişisel verilerin korunmasına ilişkin genel ilkeleri veri sorumlusunun yerine getirmesine ilişkin "hesap verilebilirlik" şartı getirilmiştir¹²³.

Avrupa Birliği'nde veri koruması reformunu tetikleyen temel unsur, topluluğun yapısı ve yönergelerin birlik hukukundaki karşılığı nedeni ile üye devletler arasındaki farklı uygulamalar olmuştur. Temel amaç, bütün üye devletler için yeknesak bir düzenleme yaparak veri koruması uygulamalarında birliği sağlamak kişisel verinin birlik

¹¹⁸ Avrupa Birliği Genel Veri Koruma Tüzüğü m. 37, işlenen kişisel veri niteliği ve veri işleme kapsamı uyarınca veri sorumluları ve veri işleyenler bakımından veri koruma görevlisi atanması bir zorunluluk haline getirilmiştir. Madde 38'de ise veri koruma görevlisinin görevlerini yerine getirmesi sırasında veri sorumlusu yahut işleyenden talimat almaması gerektiği belirtilmiştir.

¹¹⁹ Avrupa Birliği Genel Veri Koruma Tüzüğü m. 83, kişisel verilerin korunmasına ilişkin düzenlemelerin ihlalleri neticesinde verilebilecek cezalar için 20 milyon Euro veya hizmet sağlayıcının küresel gelirinin yüzde dördü olacak şekilde üst sınır belirlemesi yoluna gidilmiştir. Mevcut düzenlemeler çerçevesinde Avrupa Birliği üye devletleri hukukları arasında ihlallere ilişkin olarak tesis edilmiş olan en yüksek ceza beş yüz bin pound ile Birleşik Krallık'ta düzenlenmekte idi.

¹²⁰ Avrupa Birliği Genel Veri Koruma Tüzüğü m.7; Giriş bölümü 32. paragrafında özellikle sosyal medya uygulamaları yahut internet tarayıcıları tarafından sunulan gizlilik koşulları karşısında sessiz kalan bireylerin sessiz kalmalarına rıza verdiklerine ilişkin sonuç bağlanmaması gerektiği belirtilmiştir.

¹²¹ Avrupa Birliği Genel Veri Koruma Tüzüğü m. 35; özellikle günümüzde gelişen teknoloji ışığında, yeni geliştirilen veri işleme metodlarının kullanıldığı veri işleme faaliyetleri bakımından bireylerin kişisel verilerinin korunmasına ilişkin yüksek bir riskin oluşabileceği durumlar için söz konusu veri işleme faaliyetinin ve yönteminin kapsamı, niteliği, bağlam ve amacı da dikkate alınarak öncelikle bir etki değerlendirmesi yapılması zorunluluğu "**Data protection impact assessment**" olarak veri sorumlularına getirilmiştir. Özellikle otomatik veri işleme faaliyetleri ve profil oluşturmaya yönelik kişisel veri işleme faaliyetleri bakımından bu zorunluluk getirilmiştir.

¹²² Avrupa Birliği Genel Veri Koruma Tüzüğü m. 5, kişisel verilerin işlenmesinde uyulacak genel ilkelerden olan verilerin işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlı olarak işlenmesi ilkesi kısaca veri minimizasyonu, veri sadeleştirilmesi olarak anılmıştır.

¹²³ Avrupa Birliği Genel Veri Koruma Tüzüğü m. 5/2'de kişisel verilerin işlenmesine dair genel ilkelere veri sorumlularının uyum yükümlülüğünün yerine getirilmesine ilişkin bir hesap verilebilirlik ilkesi eklenmiştir. Bir başka deyişle, veri sorumluları genel ilkelere uyma yükümlülüklerini yerine getirdiğini göstermekle ayrıca özel olarak yükümlü kılınmıştır.

içerisinde güvenli şekilde serbest dolaşımına imkân yaratmak ve ilgili kişiyi korumaktır¹²⁴.



¹²⁴ Avrupa Birliği Genel Veri Koruma Tüzüğü'ne ilişkin getirilen düzenlemelere ve veri işleyen şirketler bakımından yer alan yükümlülöklere ilişkin olarak bkz. Tikkinen-Piri, Rohunen, Markkula, **a.g.m.**, s. 138 vd.

ÜÇÜNCÜ BÖLÜM

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

3.1. Genel Olarak

Türkiye’de yakın geçmişe kadar kişisel verilerin korunmasına ilişkin yeterli, açık ve müstakil bir yasal düzenleme ile kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurum bulunmamaktaydı. Kişisel verilerin kontrolsüz şekilde işlenmesi, bireylerin temel haklarının ihlal edilmesine sebep olmaktaydı. Ancak Türk hukuku kapsamında kişisel verilerin tamamen korumasız olduğunu söylemek de doğru olmayacaktır. Nitekim birçok anayasanın aksine Türkiye Anayasası’nda kişisel verilerin korunmasının sağlam dayanakları bulunmaktadır (m. 20/3). 2010 yılında 5982 sayılı Kanun’la Anayasa’da yapılan değişiklikle birlikte kişisel verilerin korunması temel bir anayasal hak olarak koruma altına alınmış ve detaylı düzenlemelerin kanunla getirileceği hükme bağlanmıştır.

5237 sayılı Türk Ceza Kanunu’nun 135 ve devamı maddelerinde kişisel verilerin hukuka aykırı olarak işlenmesi suç olarak düzenlenmektedir. Ancak hukuka aykırı fiiller Türk Ceza Kanunu’nda belirtilmediğinden ve bu konuda özel bir kanun da olmadığından, uygulamada sorunlar yaşanabilmekteydi.

Kişisel verilere ilişkin bir başka koruma ise Medeni Kanun’un kişiliği koruyan hükümlerinden doğmaktadır. Türk Borçlar Kanunu’nda ise işçinin kişiliğinin korunmasına ilişkin olarak özel hüküm bulunmaktadır. Bunun yanı sıra İş Kanunu, Elektronik İmza Kanunu, Noterlik Kanunu, Bankalar Kanunu, Adli Sicil Kanunu ve Nüfus Kanunu gibi kanunlar ve telekomünikasyon, internet, sağlık, elektronik ticaret gibi alanlarda bulunan sektör bazlı düzenlemeler kişisel verilerin korunmasına ilişkin özel hüküm barındırmaktadırlar.

3.1.1. 1982 Anayasası

Kişisel verilerin korunmasını talep etme hakkı Avrupa Birliği üye devletlerinde temel bir insan hakkı olarak kabul edilmesine rağmen sadece bazı üye ülkeler tarafından

anayasalarında temel bir insan hakkı olarak düzenlenmiştir¹. Türkiye Cumhuriyeti 1924 Anayasası'nda özel hayatın gizliliğiyle ilgili çeşitli hükümlere yer verildiği, ancak kişisel verilerin korunmasının bağımsız bir hak olarak yer almadığı görülmektedir. 1961 ve 1982 Anayasa'larında ise bu hak açıkça ve bağımsız olarak düzenlenmiş durumdadır. Belirtmek gerekir ki özel hayatın gizliliği bir özgürlükten ziyade hak alanı olarak düzenlenmiştir. Hak ve özgürlük kavramları, hakkın talep edilebilir yönü bulunması, özgürlüğün ise dokunulmazlığı ifade etmesi yönü ile birbirinden ayrılmaktadır². Bu bakımdan kişisel verilerin korunması ve özel hayatın gizliliğinin bir hak olarak tesis edilmesi yerindedir.

Kişilik hakkını temel bir hak olarak güvence altına alan 1982 Anayasası'nın ikinci bölümü, oldukça geniş bir temel haklar listesi içermektedir. Buna göre, *“herkes kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve özgürlüklere”* sahiptir. Kişisel verilerin korunması hakkı, 2010 Eylül ayında yapılan referandumla kabul edilen anayasa değişiklikleri³ ile Anayasanın 20. maddesine dâhil edilmiştir. Böylelikle, kişisel verilerin korunmasına ilişkin hak, anayasal güvenceye kavuşmuştur. Değişiklik ile, ilgili maddeye *“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir”*

¹ Bu ülkelerde anayasal düzeyde açık bir şekilde kişisel verilerin korunması hakkına yer verilmiştir. Örneğin; Belçika Anayasası'nda (1831), Kıbrıs Anayasası'nda (1960), İsveç Anayasası'nda (1975), Portekiz Anayasası'nda (1976) ve İspanya Anayasası'nda (1978) kişisel verilerin korunmasına ilişkin düzenlemelere yer verildiği görülmektedir. Bununla birlikte Avusturya ve Macaristan'da da zaman içerisinde benzer düzenlemelere ihtiyaç doğrultusunda yer verilmiştir; Aydın Akgül, “Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi” **Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı**, (Yayınlanmamış Doktora Tezi), Kocaeli, 2013, s. 263.

² Bülent Tanör, Necmi Yüzbaşıoğlu, **1982 Anayasasına Göre Türk Anayasa Hukuku**, 8. Baskı, İstanbul, Beta, Aralık, 2006, s. 119.

³ 7 Mayıs 2010 tarihli ve 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun ile yapılan Anayasa değişiklikleri 12/9/2010 tarihinde Halkoyuna sunulurken kabul edilmiş, buna ilişkin 22 Eylül 2010 tarihli ve 846 sayılı Yüksek Seçim Kurulu Kararı 23 Eylül 2010 tarihli ve 27708 sayılı Resmî Gazete'de yayımlanmıştır.

hükmü eklenmiştir. Bu doğrultuda Anayasa’da belirtilen kişisel verilerin korunmasını isteme hakkı kişisel verilerle ilgili bilgilendirme, erişim, düzeltme ve sildirme hakkı ile kişisel verilerin toplanma anında belirtilen amaç doğrultusunda kullanılıp kullanılmadığını öğrenme hakkını da kapsamaktadır. Söz konusu hüküm ile kişisel verilerin korunmasına ilişkin sınırlandırmaların ihdasının kanun koyucuya bırakılmış olması ve hüküm ile getirilen kurallara uyulmasını denetleyen bağımsız bir kurumun oluşturulmasına yer verilmemiş olması eleştiri konusu olmuştur⁴.

Tüm hak ve özgürlüklerde olduğu gibi kişisel verilerin korunmasına ilişkin hak da sınırsız ve mutlak bir hak değildir. Hukuken gerekli şartların oluşması halinde diğer hak ve özgürlükler lehine sınırlandırılabilir.

Ülkemizde, temel hak ve özgürlüklerin olağan dönemlerde nasıl sınırlandırılacağına ilişkin usul ve esaslar Anayasa’nın 13. maddesinde düzenlenmektedir. Anayasa’nın 13. maddesi gereğince, temel hak ve özgürlükler, yalnızca Anayasa’nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilmektedir.

Anayasa Mahkemesi, kişisel verilere ilişkin hakların ancak kanunla sınırlanacağına dair, vermiş olduğu kararda⁵, “*Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı*” amaçladığını tespit ederek, “*kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler*” sebebiyle kişisel verilerin geçmişte olduğundan çok daha fazla korunmaya muhtaç olduğunu ifade etmektedir. Anayasa Mahkemesi kararında, Anayasa’nın 20. maddesinin 3. fıkrasının son cümlesinde, “*Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*” hükmüne yer verildiğini ve “*yasama yetkisinin devredilmezliği ilkesi gereğince,*

⁴ Elif Küzeci, “Anayasal Bir Hak: Kişisel Verilerin Korunması”, **Bilişim Dergisi**, sayı 128, Ankara, Türkiye Bilişim Derneği, Ocak 2011, s. 146. (Çevrimiçi) <http://www.bilisimdergisi.org/s128/pdf/142-149.pdf> 24 Nisan 2018.

⁵ Anayasa Mahkemesi Kararı, Esas Sayısı: 2013/122, Karar Sayısı: 2014/74, Karar Tarihi: 9 Nisan 2014, Resmi Gazete Yayınlanma Tarihi: 26 Temmuz 2014 Sayısı: 29072.

Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi” verilemeyeceğine hükmederek Anayasa’da öngörülen kanuni düzenlemenin mutlaka gerçekleştirilmesi gereğinin altını çizmektedir.

Anayasa’nın 20. maddesi dışında, doğrudan “kişisel veri” ifadesine yer verilmese de kişisel verilerin korunmasına temel oluşturacak çeşitli hükümler yer almaktadır. Bu kapsamda Anayasa’nın giriş bölümünde 6. paragrafta yer alan insan onuru, 2. maddede yer alan hukuk devleti ilkesi, 17. maddede yer alan bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı, 20. maddede yer alan özel hayatın ve aile yaşamının gizliliği hakkı, 21. maddede bulunan konut dokunulmazlığı, 22. maddede bulunan haberleşmenin gizliliği, 15. ve 24. maddelerde yer alan dini ve vicdani kanaatleri açıklamaya zorlanamama ve 25. maddede yer alan düşünce ve kanaatleri açıklamaya zorlanamama hükümleri, özel hayatın korunması ve dolayısı ile kişisel verilerin korunması hakkı ile bağlantılı olup sağlamış oldukları anayasal garantiler kişisel verilerin korunmasına ilişkin normatif temelleri oluşturmaktadır⁶.

3.1.2. Türk Medeni Kanunu

Türk Medeni Kanunu’nun Kişiler Hukuku kitabının “Kişilik” bölümünde yer alan kişiliğin korunmasına ilişkin hükümler 23, 24, ve 25. maddelerde düzenlenmiştir. Kişilik hakkının doktrinde yer alan tanımları⁷ ve Yargıtay’ca⁸ kabul edilen kapsamı doğrultusunda kişisel veriler kişilik hakkı altında değerlendirilmektedir. Bu doğrultuda kişiliğin korunmasına ilişkin ilgili maddelerin sağlamış oldukları korumaya yönelik olarak doktrindeki hâkim görüşe göre, Medeni Kanun’un 23. maddesi, kişinin kendi rızası ile kişiliğine yönelmiş saldırılara karşı kişiliği korurken, 24. madde ise rıza dışı saldırılara karşı kişiliğe koruma sağlamaktadır⁹. Kişiliğe

⁶ Küzeci, **a.g.e.**, s. 287.

⁷ Bu tanımlara ilk bölümde kişisel verinin unsurlarının incelendiği başlık altında kişi, kişilik tartışmaları altında yer verilmiştir.

⁸ Yargıtay 4. Hukuk Dairesi’nin 10.04.2008 tarihli 9966/2008 esas 5096/2008 karar sayılı kararında, “kişinin doğumla kazandığı, bağımsız varlığını ve bütünlüğünü oluşturan, hayat, beden ve ruh tamlığı, vicdan, din, düşünce ve çalışma özgürlüğü, onuru, ismi, resmi, sırları ile aile bütünlüğü ve duygusal değerlerinin tümü kişilik hakkını oluşturur” ifadesine yer verilmiştir.

⁹ Dural, Ögüz, **a.g.e.**, s. 136; Oğuzman, Seliçi, Oktay Özdemir, **a.g.e.**, s. 161.

yönelik saldırılar ve kişiliğin ihlali halinde başvurulabilecek hukuki yollar ise Medeni Kanun'un 25. maddesinde düzenlenmektedir.

Hak ve fiil ehliyetlerini koruyan 23. maddenin 1. fıkrası uyarınca kimsenin, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemeyeceği hüküm altına alınmıştır. Bu maddenin 2. fıkrasında ise kimsenin özgürlüklerinden vazgeçemeyeceği veya onları hukuka ya da ahlaka aykırı olarak sınırlayamayacağı, sınırlandırılmasına rıza gösteremeyeceği belirtilmektedir.

Kişinin rızası ile yapılmış bir hukuki işlem sonucu kişilik hakkının ihlalin oluşmasını önlemeye yönelik olan ilgili madde emredici bir hukuk kuralıdır. Madde 23 kişinin, kişiler arası eşitsizliklerden, kendi öngörüsüz davranışlarından, zayıf karakterli olmasından, zaaflarından ve gözü karalığından dolayı ortaya çıkabilecek olumsuz sonuçlardan korunmasını bir başka deyişle kişinin bizzat kendisine karşı¹⁰ bir iç koruma tesisini amaçlamaktadır. Bu madde hükmü ile kişilik hakkının korunması amacı doğrultusunda kişinin kendi rızasına sonuç bağlanmaması ya da aşırı sınırlandırılması söz konusu olabileceği için sözleşme özgürlüğünün kısıtlanması akla gelebilecektir.

Kişisel verilerin, kişilik hakkı çerçevesinde değerlendirilmesi ile söz konusu hükümlerin kişinin kendi rızasına dayanan saldırılara karşı da korunmasını sağlayacağından; kişisel verilerin işlenmesi amacı ile rıza vermiş bireylerin bu kapsamda korunmasının kabulü gerekmektedir. Bir başka deyişle kişisel verilerin kişinin rızası ile kullanılmasını ve aktarılmasını konu alan sözleşmeler, madde 23'e göre geçersiz sayılabilecektir¹¹. Ancak, ilgili maddenin 2. fıkrası sözleşme özgürlüğünü ve işlem güvenliğini tamamen ortadan kaldırmamak adına, kişinin özgürlüğünü sınırlayan her türlü hukuki işlemi değil, yalnızca hukuka veya ahlaka ve adaba aykırı olan işlemlerin geçersiz sayılacağını belirtmektedir¹². Söz konusu hüküm, kişinin kişisel verilerinin hukuka ve ahlaka aykırı işlemlere konu olması halinde bir koruma alanı yaratmaktadır. Maddenin ruhu gereği kişi özgürlüğün belirli bir ölçünün

¹⁰ Dural, Ögüz, **a.g.e.**, s. 136; Zevkliler, Acabey, Gökyayla, **a.g.e.**, s. 486.

¹¹ Aksoy, **a.g.e.**, s. 109.

¹² Dural, Ögüz, **a.g.e.**, s. 150; Oğuzman, Seliçi, Oktay Özdemir, **a.g.e.**, s. 199-200; Zevkliler, Acabey, Gökyayla, **a.g.e.**, s. 486.

üzerinde sınırlandırılması yahut tamamen ortadan kaldırılması yetkisi kişi elinden dahi alınmıştır¹³. Madde hükmü ile kişinin serbest karar verme özgürlüğünün korunması amaçlanmaktadır.

Buna karşılık Medeni Kanun'un 24. maddesinin 1. fıkrası, kişinin rızası hilafına gerçekleşen saldırılara karşı korunmasını hedeflemektedir. 2. fıkrada ise belirtilen hukuka uygunluk sebepleri¹⁴ olmaksızın saldırının her halükârda hukuka aykırı kabul edileceği belirtilmektedir¹⁵.

Yukarıdaki açıklamalardan anlaşılacağı üzere kişisel veriler, kişilik hakkı ve özel hayatın gizliliği kapsamında sınırlı çerçevede olsa da medeni hukuk kapsamında korunmaktadırlar. Ancak kişisel veriler, mahiyeti gereği daha hususiyet gerektiren bir korumaya ihtiyaç duymaktadır. Özellikle Medeni Kanun ile getirilen koruma büyük ölçüde saldırı gerçekleştikten sonra yahut bir saldırı tehlikesi varlığı halinde uygulanabilecektir. Bu doğrultuda kişilerin kişisel verileri özelinde daha geniş kapsamlı bir korumaya ihtiyaç duyduğunun kabulü gerekmektedir.

3.1.3. Türk Ceza Kanunu

Kişisel verilerin korunmasına ve hukuka aykırı olarak işlenmemesine ilişkin olarak 765 sayılı mülga Türk Ceza Kanunu'nda özel bir hüküm bulunmamakla birlikte özel hayatın gizliliğine ilişkin sınırlı şekilde "sırrın masuniyeti aleyhinde cürümler" başlığındaki hükümlere yer verilmiştir. Ancak bu düzenlemeler kişisel verilerin korunmasına ilişkin hükümler içermediği ve yeterli addedilemeyeceği için kişisel verilerin izinsiz olarak kaydedilmesi, paylaşılması hususları ceza hukuku alanında değerlendirilme olanağına kavuşmamıştır. 12 Ekim 2004 tarih ve 25611 sayılı Resmî Gazete'de yayımlanarak 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Türk

¹³ Dural, Ögüz, **a.g.e.**, s. 139.

¹⁴ Medeni Kanun m. 24/2 "*Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.*" Maddede yer alan hukuka uygunluk sebepleri temel olarak bu çalışma kapsamında ele alınmış olan kişisel verilerin işlenmesine ilişkin hukuka uygunluk sebepleri ile paralellik arz etmektedir.

¹⁵ Uygulamada özellikle bir sözleşmenin parçası ya da eki olarak bireyler kişisel verilerinin işlenmesini kabule zorlanmaktadır. Önceden hazırlanmış olan matbu bu metinlerin kişilik hakkına müdahale olarak genel işlem koşulları bakımından geçerliliğine ilişkin olarak bkz. aşağıda "3.2.5.1. Açık Rıza".

Ceza Kanunu ile birlikte 132. madde ve devamında “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” düzenlenmiştir. Kanun’un 135 ve devamı maddelerinde ise hususi olarak kişisel verilerin korunmasına yönelik temel ilkelerin bazılarını konu edinen hükümlere yer verilmektedir.

Türk Ceza Kanunu kapsamında, “kişisel verilerin kaydedilmesi” suç olarak düzenlenerek kişisel verileri hukuka aykırı şekilde kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilmesi öngörülmektedir. Madde gerekçesinde¹⁶ günümüzde hastaneler, sigorta şirketleri, bankalar, mağazalar gibi çeşitli kurum ve kuruluşlar tarafından kişilerle ilgili kayıtların bilgisayar ortamında aktarılıp saklandığı, bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişilerin büyük zararlara uğrayabileceği endişesiyle bilgilerin hukuka aykırı olarak kayda alınmasının suç olarak tanımlandığı belirtilmektedir. Gerekçede ayrıca, gerçek kişiye ilişkin her türlü bilginin kişisel veri olarak kabul edileceği ve suç konusunun kişisel veriler olduğu belirtilmiştir. Suç tanımında kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir. Maddenin 2. fıkrasında ise özel nitelikli kişisel¹⁷ veriler sayılarak bu verilerin hukuka aykırı olarak kaydedilmesi nitelikli hal olarak düzenlenmektedir.

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme başlıklı 136. maddede ise kişisel verileri, bir başkasına veren, yayan veya ele geçiren kişinin hukuka aykırı fiili suç olarak düzenlenmektedir. Türk Ceza Kanunu’nun 138. maddesinde ise kanunlarda öngörülen sürelerin dolmasına karşın kişisel verileri sistem içinden yok etmekle

¹⁶ Türkiye Büyük Millet Meclisi, Adalet Komisyonunca kabul edilen madde gerekçeleri, s. 219 (Çevrimiçi) <http://www.ceza-bb.adalet.gov.tr/>, 18 Nisan 2018

¹⁷ Maddenin 2. fıkrasında kişisel verilerin kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması hali ayrıca düzenlenmiştir. Belirtmek gerekir ki Kişisel Verilerin Korunması Kanunu kapsamında 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 veri olarak sayılmıştır.

görevli olan kişilerin bu görevlerini yerine getirmemeleri durumu suç olarak düzenlenmektedir¹⁸.

Kişisel verilerin yok edilmesi, gerekli süre kadar tutulması gerek Avrupa Birliği veri koruma hukuku enstrümanları gerekse 6698 sayılı Kanun kapsamında da bir ilke olarak düzenlenmektedir. Bu önemli ilkenin suç olarak Türk Ceza Kanunu kapsamında da düzenlenmiş olması yerinde ve yararlıdır. Zira söz konusu suç tipiyle hem kişisel verilerin bizzat kendisi hem de kişisel veriler açısından istenilen güvenlik ve kamu idaresinin güvenilirliği ile işleyişi hukuki koruma altına alınmaktadır¹⁹.

Türk Ceza Kanunu ile tesis edilmiş olan korumanın önemi yadsınamaz. Nitekim Türk Ceza Kanunu hükümleri çerçevesinde 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun kabulünden önce kişisel verilerin hukuka aykırı olarak işlenmesi eylemlerinden kaydetme, verme, yayma, ele geçirme ve yok etmeme faaliyetleri kapsamında bireyler koruma talep edebilmiştir. Her ne kadar kişisel verilerin korunması alanında Yargıtay ceza daireleri bakımından bir içtihat birliğinden söz edilemeyecek olsa da Yargıtay'ın faklı dairelerinin oldukça yerinde ve hassas değerlendirmelerinin olduğu, bireyi koruyan kararlara hükmettiği görülmektedir²⁰.

¹⁸ Kişisel verilerin ceza hukuku kapsamında korunmasına ilişkin detaylı bilgi için bkz. İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, 1. Baskı, Ankara, Seçkin Yayıncılık, Nisan 2017.

¹⁹ Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 6. Baskı, Ankara, Seçkin Yayıncılık, 2015, s. 719, 720; Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 5. Baskı, Ankara, Seçkin Yayıncılık, 2014, s. 468.

²⁰ "...tefepon numarası vermek şeklinde gerçeken eylemin kişisel verilerin ele geçirilmesi ve yayılması olarak değeriendirilemeyeceği" biçimindeki isabetsiz gerekçeyle beraatlerine karar verilmesi, bozmayı gerektirmiştir." hükmüne ilişkin olarak bkz. Yargıtay 12. Ceza Dairesi, Esas Sayısı: 2014/607, Karar Sayısı: 2014/16665, Karar Tarihi: 7 Temmuz 2014; "Mağdurun aktif kullanımında olan, herkes tarafından bilinmeyen veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, ancak sınırlı bir çevre ile paylaştığı cep telefonunun numarasını hukuka aykırı olarak yayan sanığın eyleminin TCK'nın 136/1. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğunun kabulünde bir isabetsizlik görülmendiğinden, temyiz itirazlarının reddine..." hükmüne ilişkin olarak bkz. Yargıtay 12. Ceza Dairesi, Esas Sayısı: 2014/6748, Karar sayısı: 2014/22909, Karar Tarihi: 17 Kasım 2014; "...Somut olayda; sanığın, eski okul arkadaşı olan mağdurun, ad ve soyadı ve fotoğrafı ile internette facebook sosyal paylaşım sitesinde mağdur adına herkese açık sahte üye profili oluşturarak, profil sayfasında mağdurun telefon numarasını yayımlaması biçimindeki eyleminin, TCK'nın 136/1. maddesine uyan, verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu gözetilmeden, suçun nitelendirilmesinde yanlışlığa düşölerek, olayda uygulama yeri bulunmayan aynı Kanunun 135/1. maddesi uyarınca hüküm kurulması bozmayı gerektirmiştir"

3.1.4. Türkiye’de Kişisel Verilerin Korunmasına Duyulan İhtiyaç

Günümüzde hızla gelişen teknolojiler ile beraber kişisel verilerin toplanması ve işlenmesi artık neredeyse bireyler farkında olmadan sürekli olarak gerçekleşmektedir. Bilgi çağının bir gereği olarak globalleşen dünyada bütün dünyayı sarmış durumda olan bir veri akışından ve akışından bahsetmek mümkündür. Hızla gelişen ve büyüyen veri akış trafikleri kıtaları, devletleri ve insanları birbirine bağlarken kişisel verilerin korunması alanında da çekinceler meydana getirmektedir. Bu doğrultuda insan haklarına saygılı yönetimlerde kişisel verilerin korunmasına ilişkin düzenlemeler getirilmesi zorunluluk halini almaktadır. Günümüzde bir yandan kişisel veriler gittikçe daha yüksek bir öneme sahip olmakta ve adeta ekonomik bir değer arz etmeye başlarken, diğer bir yandan kişilerin özel yaşamlarına ve gizliliklerine yönelik saldırılar da hızla artmaktadır.

Türkiye, yeni teknolojileri yakından takip eden, içerisinde çok çeşitli veri ekosistemlerini barındıran, global veri akışları içerisinde yer alan bir ülkedir. Türkiye’de internet kullanım alanı ve yaygınlığı hızla artmakta ve internet ortamdaki Türkçe içerikler her geçen gün biraz daha çeşitlenmektedir²¹. Günümüzde pek çok kişi okumak, araştırmak, sosyal iletişim ağlarına bağlanmak, iletişim kurmak, ekonomik etkinliklerde bulunmak ya da yalnızca eğlenmek için interneti kullanmaktadır²².

hükmüne ilişkin olarak bkz. Yargıtay 12. Ceza Dairesi, Esas Sayısı: 2013/26654, Karar Sayısı: 2014/15414, Karar Tarihi: 23 Haziran 2014, Türk Ceza Kanunu’nda yer alan kişisel verilerin korunmasına ilişkin hükümlerin uygulanması ve Yargıtay kararları için bkz. Murat Volkan Dülger, “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”, *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 3, Sayı 2, Güz 2016, s. 101-167.

²¹ Türkiye İstatistik Kurumu’nun 2016 yılı hane halkı bilişim teknolojileri kullanım araştırması sonuçlarına göre bilgisayar ve internet kullanım oranları 16-74 yaş grubundaki bireylerde 2015 yılında sırasıyla %54,8 ve %55,9 ilen bu oran 2016 yılında sırasıyla %54,9 ve %61,2 olmuştur. Hanelerin 2016 yılı Nisan ayında %96,9’unda cep telefonu veya akıllı telefon bulunurken, sabit telefon bulunma oranı %25,6’dır. Aynı dönemde hanelerin %22,9’unda masaüstü bilgisayar, %36,4’ünde taşınabilir mevcut iken tablet bilgisayar bulunma oranı %29,6’dır. 2015 yılında %20,9 olan İnternete bağlanabilen TV oranı ise 2016 yılında %24,6 olarak hesaplanmıştır, Türkiye İstatistik Kurumu, (Çevrimiçi) http://www.tuik.gov.tr/PreTablo.do?alt_id=1028, 3 Haziran 2018.

²²Türkiye İstatistik Kurumu’nun 2016 yılı hane halkı bilişim teknolojileri kullanım araştırması sonuçlarına göre İnternet kullanım amaçları dikkate alındığında, 2016 yılının ilk üç ayında internet kullanan bireylerin %82,4’ü sosyal medya üzerinde profil oluşturma, mesaj gönderme veya fotoğraf vb. içerik paylaşırken, bunu %74,5 ile paylaşım sitelerinden video izleme, %69,5 ile online haber, gazete ya da dergi okuma, %65,9 ile sağlıkla ilgili bilgi arama, %65,5 ile mal ve hizmetler hakkında bilgi

Çevrimiçi olarak kullanabilen ve günlük hayata dâhil olan cihaz sayısı da gün geçtikçe hızla artmaktadır. Günümüzde cihazlar sıcaklık, basınç, titreşim, ses, ışık, koku gibi birçok sensör ile donatılmakta ve birbirine bağlanmaktadır. Akıllı şehirler, akıllı arabalar, evler, mutfak eşyaları, telefonlar, giyilebilir teknolojiler ve bilgisayarlar ile toplanan kişisel veri miktarı hızla katlanmaktadır²³.

Teknolojik gelişmelerin yakından takip edildiği ülkemizde söz konusu cihazların kullanımı şimdiden yaygınlaşmaya başlamıştır. Bu doğal akış aynı zamanda dünya ekonomik trendlerini de yakalamak için büyük önem arz etmektedir. Türkiye Sanayici ve İş adamları Derneği, Sanayi 4.0 Raporu'nda²⁴, bu gerekliliğe ilişkin olarak Türkiye ekonomisine yönelik, *"Rekabet gücü yüksek ekonomiler kümesi içinde yer almak isteyen Türkiye için, küresel düzeydeki bu gelişmeleri takip etmek ve bunun ötesinde Sanayi 4.0'ın uygulayıcı öncü ekonomileri arasında yer almak kaçınılmaz bir önemdedir"*²⁵ ifadesi kullanılmaktadır. Bilişim teknolojileri ve birbiriyle ve internetle bağlı pek çok cihaz özel ve kamu kuruluşlarınca kullanılmaktadır. Bu bağlamda tüketiciler kimi zaman fark ederek kimi zaman ise farkında olmayarak bu sisteme veri sağlamaktadır.

Türkiye teknolojik gelişmeleri bu kadar yakından takip ederken ne yazık ki kişisel verilerin korunmasına ilişkin hukuki korumaları içeren temel bir düzenlemeyi hayata geçirmek için fazla aceleci davranmamıştır. Kişisel verilerin korunması konusunda

arama ve %63,7 ile İnternet üzerinden müzik dinleme (web radyo) takip etmiştir, Türkiye İstatistik Kurumu, (Çevrimiçi) http://www.tuik.gov.tr/PreTablo.do?alt_id=1028, 3 Haziran 2018.

²³ 2015 yılında 15.4 milyar cihazdan oluşan nesnelerin interneti (**internet of things**) pazarının 2020 yılında 30,7 milyar cihaza ve 2025'te 75.4 milyara ulaşacağını tahmin edilmektedir. (Çevrimiçi) <http://news.ihsmarkit.com/press-release/technology/tech-companies-creating-strategic-platforms-support-internet-things-ihs-say>, 18 Nisan 2018; McKinsey tarafından hazırlanmış raporda ise 2015 yılında toplam pazar büyüklüğünün 900 milyon dolara ulaşan nesnelerin interneti teknolojilerinin 2020'de %32,6 büyüyerek 3.7 milyar dolara ulaşacağı öngörülmüştür. McKinsey&Company, "Internet of Things: The IoT opportunity – Are you ready to capture a once-in-a lifetime value pool?", Hong Kong IoT Conference, 21 Haziran 2016, (Çevrimiçi) [http://hk-iot-conference.gs1hk.org/2016/pdf/04_Mc%20Kinsey%20-%20\(Chris%20Ip%20\)%20ppt%20part%20%201%20_IoT%20-%20Capturing%20the%20Opportunity%20vF%20-%202021%20June%202016.1p_ptx.pdf](http://hk-iot-conference.gs1hk.org/2016/pdf/04_Mc%20Kinsey%20-%20(Chris%20Ip%20)%20ppt%20part%20%201%20_IoT%20-%20Capturing%20the%20Opportunity%20vF%20-%202021%20June%202016.1p_ptx.pdf) 18 Nisan 2018.

²⁴ Burak Tansan v.d., "Türkiye'nin Küresel Rekabetçiliği İçin Bir Gereklik Olarak Sanayi 4.0: Gelişmekte Olan Ekonomi Perspektifi", ed. Nurşen Numanoglu v.d., Yayın no: TÜSİAD-T/2016-03/576, TÜSİAD, Mart 2016. Bu çalışma kapsamında Sanayi 4.0 Raporu olarak anılacaktır.

²⁵ Sanayi 4.0 Raporu, s. 13.

uzunca bir süre yasal düzenleme yapılması ile bu konuda düzenleyici ve denetleyici bir kurum ya da kurul kurulması, Avrupa Birliği müzakereleri süresince fasıllarından dördüncüsünde²⁶ bir sorun olarak değerlendirilmektedir. Yukarıda bahsedildiği üzere dünyada geniş etkilere sahip olan Kıta Avrupası veri koruma ekolü, OECD ilkeleri ile öne çıkarılan verinin serbest dolaşımını prensibine zıt olarak kişisel verilerin güvenliğine ilişkin yeterli güvenliğin sağlanmadığı ülkelere veri akışını yasaklamaktadır. Avrupa Birliği'nin, uygulamada yaşadığı pek çok probleme karşın, kişisel verilerin korunması alanında, kendi ekolünü uluslararası alanda etkili bir model olarak kabul ettirdiği söylenebilmektedir²⁷.

İlerleme Raporları'nın yanı sıra Katılım Ortaklığı Belgesi²⁸, 23. Fasıll Tarama Sonu Raporu gibi belgelerde, bu konuda bir kanunun yürürlüğe girmemiş olması, Kişisel Verilerin Korunması Kanunu'nun kabulünden önceki dönemde önemli bir eksiklik olarak nitelendirilmiştir. Söz konusu raporlarda da değinildiği üzere kişisel verilerin korunması alanındaki yasal düzenleme eksikliği ve kişisel verilerin korunmaması, Avrupa Polis Teşkilatı Europol ile operasyonel iş birliği anlaşmasının yapılması önünde engel teşkil etmiş, pek çok alanda birlik üyesi devletler ile bilgi ve belge

²⁶ Komisyon Çalışma Dokümanı 2016 Türkiye Çalışma Raporu, Brüksel, 9 Kasım 2016; "...Verilerin korunmasına ilişkin mevzuat bulunmaması AB kurumlarıyla ve üye devletlerle daha geniş kapsamlı işbirliği yapılmasının önünde bir engeldir." Rapor özeti, s.4; "Ancak, ifade özgürlüğünün, gizliliğin, kişisel verilerin yeterli seviyede korunmaması ciddi bir endişe kaynağı olmaya devam etmektedir." Fasıll 10: Bilgi Toplumu ve Medya, s. 44; "...kişisel verilerin korunması ve azınlıklara mensup kişilerin korunması başta olmak üzere, temel hak ve özgürlüklerin tam olarak gözetilmesini sağlaması gerekmektedir", "İlgili Avrupa Konseyi Sözleşmesi ve Protokolü henüz onaylanmamıştır. AB müktesebatıyla uyumlu bir Kişisel Verilerin Korunması Kanunu'nun kabul edilmesi, vize serbestisi diyalogu kapsamındaki bir gereklilik olduğu kadar, Eurojust ve Europol ile operasyonel işbirliği anlaşmalarının akdedilmesi ve terörizmle mücadele dâhil olmak üzere AB üye devletleri adli ve polis işbirliğinin güçlendirilmesi için de bir gerekliliktir." Fasıll 23: Yargı ve Temel Haklar, s. 59, 67; "AB üye devletleri ile adli ve polis işbirliğinin kolaylaştırılması amacıyla Avrupa standartları ile uyumlu kişisel verilerin korunmasına ilişkin kanunu kabul etmesi ve uygulaması gerekmektedir.", "Özellikle, Avrupa standartları ile uyumlu kapsamlı bir kişisel verilerin korunması kanununun kabul edilmesi ile Türkiye'nin siber suçlar ve tanık koruma alanlarında mevzuatını iyileştirmesi gerekecektir." Fasıll 24: Adalet, Özgürlük ve Güvenlik, s. 74,78; "Ulusal sağlık bilgi sistemine çok az sayıda kalite göstergesi dâhil edilmiştir, ancak buradaki kişisel verilerin gizliliği ve güvenliği çözüm bulunması gereken hassas bir konu olmaya devam etmektedir." Fasıll 28: Tüketicinin ve Sağlığın Korunması, Türkiye Düzenli İlerleme Raporu, 2015, s. 83, (Çevrimiçi) <http://www.ab.gov.tr/index.php?p=46224> , 4 Nisan 2018.

²⁷ Küzeci, **a.g.e.**, s. 187.

²⁸ Katılım Ortaklığı Belgesi, adaylığı resmen kabul edilen her ülke için Avrupa Komisyonu tarafından hazırlanan ve Konsey tarafından onaylandıktan sonra, AB Resmi Gazetesi'nde yayımlanan bir belgedir.

değişimi, paylaşımına ilişkin iş birliğinin sağlanamamasına neden olmuştur. Bununla birlikte geçtiğimiz dönem içerisinde kişisel verilerin korunmasına ilişkin yasal bir düzenlemenin olmamasının ekonomik etkileri de bulunmaktadır²⁹.

Bütün bu gereklilikler ışığında ve uzunca bir tasarı sürecinin ardından 6698 sayılı Kişisel Verilerin Korunması Kanunu uzun bir hazırlık ve yasama süreci neticesinde 7 Nisan 2016'da Resmî Gazete'de yayımlanmıştır. Ancak belirtmek gerekir ki söz konusu kanun, Avrupa Birliği Veri Koruma Yönergesi'ni temel almış olup, yeni teknolojik gelişmeler ışığında bir reform ihtiyacı sonucu ortaya konmuş olan Avrupa Birliği Genel Veri Koruma Tüzüğü'nde belirlenen ilke ve yaklaşımlar temel alınmamıştır. Kanun koyucu, her ne kadar gerekçesinde Avrupa Birliği Genel Veri Koruma Tüzüğü'ne atıfta bulunmuş³⁰ ise de, Kanun'un 2018 yılının Mayıs ayı içerisinde yürürlükten kaldırılan Yönerge'yi temel alarak hazırlanması öğretide haklı eleştirilere konu olmuştur³¹.

3.2. 6698 sayılı Kişisel Verilerin Korunması Kanunu

3.2.1. Amaç ve Kapsam

Uzun yıllar boyunca kişisel verilerin korunmasına ilişkin olarak müstakil bir düzenlemenin olmaması, gerek uluslararası alanda şirketlerin kişisel veri aktarım faaliyetleri bakımından gerekse bireylere temel hak ve özgürlüklerinin tanınması bakımından pek çok aksaklık meydana getirmiştir. Uluslararası sözleşmeler ve belgeler, mukayeseli hukuk uygulamaları ve Türk toplumunun ihtiyaçları göz önünde bulundurularak hazırlanan Kişisel Verilerin Korunması Kanunu ile kişisel verilerin çağdaş standartlarda işlenmesi ve koruma altına alınması amaçlanmaktadır. Bu kapsamda Kişisel Verilerin Korunması Kanunu, kişisel verilerin işlenme şartlarını, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel

²⁹ Kişisel Verileri Koruma Kurumu, “Ulusal Ve Uluslararası Alanda Kişisel Verilerin Korunmasına Duyulan İhtiyaç”, Ankara, s.6, (Çevrimiçi) <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8e39e0a1-6ec4-4179-a5d3-bbd8e78dce31.pdf>, 13 Nisan 2018.

³⁰ “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 66.

³¹ “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 87, 91; Çekin, a.g.e., s. 3.

hak ve özgürlüklerinin korunmasını ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektedir³². Kanun'un gerekçesinde, kişinin mahremiyet hakkı ile bilgi güvenliği hakkının korunması da bu amaç kapsamında değerlendirilmektedir. Ayrıca, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlenmesi de Kişisel Verilerin Korunması Kanunu'nun amaçları arasında yer almaktadır.

Kişisel Verilerin Korunması Kanunu'nun kapsam maddesinde³³, hükümlerinin, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağı belirtilmektedir. Bu doğrultuda Kişisel Verilerin Korunması Kanunu'nun uygulama alanı bakımından kamu-özel sektör ayrımının bulunmadığı söylenebilecektir. Nitekim Kişisel Verilerin Korunması Kanunu kapsamından çıkarılan ikincil düzenlemelerde kamu sektörüne özgülenmiş hükümler yer almaktadır. Kişisel Verilerin Korunması Kanunu gerek özel kurum ve kuruluşlar gerekse kamu kurum ve kuruluşları, devlet daireleri de dâhil olmak üzere tamamen ya da kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydı ile otomatik olmayan yollarla kişisel veri işleyen herkes bakımından bağlayıcı olmak üzere hazırlanmıştır.

3.2.2. Genel Kavramlar

Kişisel Verilerin Korunması Kanunu, **i.** amaç, kapsam ve tanımlar, **ii.** kişisel verilerin işlenmesi, **iii.** haklar ve yükümlülükler, **iv.** başvuru, şikâyet ve veri sorumluları sicili, **v.** suçlar ve kabahatler, **vi.** Kişisel Verileri Koruma Kurumu ve teşkilatı, **vii.** çeşitli hükümler ve alt başlıkları halinde düzenlenmiş olup 33 maddeden oluşmaktadır. Tanımlar başlığı³⁴ altında Kanun'da yer alan temel kavramlar açıklanmıştır.

³² Kişisel Verilerin Korunması Kanunu, m. 1.

³³ Kişisel Verilerin Korunması Kanunu, m. 2.

³⁴ Tanımlar başlığı altında, açık rıza, anonim hale getirme, başkan, ilgili kişi, kişisel veri, kişisel verilerin işlenmesi, kurul, kurum, veri işleyen, veri kayıt sistemi e veri sorumluları kavramlarına ilişkin tanımlamalar yer almaktadır. Kişisel Verilerin Korunması Kanunu, m. 3.

3.2.2.1. Kişisel Veri

Kişisel Verilerin Korunması Kanunu’nun 2. maddesinde, kişisel veri, pek çok hukuki metin ile paralel ve örtüşür şekilde “*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlanmıştır. Kişisel veri kavramına dâhil olan veri grubunu sınırlandırmamak için seçilen bu tanım gerçekten de Kanun’un uygulama alanını genişletmektedir. Kişisel veri kavramından söz edebilmek için verinin bir kişiye ilişkin olması ve bu kişinin de belirli ya da belirlenebilir nitelikte olması gerekmektedir.

Kişisel Verilerin Korunması Kanunu’nda yer alan tanım doğrultusunda, gerçek bir kişiyi belirli veya belirlenebilir kılan her türlü verinin herhangi bir sınırlamaya tabi tutulmaksızın kişisel veri olarak kabul edilmesi gerekmektedir. Kişisel veri kavramının sayılarak sınırlandırılması, gelişen teknolojiler ile yakın gelecekte üretilebilecek yeni veri kategorilerini kapsamama tehlikesi yaratabileceği için geniş bir tanımlama ile kapsayıcı bir kişisel veri kavramı oluşturmak yerindedir. Kanun’daki tanım uyarınca kişisel veri sadece gerçek bir kişiye ilişkin olabilmekte bu doğrultuda yerinde bir şekilde tüzel kişilere ilişkin veriler kişisel veri kapsamına dâhil edilmemektedir. Ancak belirtmek gerekir ki tüzel kişi şirket yetkilisinin bilgilerini içeren imza sirküleri gerçek kişi verisi içerdiği için kişisel veri içeren belge olarak konumlandırılmalı ve bu durum göz ardı edilmemelidir.

Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi ile o kişinin tanımlanabilir hale getirilmesini ifade etmektedir. Kişisel Verilerin Korunması Kanunu’nun gerekçesinde³⁵ bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi bireylerin kesin tespitini sağlayan verilerin yanı sıra, kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin verilerin de kişisel veri niteliğinde olduğu belirtilmiştir. Kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan veriler gibi kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğine ilişkin veriler bağlamına göre kişiyi belirlenebilir kılan somut bir içerik taşıyabileceği için kişinin belirlenmesini sağlayan tüm veriler kişisel veri olarak nitelendirilmektedir.

³⁵ “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 7.

Nitekim Kişisel Verilerin Korunması Kanunu'nun gerekçesinde de telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, aile bilgileri gibi verilerin dolaylı da olsa kişiyi belirlenebilir kılabilmek özellikleri nedeniyle kişisel veri olarak kabul edilmesi gerektiğine işaret edilmiştir³⁶.

3.2.2.2. Kişisel Verinin İşlenmesi

Kişisel Verilerin Korunması Kanunu madde 2'de tanımlanan kişisel verilerin işlenmesi kavramı uyarınca, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla ilk defa elde edilmesiyle başlayan bir süreç ve devamındaki her türlü işleme, veri işleme olarak ifade edilmektedir. Kişisel veriler, belirtilen şartlara uygun şekilde elde edilmesinden itibaren silme, yok etme ya da anonim hale getirme işlemlerine kadar olan süreçte gerçekleştirilen her türlü faaliyet uluslararası örneklerde de olduğu gibi Kişisel Verilerin Korunması Kanunu kapsamında kişisel verilerin işlenmesi olarak değerlendirilmektedir. Bu bakımdan Kişisel Verilerin Korunması Kanunu'nda sayılmış olan kişisel veri işleme halleri, örnekleme amacı gütmekte olup herhangi bir sınırlama amacı teşkil etmemektedir. Kişisel verilerin işlenmesi kavramı incelenecek olduğunda, tanım itibarı ile yöntem bakımından bir sınırlandırmanın söz konusu olduğu görülebilecektir. Bu doğrultuda Kişisel Verilerin Korunması Kanunu kapsamında bir kişisel veri işleme faaliyetinden bahsedebilmek için söz konusu faaliyetin **i.** tamamen veya kısmen otomatik olan ya da **ii.** herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi gerekmektedir. Bu tanım uyarınca bir veri işleme faaliyetinin öncelikle otomatik olup olmadığı belirtilmeli, sonrasında ise otomatik olmayan işleme varsa, bu defa da verinin bir veri kayıt sistemi içerisinde işlenip işlenmediğinin tespit edilmesi gerekmektedir.

Otomatik işleme ile terimsel olarak ne kastedildiği gerek Avrupa Birliği Veri Koruma Yönergesi gerekse Kişisel Verilerin Korunması Kanunu kapsamında tanımlanmamıştır. Ancak OECD tarafından “*İnsan müdahalesi ya da yardımı konusundaki ihtiyacı asgari seviyeye indiren, kendi aralarında bağlantılı ve etkileşimli elektrikli veya elektronik bir sistem tarafından gerçekleştirilen veri işleme faaliyeti*”

³⁶ “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 7.

olarak tanımlanmıştır³⁷. Bununla birlikte Kişisel Verilerin Korunması Kanunu gerekçesinde, Kanun'un kapsamı açıklanırken, “Günümüzde bu veriler gerek özel sektör gerekse kamu sektörü tarafından bilişim sistemleri üzerinden otomatik yollarla sıkça kullanılmaktadır” ifadesine yer verilmiştir³⁸. Bu ifade ile kanun koyucu dolaylı yoldan otomatik işlemenin, bilişim sistemleri üzerinde gerçekleştirilen faaliyetler olduğunu belirtmektedir. Bu doğrultuda belirtmek gerekir ki otomatik bir veri işleme faaliyetinden bahsedebilmek için insan etkisinin en aza indirildiği elektronik cihazlar vasıtası ile bir işleme faaliyetinin gerçekleşiyor olması şartı aranmalıdır. Bu kapsamda kanun koyucunun teknolojik gelişmelerin hızını dikkate alarak sınırlayıcı bir otomatik işleme tanımı getirmemiş olması yerinde bir tespittir. Zira gelişen teknolojiler ile birlikte otomatik yollarla veri işleyebilen cihaz sayısı günden güne artabilmektedir. Bu nedenler herhangi bir yazılım ya da donanım tanımlamasına bağlı kalmaksızın yazılım veya donanım özellikleri aracılığıyla önceden hazırlanan algoritmalar kapsamında insan müdahalesi olmadan kendiliğinden gerçekleşen işleme faaliyetleri olarak otomatik veri işleme kavramını tanımlamak yerinde olacaktır³⁹.

Otomatik olmayan veri işleme faaliyetlerinin Kişisel Verilerin Korunması Kanunu kapsamında değerlendirilebilmesi için veri işleme faaliyetinin herhangi bir veri kayıt sisteminin parçası olması gerekmektedir. Kişisel Verilerin Korunması Kanunu kapsamında veri kayıt sistemi, “*kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi*” olarak tanımlanmaktadır. Bu sistemlerin elektronik ya da fiziki ortamda oluşturulabileceği Kişisel Verileri Koruma Kurumu tarafından çıkartılan bilgilendirici yayınlarda belirtilmektedir⁴⁰. Kişisel Verilerin Korunması Kanunu gerekçesinde örnek olarak, veri kayıt sisteminde kişisel veriler; ad, soyad veya kimlik numarası üzerinden sınıflandırılması yahut kredi borcunu ödemeyenlere ilişkin oluşturulacak sınıflandırmanın bu kapsamda değerlendirilebileceği belirtilmektedir⁴¹. Kanun gerekçesine açık bir şekilde, otomatik olmayan yollarla işlenen kişisel verilerin

³⁷ OECD, *Oecd Glossary of Statistical Terms*, Paris, OECD Publishing, 2007, s. 48.

³⁸ “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 4.

³⁹ Kişisel Verileri Koruma Kurumu, “6698 Sayılı Kanun’da Yer Alan Temel Kavramlar”, 2017, s. 18, (Çevrimiçi) <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/45af208d-3718-49ed-b51a-9be9edde6ff2.pdf>, 14 Nisan 2018.

⁴⁰ a.y.

⁴¹ “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 7.

bir veri kayıt sisteminin parçası olarak işlenmemesi halinde Kanun kapsamında değerlendirilmeyeceği ifade edilmektedir.

3.2.2.3. Veri Sorumlusu

Kişisel Verilerin Korunması Kanunu'nda yer alan tanım uyarınca veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade etmektedir. Bu tanım, Avrupa Birliği Veri Koruma Yönergesi ve diğer uluslararası düzenlemeler ile uyumluluk arz etmektedir⁴². Kişisel Verilerin Korunması Kanunu'nun önceki tasarı metinlerinde “veri sorumlusu” yerine “veri kütüğü sahibi” ifadesi kullanılarak, kişisel verilerin işlenmesinin amaç ve metotlarını tek başına veya başkaları ile birlikte belirleyen gerçek ve tüzel kişiler olarak tanımlanmaktadır. Örnek alınan düzenlemeler bakımından veri sorumlusu teriminin seçilmesinin yerinde bir düzenleme olduğunu ifade etmek gerekir. Veri sorumlusu terimi, unsurları bakımından tanımı ışığında şu şekilde incelenmelidir; **(i)** işleme amaçlarını ve vasıtalarını belirleyen, **(ii)** Veri kayıt sisteminin kurulmasından ve yönetilmesinde sorumlu olan, **(iii)** gerçek ya da tüzel kişi. Bu doğrultuda veri sorumlusu kişisel verilerin nasıl ve neden işlendiği sorularına cevap verebilecek olan gerçek ya da tüzel kişi olarak kabul edilmesi gerekmektedir. Kişisel Verileri Koruma Kurumu tarafından yayımlanan bilgilendirici yayında⁴³ veri sorumlusunun tespiti için sayılan hususlara kimin karar verdiğinin dikkate alınması gerektiği belirtilmektedir: **(i)** kişisel verilerin toplanması ve toplama amacı, **(ii)** toplanacak kişisel veri türleri, **(iii)** toplanan verilerin hangi amaçlarla kullanılacağı, **(iv)** hangi bireylerin kişisel verilerinin toplanacağı, **(v)** toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı, **(vi)** verilerin ne kadar süreyle saklanacağı, **(vii)** İlgili kişilerin erişim hakkı ve diğer haklarını uygulanıp uygulanmayacağı. Veri sorumlusunun belirtilen sorulara cevap vermesi ve verebilecek durumda olması, yürütülecek veri işleme faaliyetleri bakımından bir karar verme iradesi oluşturuyor olması önem arz etmektedir. Veri kayıt sisteminin oluşturulması ve yönetimi bakımından ise karar verici konumda olması

⁴² Küzeci, **a.g.e.**, s. 18.

⁴³ Kişisel Verileri Koruma Kurumu, “6698 Sayılı Kanun'da Yer Alan Temel Kavramlar”, 2017, s. 24.

gerekmektedir. Veri sorumlusunun tek bir kişi olacağı yönünde tartışmalar isabetsiz olmakla beraber Kişisel Verilerin Korunması Kanununda açık bir şekilde tüzel kişilerin de veri sorumlusu olabileceği belirtilerek, tüzel kişiler, kişisel verileri işleme konusunda gerçekleştirdiği faaliyetler kapsamında bizzat kendileri “veri sorumlusu” olup, ilgili düzenlemelerde belirtilen hukuki sorumluluğun tüzel kişi üzerinde herhangi bir organ ya da şahıs seçilmeksizin doğacağına kabulü gerekmektedir. Tanımlar maddesi uyarınca Kişisel Verilerin Korunması Kanunu kamu-özel ayrımı gözetmemiş, bu nedenle söz konusu kişisel verilerin korunması mevzuatı hem kamu hukuku tüzel kişileri hem de özel hukuk tüzel kişileri açısından uygulama alanı bulabilecektir. Nitekim devam maddelerde ve ikincil düzenlemelerde kamu hukuku tüzel kişilerine doğrudan getirilen yükümlülükler bulunmaktadır.

3.2.2.4. Veri İşleyen

Kişisel Verilerin Korunması Kanunu’nda yer alan tanım itibarı ile veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade etmektedir. Tanım doğrultusunda dikkat etmek gerekir ki, veri işleyen kişilerin veri sorumlusunun talimat ve emirleri ile sınırlı olarak bir veri işleme faaliyeti gerçekleştiriyor olması gerekmektedir. Gerekçede her ne kadar veri işleyenin kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen çalışanlar olabileceği gibi, veri sorumlusunun hizmet satın almak suretiyle belirlediği ayrı bir gerçek veya tüzel kişi de olabileceği belirtilmiş olsa da veri işleyen terimi ile vurgulanmak istenen veri sorumlusunun çalışanları değil, dışardan hizmet aldığı üçüncü kişilerdir. Kişisel Verileri Koruma Kurumu tarafından çıkartılmış olan bilgilendirici yayınlarda bu konuya ilişkin olarak “Veri işleyen, tüzel kişilik içerisindeki bir birim midir yoksa başka bir tüzel kişilik veya organizasyon dışındaki kişi midir?” sorusu açık bir şekilde “*veri işleyen organizasyon dışındaki bir kişidir*” ifadesi ile cevaplanmaktadır⁴⁴. Nitekim 28 Ekim 2017 tarihli 30224 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi

⁴⁴ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, Ankara, KVKK Yayınları, Mart 2018, s. 56, (Çevrimiçi) <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf>, 14 Nisan 2018.

Hakkında Yönetmelik'te ilgili kullanıcı terimi getirilerek, verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri kapsayacak şekilde tanımlanmaktadır. Bu doğrultuda veri işleyen konumunda olan gerçek ya da tüzel kişinin veri sorumlusu altında çalışan bir kişi olamayacağı aşıkardır⁴⁵.

Kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen veri sorumlusunun; örneğin, hizmet satın almak suretiyle belirlediği ve veri sorumlusu organizasyonu altında yer almayan, ayrı bir gerçek veya tüzel kişi olan veri işleyene örnek olarak dışarıdan hizmet alınması suretiyle çağrı merkezi hizmeti sunan çağrı merkezi şirketi, pazar araştırma şirketleri, kuryeler, avukatlar, muhasebeciler gerekçe ve kurum yayınlarda verilmektedir.

Belirtmek gerekir ki herhangi bir gerçek veya tüzel kişi farklı veri grupları ve ilgili kişiler nezdinde hem veri sorumlusu hem de veri işleyen olabilecektir. Örnek olarak bir muhasebe şirketi kendi personeliyle ilgili tuttuğu verilere ilişkin olarak bu kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olacağı için veri sorumlusu sayılırken; müşterisi olan şirketlere ilişkin tuttuğu veriler bakımından müşterilerinin emir ve talimatları ile bağlı olarak veri işleme faaliyeti gerçekleştireceği için veri işleyen olarak da kabul edilecektir⁴⁶.

3.2.3. Veri Sorumlularının Uyması Gereken Genel İlkeler

Kişisel Verilerin Korunması Kanunu ile veri sorumlusu konumunda bulunan şirketlerin kişisel verilerin işlenmesi ile ortaya çıkacak faydadan hukuki sınırlar çerçevesinde en yüksek seviyede yararlanabilmeleri amaçlanmıştır. Bu doğrultuda kişisel verilerin korunmasına ilişkin olarak, uluslararası metinler ve Avrupa Birliği Veri Koruma Yönergesi ile paralel olacak şekilde temel ilkeler belirlenmiştir. Kural olarak kişisel verilerin veri sorumlusu tarafından işlenmesinde meşru amaçların tespit edilebiliyor olması halinde söz konusu faaliyet hukuka uygun kabul edilmektedir.

⁴⁵ Bu konuda aksi görüş ve Tüzük'ün veriyi doğrudan işleyen kişiye ilişkin getirdiği tanım hakkında detaylı bilgi ve Kanun eleştirisi için bkz. Çekin, **a.g.e.**, s. 40-42.

⁴⁶ “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 7.

Ancak yine de hukuka uygunluk sebeplerinin varlığının yanı sıra kişisel veri işleme faaliyetlerinin belirlenen ilkeler çerçevesinde yürütülmesi gerekmektedir. Nitekim kişisel verilerin belirli usul ve esaslar ve ilkeler çerçevesinde korunması ve bu koşullar altında işlenebiliyor olması, ilk bakışta düşünülenin aksine kişisel verilerin serbest dolaşımını ve işlenmesini güven altına alarak, kolaylaştıran bir uygulama olarak düşünülmelidir. Bir başka deyişle, kişisel veri koruma düzenlemelerinde yer alan temel ilke ve sınırlandırılmalar ile veri korumasının bir diğer amacı olan verinin serbest dolaşımının sağlanması hedeflenmektedir. Kişilerin veri güvenliği ve mahremiyetin ihlâl edilmediğine ilişkin kanaati güçlendikçe, ulaşılabilirliği ve paylaşımı artan veri miktarı ve çeşitliliği artabilecektir. Aksi halde, bireyler kişisel verilerini üçüncü kişilerin erişimine kapatma ya da yanlış bilgi verme yönelimi göstererek ve günümüz ekonomisinin hammaddesi olan nitelikli ve kaliteli veriye ulaşmak güçleşebilecektir.

Kişisel Verilerin Korunması Kanunu’nda, Avrupa Birliği Veri Koruma Yönergesi ve 108 sayılı Sözleşme ile paralel olarak belirlenen bu ilkeler⁴⁷ ışığında, veri sorumlusuna bir takım yükümlülük ve sorumluluklar getirilmiştir. Aydınlatma yükümlülüğü⁴⁸, veri güvenliğine ilişkin yükümlülükler⁴⁹, ilgili kişiler tarafından yapılan başvuruların cevaplanması⁵⁰ ve Kişisel Verilerin Korunması Kurulu kararlarının yerine getirilmesi

⁴⁷ Kişisel Verilerin Korunması Kanunu, madde 4 kapsamında kişisel verilerin işlenmesi sırasında uyulacak ilkeler sayılarak belirtilmiştir: i. hukuka ve dürüstlük kurallarına uygun olmalı, ii. doğru ve gerektiğinde güncel olmalı, iii. belirli, açık ve meşru amaçlar için işlenmeli, iv. işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmalı ve v. ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

⁴⁸ Kişisel Verilerin Korunması Kanunu, madde 10 uyarınca veri sorumlusu, kişisel verilerin elde edilmesi sırasında bizzat veya yetkilendirdiği kişi aracılığıyla aşağıdaki bilgileri ilgili kişiye sağlamakla yükümlüdür; **i.** veri sorumlusunun ve varsa temsilcisinin kimliği; **ii.** kişisel verilerin hangi amaçla işleneceği, **iii.** kişisel verilerin kimlere ve hangi amaçla aktarılabileceği; **iv.** kişisel veri toplamanın yöntemi ve hukuki sebebi; **v.** Kişisel Verilerin Korunması Kanunu madde 11’de sayılan ilgili kişinin hakları.

⁴⁹ Kişisel Verilerin Korunması Kanunu, madde 12 uyarınca veri sorumlusu veri güvenliğine ilişkin olarak sayılan hususları temin ile yükümlüdür; **i.** kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, **ii.** kişisel verilere hukuka aykırı olarak erişilmesini önlemek, **iii.** kişisel verilerin muhafazasını sağlamak.

⁵⁰ Kişisel Verilerin Korunması Kanunu, madde 13 ve bu maddeye istinaden 10 Mart 2018 tarihli Resmi Gazetede yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ uyarınca veri sorumluları, ilgili kişiler tarafından yazılı olarak veya bahse konu Tebliğ’de yer verilen şekilde yapılan

yükümlülüğü⁵¹, veri sorumluları siciline kaydolma yükümlülüğü⁵², ilgili kişinin haklarını kullanmasına imkân sağlayan mekanizma oluşturma yükümlülüğü bu kapsamda temel ilkelerin bir görünümü olarak düzenlenmiştir.

3.2.4. Kişisel Verilerin İşlenmesini Meşru Kılan Hukuka Uygunluk Nedenleri

Kişisel Verilerin Korunması Kanunu kapsamında kaynak düzenlemede olduğu gibi kişisel verilerin işlenmesinde, amaç unsuru bakımından değerlendirilecek olan hukuka uygunluk sebepleri, kişisel verilerin işlenme şartları olarak adlandırılmaktadır. Kaynak düzenlemede olduğu gibi kişisel verilerin işlenme şartları, kişisel veri kategorileri ve verilerin aktarımına ilişkin bir ayrıma gidilerek farklı maddeler altında düzenlenmiştir.

Ayrımcılığa neden olabilecek bir takım kişisel veriler, Avrupa Birliği düzenlemelerinde olduğu gibi Kişisel Verilerin Korunması Kanunu kapsamında da özel olarak sayılarak, işlenme koşulları daraltılarak düzenlenmiştir. Hatta öyle ki Kişisel Verilerin Korunması Kanunu kapsamında kaynak düzenlemeden farklı olarak özel nitelikli kişisel veriler içerisinde de ikili bir ayrıma gidilerek, sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesi daha dar ve ağır koşullara bağlanmaktadır. Belirtmek gerekir ki Yönerge lafzından farklı olarak Kişisel Verilerin Korunması Kanunu’nda kişisel verilerin işlenmesi ilgili kişinin açık rızasının bulunması şartına bağlı kılınarak, diğer sayılan hukuka uygunluk halleri birer istisna olarak düzenlenmektedir⁵³. Bir başka deyişle Kişisel Verilerin Korunması Kanunu’nda rıza temeline dayalı veri işleme ile diğer gerekçelerle veri işleme arasında bir ayrım

başvuruları niteliklerine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırmakla yükümlü kılınmıştır.

⁵¹ Kişisel verilerin Korunması Kanunu, madde 15/5 uyarınca şikâyet üzerine veya resen inceleme yapan Kişisel Verilerin Korunması Kurulu tarafından ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar doğrultusunda veri sorumlusu kararın kendine tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde kararın gereğini yerine getirmekle yükümlü kılınmıştır.

⁵² Aleniyet ilkesinin bir görünümü olarak, Kişisel verilerin Korunması Kanunu madde 16 hükmü gereğince Kişisel Verilerin Korunması Kurulu tarafından getirilecek olan istisnalar gözetilerek veri sorumlularına Kişisel Verileri Koruma Kurumu Başkanlığı tarafından kamuya açık olarak tutulacak olan Veri Sorumluları Sicili’ne kayıt yükümlülüğü getirilmiştir.

⁵³ Yücedağ, **a.g.m.**, s. 773.

yapılmaktadır. Rızayı ayrı bir gerekçe ya da sebep olarak değil, diğerlerine eşit bir gerekçe olarak dâhil etmenin daha uygun olacağına ilişkin eleştiriler mevcuttur⁵⁴.

Kişisel Verilerin Korunması Kanunu 5. madde kapsamında sayılan ve ilgili kişinin açık rızası aranmaksızın genel nitelikli kişisel verilerinin işlenmesi için bulunması gereken ve hukuka uygunluk sebebi olarak kabul edilen haller şöyle sayılmıştır:

- i.** Kanunlarda açıkça öngörülmesi,
- ii.** 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,
- iii.** Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- iv.** Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- v.** İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- vi.** Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- vii.** İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Yukarıda sayılan hukuka uygunluk hallerinin kişisel veri işleme faaliyetinde güdülen amaca yönelik olması ve kişinin bu amaç doğrultusunda bilgilendirilmiş olması önem teşkil etmektedir. Kişisel Verilerin Korunması Kanunu'nun uygulanmasına ilişkin çıkarılan ikincil düzenlemelerde kişisel verilerin işlenmesinde “belirli, açık ve meşru amaçlarla işleme” ilkesinin bir görünümü olarak getirilen aydınlatma yükümlülüğü bu bilgilendirmenin içeriğini düzenlemektedir. Aydınlatma yükümlülüğünün yerine getirilmesinde kişisel verilerin işlenmesinde yer alan amaçların dâhil edildiği hukuka uygunluk sebeplerinin belirtilmesi gerekmektedir.

⁵⁴ Tekin, **a.g.e.**, s. 251.

3.2.4.1. Açık Rıza

Kişisel Verilerin Korunması Kanunu kapsamında Avrupa Birliği Veri Koruması Yönerge'sinde öngörülenden daha nitelikli bir rıza düzenlemesi bulunmaktadır. Avrupa Birliği Veri Koruma Yönergesi'nde özel nitelikli olmayan kişisel verilerin işlenmesi için ilgili kişinin rızası yeterli iken Kişisel Verilerin Korunması Kanunu kapsamında *açık* rıza kişisel veriler arasında herhangi bir ayırım yapılmaksızın şart koşulmaktadır. Belirtmek gerekir ki, Kanun'da Avrupa Birliği Veri Koruma Yönergesi'nde tesis edilmiş olan hukuka uygunluk sistematiğinden farklı bir sistematik kullanılmıştır. Kanun'un 5 maddesinin 1. fıkrasında kural olarak kişisel verilerin ilgilili kişinin açık rızası olmaksızın işlenemeyeceği belirtilmiş ve devamı fıkra hukuka uygunluk halleri sayılmıştır. Bu durum, rızanın diğer hukuka uygunluk sebeplerine karşısında hiyerarşik bir önceliği varmış izlenimi yarattığı gerekçesi ile eleştirilmiştir⁵⁵. Bu duruma ilişkin olarak Kişisel Verileri Koruma Kurumu tarafından hazırlanan kılavuzda⁵⁶ “açık rıza”nın, ilgili maddenin 2. fıkrasında sayılan diğer kişisel veri işleme şartlarına nazaran herhangi bir üstünlüğü olmadığı belirtilerek açıklığa kavuşturulmuştur.

Kanun'da açık rıza ise “*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*” olarak tanımlanmıştır. Kanunun gerekçesinde ise açık rızaya ilişkin olarak “*ilgili kişinin özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı*” ifadesine yer verilmiştir. Bu doğrultuda her bir somut olay bakımından geçerli bir açık rızanın koşullarının değerlendirilmesi gerekmektedir.

Her ne kadar Kanun'da açık rıza için herhangi bir şekil şartı aranmıyor olsa da veri sorumlusunun yükümlülüğünü yerine getirdiğinin ispatı adına kayıt edilebilir araçların açık rıza süreçlerinde kullanılması gerekmektedir. Öte yandan açık rızanın alınmasına ilişkin olarak hazırlanacak olan metinlerin açık, anlaşılır ve sade olması önem taşımaktadır. Kurum tarafından hazırlanan kılavuzlarda açık rızanın alındığı ortam

⁵⁵ Yücedağ, **a.g.m.**, s. 773.

⁵⁶ Kişisel Verileri Koruma Kurumu, “6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar”, s. 21.

veya metin dışındaki başka bir ortama veya metne atfı yapılarak ilgili kişinin açık rızasının alınamayacağı ifade edilmiştir. Bununla birlikte açık rızanın belirtilen unsurlarının yorumlanmasında somut olay bazında genel ilkeler ışığında bir değerlendirme yapmak önem arz etmektedir. Örneğin; özgür iradeye dayanma unsuru bakımından kişisel verilerin işlenmesine ilişkin olarak bireye sorulan açık rızanın bir sözleşmenin ifası ya da kurulması için ön şart olarak düzenlenip düzenlenemeyeceği tartışılmaktadır⁵⁷. Özgür iradede bahsedebilmek için açık rızanın kolay ve bedelsiz bir yol ile birey tarafından geri alınabiliyor olması gerekmektedir⁵⁸. Kişisel Verileri Koruma Kurumu özgür irade unsurunun değerlendirilmesinde taraflar arasındaki ilişkinin de göz önünde bulundurulması gerektiğine işaret etmektedir⁵⁹. Bu bakımdan işçi işveren arasındaki ilişki çerçevesinde işçi tarafından verilen rızanın özgür iradeye dayanıp dayanmadığı hassas bir şekilde değerlendirilmelidir.

Bilgilendirme yükümlülüğünü yerine getirmek adına hazırlanan uzun ve okuyucu dostu olmayan metinler aracılığı ile bireylere açık rızalarının sorulması dürüstlük ilkesiyle bağdaşmamaktadır. Açık rıza metinlerinin içerisinde kişisel verilerin işlenmesine ilişkin olarak doğrudan belirtilmeyen, geniş düzenlenmiş amaç bildirimleri rızanın geçersizliği sonucunu meydana getirebilecektir. Kişisel Verileri Koruma Kurumu, ilgili kişinin anlamayacağı terimlerin kullanılmaması gerektiğini ve yazılı olarak açık rızanın ilgili kişiden talep edilmesi halinde ilgili kişinin güçlük çekeceği oranda küçük puntolar kullanılmaması gerektiğini belirtmektedir⁶⁰. Bu doğrultuda tüketicinin korunması mevzuatında aranan 12 punto şartının kişisel verilerin işlenmesine ilişkin bilgilendirme metinlerinde de aranması gerekmektedir⁶¹.

⁵⁷ Mesut Serdar Çekin, “6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt 74, Sayı 2, 2016, s. 637.

⁵⁸ Küzeci, **a.g.e.**, s. 241.

⁵⁹ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, s. 50.

⁶⁰ **a.e.**, 49.

⁶¹ 6502 sayılı Tüketicinin Korunması Hakkında Kanun’un temel ilkeler başlıklı 4. Maddede “*Bu Kanunda yazılı olarak düzenlenmesi öngörülen sözleşmeler ile bilgilendirmeler en az on iki punto büyüklüğünde, anlaşılabilir bir dilde, açık, sade ve okunabilir bir şekilde düzenlenir ve bunların bir nüshası kâğıt üzerinde veya kalıcı veri saklayıcısı ile tüketiciye verilir. Sözleşmede bulunması gereken şartlardan bir veya birkaçının bulunmaması durumunda, eksiklik sözleşmenin geçerliliğini etkilemez. Bu eksiklik sözleşmeyi düzenleyen tarafından derhâl giderilir*” hükmü yer almaktadır.

Bununla birlikte özellikle kişiye seçenек tanımayan ve matbu olarak hazırlanıp bir sözleşme yahut eki kapsamında alınan rızaların Türk Borçlar Kanunu'nda yer alan genel işlem koşulları bakımından da değerlendirilmesi gerekmektedir⁶². Türk Borçlar Kanunu'nun 27. Maddesi uyarınca kişilik hakkına aykırı olan sözleşmeler kesin olarak hükümsüzdür. Bununla birlikte sözleşmeyi düzenleyen tarafa tek taraflı olarak karşı taraf aleyhine sözleşme hükümlerini değiştirme ya da yeni düzenleme getirme yetkisi veren genel işlem koşullarının bulunduğu ya da ayrı bir sözleşme kapsamında yer alan kayıtların yazılmamış sayılacağı Türk Borçlar Kanunu'nda hüküm altına alınmıştır (m. 24). Kişilik hakkı açısından sözleşme yahut eklerinde geniş kapsamlı muğlak ve sözleşmeyi hazırlayan tarafın değiştirmesine elverişli bir açık rıza metnine yer verilmesi, bu kapsamda değerlendirilebilecektir. Ancak yukarıda da belirtilmiş olduğu üzere, bireylerin kişilik hakkına aykırılık, Medeni Kanun uyarınca kesin hükümsüzlük yaptırımına tabi tutulmuştur. Buna göre Türk Borçlar Kanunu'nda yer alan genel işlem koşullarına ilişkin düzenleme (m. 24) uyarınca yazılmamış sayılma hali söz konusu olacakken; Medeni Kanun'un kişiliği koruyan hükümleri (m. 23/2) ve Türk Borçlar Kanunu'nun sözleşmenin içeriğine ilişkin hükümler (m. 27) uyarınca kesin hükümsüzlük yaptırımına tabi tutulacaktır. Belirtmek gerekir ki genel işlem koşulları bakımından bir kapsam değerlendirilmesi yapıp değişiklik yapma yetkisini sözleşmeyi düzenleyen tarafta tutan, açık rıza hükümlerinin yazılmamış sayılma yaptırımına tabi tutulması için mutlaka bir kişilik hakkı ihlali ispatı zorunlu değildir. Söz konusu değiştirme yetkisinin ayrıca kişilik hakkını ihlal edecek düzeyde yetkiler sağlaması aranmamaktadır⁶³.

Belirtmek gerekir ki kişisel verilerin işlenmesi bakımından açık rıza her koşulda uygulanması gereken garanti bir yol olarak düşünülmemelidir. Nitekim, sürekli ve aktif olarak bireylerden açık rızalarının sorulması bireylerin tepkisizliğini gündeme getirebilecektir. Rıza yorgunluğu olarak adlandırılabilir olan bu durumun önüne geçmek için Avrupa Birliği Genel Veri Koruma Tüzüğü'nde varsayılan ayarlarla veri

⁶² Genel işlem koşulları bağlamında kişisel verilerin korunması hakkında detaylı bir inceleme ve değerlendirme için bkz. Taştan, **a.g.e.**, s. 94 vd.

⁶³ Başak Görgeç, "Genel İşlem Koşullarının Kişilik Hakkı Kapsamında Değerlendirilmesi", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 19, Sayı 1, 2013, s. 436-437.

koruma ilkesi bir çözüm olarak değerlendirilmektedir⁶⁴. Bu bakımdan Türk hukukunda bu ilkeye yer verilmemesi eleştirilmeye değerdir.

Belirtmek gerekir ki 10 Mart 2018 tarihli 30356 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ’inde kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiği belirtilmektedir. Bu bakımdan açık rıza gerektirmeyen hukuka uygunluk sebeplerinin doğru değerlendirilmesi ve açık rıza gerektiren kişisel veri işleme amaçlarının tespiti önem arz etmektedir. Nitekim kişisel verilerin işlenmesini gerektirecek sebebin Kanun’da öngörülmüş olan bir hukuka uygunluk sebebine dayanması halinde açık rızanın ilgili kişiden talep edilmesine gerek olmayacaktır⁶⁵.

3.2.4.2. Kanunlarda Açıkça Öngörülmüş Olma

Kişisel Verilerin Korunması Kanunu’nda, Yönerge’den ayrı olarak kişisel verilerin işlenmesinin kanunlarda açıkça öngörülmüş olması bir hukuka uygunluk nedeni olarak belirtilmektedir. Kişisel Verilerin Korunması Kanunu’nun gerekçesinde kolluk tarafından bir suç soruşturması sebebiyle, 2559 sayılı Polis Vazife ve Salahiyet Kanununun 5. maddesi uyarınca şüphelilerin parmak izlerinin alınması; 5352 sayılı Adli Sicil Kanunu uyarınca Adalet Bakanlığının kişilerin ceza mahkûmiyetlerine ilişkin verilerini işlemesi gibi örnekler yer almaktadır. Kanunlarda açıkça öngörülme hukuka uygunluk sebebi esasen Anayasa’da da yer alan “*kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*” hükmünün bir yansıması olarak görülebilir. Gerçekten de gerek Kişisel Verilerin Korunması Kanunu genel ilkeleri, gerekse Anayasa hükümleri gereği kişisel verilerin kanunlarda açıkça öngörülmüş olması şartı ile işlenebileceğinin bu hüküm olmasa bile kabulü gerekebilecektir. Ancak bu hükmün yer alması özel nitelikli kişisel veriler bakımından bir belirsizlik yaratmaktadır. Zira özel nitelikli kişisel verilerin işlenme hallerinin düzenlendiği 6. maddenin 3. fıkrasında

⁶⁴ Rıza yorgunluğuna ilişkin açıklamalar için bkz. Taştan, **a.g.e.**, s. 166.

⁶⁵ Çekin, **a.g.e.**, s. 64.

sağlık ve cinsel hayata ilişkin kişisel verilerin kanunlarda öngörülen hallerde işlenebilmesi bir hukuka uygunluk sebebi olarak belirtilmektedir.

Kanunlarda açıkça öngörülme hukuka uygunluk sebebinin uygulanması bakımından ilgili mevzuatta öngörülen süre kadar muhafaza edilme ilkesi büyük önem taşımaktadır. Kişisel veri işleme faaliyetinin amaç unsurunun bir kanun hükmüne dayandırılması halinde kanun hükmü ile sınırlı ve ölçülü olarak değerlendirme yapılması gerekmektedir. Örnek olarak işveren açısından çalışan bilgilerinin sosyal güvenlik mevzuatı gereği kaydedilmesi bu hukuka uygunluk sebebi altında değerlendirilebilecek iken bu verilerin çalışan işten çıktıktan sonra dahi tutulması hakkın tesisi korunması hukuka uygunluk sebebi altında değerlendirilebilecektir. Yine 4857 sayılı İş Kanunu 75. madde uyarınca işçinin özlük dosyasının oluşturulması bu dosya içerisinde bulunması gereken belge ve verileri toplayarak oluşturması kanunlarda açıkça öngörülme hukuka uygunluk sebebi olarak değerlendirilebilecektir. Verilerin toplanma amacı ile işleme amacının örtüşmesi gerekmektedir. Bu nedenle herhangi bir kanun hükmüne dayanarak toplanan kişisel verilerin kanunda belirtilen amaçları aşacak şekilde işlenmesi, daha uzun süre ile saklanması hukuka aykırılık teşkil edecektir.

Kanunlarda açıkça öngörülmüş olma hukuka uygunluk sebebi bakımından bir diğer önemli husus, kanunlarda belirtilmiş olan veri içeriği ile işlenen veri içeriğinin sınırlı olması gerekliliğidir. Bu bakımdan 5070 Sayılı Elektronik İmza Kanunu madde 9 örnek verilebilir. İlgili kanunda nitelikli elektronik sertifikada bulunması gereken hususlar ve bu hususlar altında hangi kişisel verilerin toplanması ve işlenmesi gerektiği belirtilmiştir. Yine kamu açısından 5490 sayılı Nüfus Hizmetleri Kanunu 43. maddede *“Nüfus kayıt örneklerinde, bunları istemeye yetkili olanlar tarafından açıkça ve gerekçeli olarak istenmediği takdirde, kimlik bilgileri dışında kişisel bilgilere yer verilmez. Bu belgeler üzerinde silinti ve kazıntı yapılamaz”* ibaresi yer almaktadır. Bu doğrultuda nüfus kaydı örneği vermeye yetkili kamu kuruluşunda talep edilenden daha fazla kimlik bilgisi dışında kişisel verinin yer aldığı belgenin düzenlenmesi ve paylaşılması hukuka aykırılık teşkil edecektir.

Kişisel Verilerin Korunması Kanunu öncesi hazırlanarak yürürlüğe giren bu düzenlemede ayrıca 12. maddede ile elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edilemeyeceği ve bu bilgilerin kişinin rızası dışında elde edilemeyeceği belirtilmektedir. Bilgilerin korunması başlıklı söz konusu madde olmasa bile Kişisel Verilerin Korunması Kanunu hükümleri gereğince bir kısıtlama ve dar yorumlama gerekliliği bulunmaktadır.

Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesi ile birlikte kişisel verilerin işlenmesini öngören kanun ve yönetmelik hükümlerine ayrıca koruyucu hükümler eklenmiştir. 11 Ekim 2016 tarihli 29854 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Özel İstihdam Büroları Yönetmeliği'nde 24. Madde de *"24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ve 4904 sayılı Kanunun 19 uncu maddesi hükümleri çerçevesinde; özel istihdam bürosu, iş ve işçi bulmaya aracılık için derlediği verileri bu amaçlar dışında kullanamaz"* hükmü yer almaktadır.

Yukarıdaki örneklerden de görülebileceği üzere ilgili hukuka uygunluk sebebinin hem kamu sektörü hem de özel sektör açısından bağlayıcılığı bulunmakla birlikte veri sorumlularının herhangi bir kanun hükmüne dayanarak kişisel veri işleme faaliyetinde bulunmaları halinde gereklilik ve ölçülülük denetimlerini hassas bir şekilde yapmaları büyük önem taşımaktadır. Kişisel Verilerin Korunması Kanunu'nda ilgili hukuka uygunluk sebebinde sadece kanunlarda açıkça öngörülme şartı aranmakta olduğu için yönetmelik, tüzük gibi diğer mevzuatlarda öngörülen kişisel veri işleme faaliyetlerinin ne şekilde değerlendirileceğinin netleştirilmesi gerekmektedir. Ancak Anayasa'da yer alan kişisel verilerin işlenmesine ilişkin hususların ancak kanunlar ile düzenlenebileceğine ilişkin hüküm gereğince zaten tek başına herhangi bir kanundan yetki almamış bir yönetmelik ile kişisel verilerin işlenmesinin düzenlenmesi Anayasa'ya aykırılık teşkil edeceğinden⁶⁶ kanunlarda açıkça öngörülmesi kaydı ile bir

⁶⁶ Yasama yetkisinin devredilemezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemeyeceğine ilişkin olarak elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisini Bilgi Teknolojileri ve İletişim Kurumuna veren 5809 sayılı Elektronik Haberleşme Kanunu'nun 51. maddesinin Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla

yönetmelik çerçevesinde düzenlenen kişisel verilerin işleme faaliyetlerinin de hukuka uygunluk sebebi teşkil edeceğinin kabulü gerekmektedir.

3.2.4.3. Fiili İmkânsızlık Durumunda Yaşamsal Çıkarların Koruması

Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan kişinin veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması halinde ilgili kişinin kişisel verilerinin ilgili kişinin rızası aranmaksızın işlenebileceği Kişisel Verilerin Korunması Kanunu’nda hüküm altına alınmaktadır. Yönerge ile paralel olan bu düzenleme ile ilgili kişi ya da üçüncü bir kişinin yaşamsal çıkarlarının korunması için gerekli olması halinde ilgili kişinin rızasını açıklamayacak durumda olması yahut rızasına sonuç bağlanamayacak olması halinde kişisel verilerinin işlenebileceğinin kabulü gerekmektedir⁶⁷. Ancak söz konusu hukuka uygunluk hali özel nitelikli kişisel veriler bakımından Kişisel Verilerin Korunması Kanunu’nda geçerli sayılmamaktadır.

Kişisel Verilerin Korunması Kanunu’nun uygulanmasına ilişkin açıklık getirmek amacı ile Kişisel Verileri Koruma Kurumu tarafından hazırlanmış olan yayında⁶⁸ ve ilgili Kanun gerekçesinde bu duruma örnek olarak kişinin bilincinin yerinde olmadığı veya akıl hastası olması sebebiyle rızasının geçerli olmadığı bir durumda, hayat veya beden bütünlüğünün korunması amacıyla, tıbbi müdahale anında kişinin kan grubu, geçirdiği hastalıklar ve ameliyatlar kullandığı ilaçlar gibi bilgilerin edinilmesi ve ilgili sağlık sistemi üzerinden kişisel verilerin işlenebilmesi halleri sayılmaktadır. Sayılan verilerin özel nitelikli kişisel veri içermesi sebebi ile Kişisel Verilerin Korunması Kanunu’nun özel nitelikli kişisel verilerin işlenmesine ilişkin şartların yer aldığı 8. maddenin ne şekilde yorumlanacağına ilişkin bir belirsizlik doğmaktadır. Söz konusu kaynaklarda verilerin örneklerin sehven yahut bilinçli olarak mı sayıldığına ilişkin

düzenlenebileceğine ilişkin güvenceye aykırı olduğuna ilişkin Anayasa Mahkemesi Kararı için bkz. 26 Temmuz 2014 tarihli 29072 sayılı Resmi Gazete’de yayımlanan Esas Sayısı: 2013/122 Karar Sayısı: 2014/74 olan Anayasa Mahkemesi Kararı.

⁶⁷ Yücedağ, **a.g.m.**, s. 777.

⁶⁸ Kişisel Verileri Koruma Kurumu, “Kişisel Verilerin Korunması Kanunu ve Uygulaması”, Ankara, s.50, (Çevrimiçi) <http://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf> , 18 Nisan 2018.

Kişisel Verileri Korunma Kurumu tarafından açıklık getirilmesi gerekmektedir. Özel nitelikli kişisel verilerin işleme şartlarında söz konusu hukuka uygunluk nedeninin sayılmamış olması sebebi ile hürriyeti kısıtlanan bir kişinin kurtarılması amacıyla kendisinin veya şüphelinin taşımakta olduğu telefon, bilgisayar, kredi kartı, banka kartı veya diğer teknik bir araç üzerinden yerinin belirlenmesi için bu verilerin işlenmesi yahut bilinci kapalı kişinin ya da yakınının iletişim veya adres bilgisinin öğrenilmesi gibi örneklerin hükmün uygulama alanı açısından daha uygun olacağının kabulü gerekmektedir.

İlgili hukuka uygunluk sebebinin temel unsurları olan fiili imkânsızlık ve ilgili kişi yahut üçüncü bir kişinin hayatı yahut beden bütünlüğünün korunması için gerekli olma hallerinin tespiti önem taşımaktadır. Söz konusu hukuka uygunluk sebebinin uygulama alanı bulabilmesi için bir aciliyet söz konusu olması gerekmektedir. Kişinin rızasının açıklanmasının beklenebileceği durumlarda işbu hukuka uygunluk sebebi geçerli olmayabilecektir.

3.2.4.4. Sözleşmenin Kurulması veya İfası Kapsamında Gerekli Olma

Kişisel Verilerin Korunması Kanunu'nda yer alan hüküm uyarınca bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde hayatın olağan akışı gereği ilgili kişilerin kişisel verilerinin gereklilik ve ölçülülük ilkeleri uyarınca işlenmesinin hukuka uygunluk sebebi teşkil edeceğinin kabulü gerekmektedir. Ancak belirtmek gerekir ki Kişisel Verilerin Korunması Kanunu kapsamında özel nitelikli kişisel verilerin bir sözleşmenin kurulması yahut ifası kapsamında işlenmesi bir hukuka uygunluk hali olarak düzenlenmemiştir. Bu bakımdan bu başlık altında yer alan hukuka uygunluk sebebine ilişkin açıklamaların genel nitelikli kişisel veriler bakımından olduğunun belirtilmesi gerekmektedir. Genel nitelikli kişisel verilerin bir sözleşmenin kurulması veya ifası için gerekli olması halinde söz konusu verilerin sadece sözleşme tarafları için mi yoksa ifa yardımcısı sıfatında bulunan üçüncü kişiler bakımından da yararlanılabilecek bir hukuka uygunluk sebebi olup olmadığının tartışılması gerekmektedir. Kanun'da açıkça işleme konu olacak kişisel verilerin sözleşme taraflarına ilişkin olması gerektiği belirtilmiş ancak veri sorumlusu yahut

veri işleyen sözleşmenin tarafı olup olmayacağına ilişkin bir ibare eklenmemiştir. Avrupa Birliği'nde yer alan düzenlemelerde de bu açıklık yer almamaktadır. Bu doğrultuda madde hükmünün bu konuyu bilerek düzenlemediğinin kabulü gerekmektedir. Nitekim söz konusu hukuka uygunluk sebebi aynı zamanda veri aktarımı bakımından da geçerli bir hukuka uygunluk sebebi olup, sözleşmenin ifası için kişisel verilerin sözleşmeye taraf olmayan üçüncü kişiler ile paylaşılması ve söz konusu üçüncü kişilerin sadece sözleşmenin ifası ile sınırlı olarak bu verileri işleyebilmesi madde hükmünden beklenen yararın karşılanması için gereklidir⁶⁹. Örnek olarak mesafeli satış sözleşmesi ile satın alınan bir ürünün kargo ile teslim edilmesi sırasında adres ve kimlik bilgilerinin taşıyıcı firma ile paylaşılması, taşıyıcı firmanın bu verileri sadece malın teslimi için işlemesi faaliyeti hukuka uygun bulunmalıdır⁷⁰.

Belirtmek gerekir ki söz konusu hukuka uygunluk sebebinin üç temel unsuru bulunmaktadır: **i.** akdedilmesi görüşülen yahut akdedilmiş bir sözleşme olması, **ii.** işlenecek kişisel verilerin sözleşmenin taraflarına ilişkin olması, **iii.** sözleşmenin ifası yahut kurulması için doğrudan doğruya ilgili ve gerekli olması gerekmektedir.

Hayatın olağan akışı gereği bir sözleşmenin müzakereleri, kurulması ve ifası aşamalarında kişisel verilerin işlenmesi kaçınılmazdır. Sözleşme yapmak amacı ile görüşmeye başlayan taraflar arasında tarafların birbirlerinin kişisel verilerini işlemesi sözleşmenin kurulması kapsamında değerlendirilebilecektir. Bu duruma örnek olarak iş görüşmesi kapsamında işverenin adaya yönelmiş olduğu sorular ve cevapları sayılabilecektir. Ancak belirtmek gerekir ki bu soruların amacı iş sözleşmesinin kurulmasına yönelik, hukuka ve dürüstlük kuralına uygun olmalıdır. Aksi takdirde **culpa in contrahendo** sorumluluğu söz konusu olabilecektir⁷¹. Asgari olarak sözleşme içerisinde tarafların, ifa konusunun niteliğinin ve şartlarının düzenlenmesi aranmaktadır. Bu bakımdan her sözleşme tipi bakımında muhteviyatı değişmekle

⁶⁹ Hüseyin Murat Develioğlu, **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, 1. Baskı, İstanbul, On İki Levha Yayıncılık, 2017, s. 61.

⁷⁰ Aksi görüş için bkz yukarıda s. 79.

⁷¹ Selen Uncular, **İş İlişkisinde İşçinin Kişisel Verilerinin Korunması**, Ankara, Seçkin Yayıncılık, 2014, s. 72-73.

birlikte sözleşme süreçleri kapsamında kişisel veri işleme faaliyetlerinin hukuka uygunluğunun kabulü gerekmektedir. Ancak tarafların birbirine yöneltilmiş olarak bir sözleşme kurma yönünde beyanı açık yahut örtülü olarak aranmalıdır. Bu doğrultuda ilgili kişinin iradesi olmaksızın bir sözleşme taslağı iletmek ve bu kapsamda ilgili kişinin kişisel verilerini işlemek hukuka uygun olmayacaktır. İşlenen kişisel verilerin sözleşmenin taraflarına ilişkin olması gerekmele birlikte üçüncü kişi yararına yapılan sözleşmeler bakımından bir belirsizlik doğabilecektir. Bu doğrultuda konusu sözleşme taraflarından farklı bir kişiye hediye gönderilmesi, çiçek gönderilmesi gibi olan sözleşmelerde üçüncü kişinin açık rızasının aranması gerekmektedir⁷².

Bir üst paragrafta da belirtildiği üzere, sözleşme süreçleri dâhilinde kişisel veri işlemenin hayatın olağan bir akışı olduğunun kabulü ile birlikte her bir somut olay kapsamında gereklilik ilkesi bakımından ayrıca bir değerlendirme yapılmalıdır. Örnek olarak yüz yüze satış süreçlerinde müşteri ve mal sahibi arasında kurulacak sözleşme için teslimat adresi gerekmediğinden kişinin adresi⁷³ sözleşmenin kurulması ifası hukuka uygunluk nedeni ile talep edilemezken, mesafeli satış sözleşmelerinde kişinin adres bilgisinin talep edilmesi sözleşmenin ifası için doğrudan doğruya ilgili kabul edilmektedir.

Kişisel Verilerin Korunması Kanunu’nun uygulanmasına ilişkin açıklık getirmek amacı ile Kişisel Verileri Koruma Kurumu tarafından hazırlanmış olan yayında⁷⁴ ve Türkiye Büyük Millet Meclisi’ne sevk edilen tasarı metni gerekçesinde bu duruma örnek olarak, yapılan bir sözleşme gereği paranın ödenmesi için alacaklı tarafın hesap numarasının talep edilmesi, banka ile kredi sözleşmesi yapılması sırasında bankanın, o kişiye ait maaş bordrosunu, tapu kayıtlarını, icra borcu olmadığına dair belgeyi talep etmesinin bu kapsamda değerlendirileceği belirtilmektedir.

⁷² Sözleşmeye taraf olmayan üçüncü kişi yararına yapılan sözleşmelerde ilgili kişinin kişisel verilerinin Kişisel Verilerin Korunması Kanunu m. 5/2 (c) kapsamında değerlendirilebileceğine ilişkin olarak bkz. Çekin, **a.g.e.**, s. 74.

⁷³ Vergi Usul Kanunu madde 230 uyarınca faturada bulunması zorunlu bilgiler kapsamında müşterinin adres bilgisinin talep edilmesi kanunlarda açıkça öngörülme hukuka uygunluk sebebi altında değerlendirilmelidir.

⁷⁴ Kişisel Verileri Koruma Kurumu, “Kişisel Verilerin Korunması Kanunu ve Uygulaması”, s. 51.

3.2.4.5. Veri Sorumlusunun Hukuki Yükümlülüğü

Kişisel Verilerin Korunması Kanunu madde 5 uyarınca veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için kişisel verileri işleminin zorunlu olması halinde veri işleme faaliyeti hukuka uygun olacaktır. Bu hukuka uygunluk sebebi bakımından veri sorumlusunun kişisel veri işlemini gerektirecek bir hukuki yükümlülüğünün olması gerekmektedir. Kişisel Verilerin Korunması Kanunu'nun uygulanmasına ilişkin açıklık getirmek amacı ile Kişisel Verileri Koruma Kurumu tarafından hazırlanmış olan yayında⁷⁵ ve Kanun'un gerekçesinde bir işverenin çalışanına ödeyeceği maaşı tespit edebilmesi ve ödeyebilmesi için, evli olup olmadığı, bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı, sosyal sigorta numarası ve banka hesap numarası gibi verileri elde etmesi ve işlemesi; işverenin vergi denetimi sırasında çalışanlarına veya müşterilerine ait bilgileri ilgili kamu görevlilerinin incelemesine sunması bu hukuka uygunluk sebebi çerçevesinde örnek olarak sayılmaktadır. Bir başka deyişle vergi hukuku ile ilgili düzenlemeler veya sosyal güvenlik mevzuatı uyarınca getirilen yükümlülükler kapsamında yürütülen kişisel veri işleme faaliyetleri bu kapsamda değerlendirilebilecektir. Belirtmek gerekir ki özel nitelikli verilerin veri sorumlusunun hukuki yükümlülüğü kapsamında işlenmesi, Kanunu'ndaki hukuka uygunluk sebepleri arasında sayılmamıştır.

Veri sorumlusunun hukuki yükümlülüğünü yerine getirirken dikkat etmesi gereken en önemli sınırlamalardan biri ise gereklilik ve ölçülülük ilkelerine uygun olarak kişisel verileri işleme faaliyetini yürütmesidir. Bu bakımdan mahkeme tarafından talep edilen bir bilgi yahut belgenin sunulması her ne kadar hukuki bir yükümlülük olarak değerlendirilecek olsa da zorunlu ve talep edilen belgelerin dışında fazlaca bilgi ve belge sunulması hukuka aykırı olarak nitelendirilecektir. Bu doğrultuda Kişisel Verileri Koruma Kurumu, 23 Şubat 2018 tarihli kararında, mahkemece talep edilmemiş olmasına rağmen davalıya ait kredi kartının Kasım 2016 - Nisan 2017 dönemine ait 6 aylık ekstresinin de mahkemeye iletilmiş olmasını hukuka aykırı bularak, idari para cezası yaptırımını uygulamıştır. İlgili kişinin temel hak ve özgürlüklerinin korunması bakımından veri sorumlularının kamu otoriteleri tarafından

⁷⁵ a.e., s. 51-52.

talep edilen bilgi ve belgelere ilişkin olarak şüpheli yaklaşımları gerekmektedir. Nitekim Yargıtay 12. Hukuk Dairesi 16 Kasım 2015 tarihli vermiş olduğu bir kararda⁷⁶, borçlu şirketin tebligata yarar adresinin, telefon numaralarının, hesap açılırken üçüncü kişiye verilen bütün evraklarının birer suretinin, borçlunun ortaklarının adres, kimlik ve iletişim bilgilerinin, borçlunun çek hesabı dışında başkaca hesabının bulunup bulunmadığının, başkaca hesaplar var ise hesap numaralarının ve hesapların bakiye bilgilerinin bankadan 2004 sayılı İcra ve İflas Kanunu'nun 367. maddesinde yer alan “*İcra ve İflas dairelerinin borçlunun mevcuduna dair isteyeceği bütün malumatı hakiki ve hükmi her şahıs derhal vermeğe ve talep halinde mevcudu bu dairelere teslim mecburdur*” hükmü kapsamında istenemeyeceğine hükmetmiştir.

Veri sorumlusunun hukuki yükümlülüğünü yerine getirirken kişisel verileri işlemesi gerekmesi durumunda dikkat edilmesi gereken bir diğer önemli sınırlama ise kişisel verilerin işleme amacı doğrultusunda gerekli olan süre kadar muhafaza edilme ilkesine uyulmasıdır. Örneğin; 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve 11 Nisan 2017 tarihli ve 30035 sayılı Resmî Gazete’de yayımlanarak yürürlüğe giren İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik ile internet toplu kullanım hizmet sağlayıcılara erişim kayıtlarını elektronik ortamda kendi sistemlerine kaydetme ve iki yıl süre ile saklama yükümlülüğü getirilmiştir. Bu doğrultuda internet toplu kullanım hizmet sağlayıcının söz konusu verileri saklama yükümlülüğü bulunmakla birlikte bu verileri saklaması için getirilmiş olan süre gerekliliği iki yıldır. İki yıldan uzun süre söz konusu verileri saklayan internet toplu kullanım hizmet sağlayıcının söz konusu fiili hukuka uygunluk sebeplerinden yoksundur.

3.2.4.6. Kişisel Verinin İlgili Kişi Tarafından Alenileştirilmesi

Yönerge’de özel nitelikli kişisel verilerin işlenmesinde sayılan hukuka uygunluk nedenleri arasında olan bir kişisel verinin kamuya açıklanmış olması bir başka deyişle, alenileştirilmesi hususu Kişisel Verilerin Korunması Kanunu kapsamında genel

⁷⁶ Yargıtay 12. Hukuk Dairesi, Esas Sayısı: 2015/16406, Karar sayısı: 2015/28245, Karar tarihi: 16 Kasım 2015.

nitelikli kişisel verilerin işlenmesi bakımından bir hukuka uygunluk nedeni olarak belirtilmiştir. Kişisel Verilerin Korunması Kanunu kapsamında özel nitelikli kişisel veriler için ise alenileşmiş olma bir hukuka uygunluk nedeni teşkil etmemektedir. Kişisel Verileri Koruma Kurumu tarafından hazırlanmış olan yayında⁷⁷ alenileştirme kavramı herkes tarafından bilinir kılma şeklinde tanımlanmıştır. Kişisel Verilerin Korunması Kanunu gerekçesinde ilgili kişinin kendisi tarafından alenileştirilen bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verilerin işlenebileceği, ilgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinebilecek hale gelen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın bulunmadığı ifade edilmiştir. Ancak belirtmek gerekir ki bir verinin aleni hale gelmiş olması o veriye ve ilgili kişiye atfedilen koruma alanını ortadan kaldırmamaktadır⁷⁸. Nitekim Kişisel Verilerin Korunması Kanunu gerekçesinde, kişisel verilerin herhangi bir nedenle başkaları tarafından bilinebilir hâle gelmesi ile sadece bu nedenle söz konusu verinin kişisel veri olma niteliğini kaybetmeyeceği belirtilmiştir⁷⁹. İlgili bölümde yapılan değerlendirmede, bir bilginin kişisel veri olma niteliğinin başkalarının öğrenmesi ile bağlantılı olmadığı aksine ilgili kişinin söz konusu kişisel veri olarak tutma yönünde bir iradeye sahip olup olmamasının bir ölçüt olduğu tespiti yapılmıştır. Bu tespit ile ilgili kişi tarafından alenileştirilmemiş olmasına rağmen bir biçimde kamu tarafından öğrenilen ve aleni hale gelen verinin sadece bu durum nedeni ile kişisel verilere ilişkin korunmadan yararlanamayacağı söylenemez. Bu doğrultuda söz konusu hukuka uygunluk sebebinin en önemli unsuru alenileştirme işleminin ilgili kişinin iradesi ile yapılmış olma şartıdır.

Kişisel Verileri Koruma Kurumu tarafından hazırlanmış olan bir diğer yayında⁸⁰ ve Kişisel Verilerin Korunması Kanunu'nun gerekçesinde bir kişinin belirli durumlarda kendisiyle iletişime geçilmesi amacıyla iletişim bilgilerini kamuya açık şekilde ilan etmesi, kurumsal internet sitelerinde, çalışanların işyeri telefon numaraları ve

⁷⁷ Kişisel Verileri Koruma Kurumu, “6698 Sayılı Kanun’da Yer Alan Kurumsal Terimler”, s. 9, (Çevrimiçi) <http://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20KANUN%E2%80%99DA%20YER%20ALA%20KURUMSAL%20TER%20C4%B0MLER.pdf>, 22 Mart 2018.

⁷⁸ Yücedağ, **a.g.m.**, s. 780.

⁷⁹ “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 24.

⁸⁰ Kişisel Verileri Koruma Kurumu, “Kişisel Verilerin Korunması Kanunu ve Uygulaması”, s. 52.

kurumsal elektronik posta adreslerinin üçüncü kişilerin erişimine açık şekilde paylaşılması halinde de söz konusu verilerin alenileştirildiği ve bu kişisel verilerin hukuka uygun olarak işlenebileceği ifade edilmektedir. Kişisel verilerin alenileştirilmiş olması halinde diğer hukuka uygunluk sebeplerinden ayrı olarak bir başka istisna da Kişisel Verilerin Korunması Kanunu kapsamında tanınmıştır. Kişisel Verilerin Korunması Kanunu’nun istisnalar başlıklı 28. maddesinin 2. fıkrasında Kanun’un amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10. maddesinin; zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11. maddesinin ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16. maddesinin ilgili kişinin kendisi tarafından verilerinin alenileştirilmiş olması halinde uygulanmayacağı hüküm altına alınmaktadır.

İlgili kişi tarafından alenileştirilmiş olması sebebine dayanarak yürütülecek kişisel veri işleme faaliyetleri bakımından ilgili kişinin söz konusu kişisel verileri alenileştirme bağlamı ve amacı göz önünde bulundurularak bir değerlendirme yapılması gerekmektedir.

3.2.4.7. Hakkın Tesisi, Kullanılması veya Korunması için Zorunlu Veri İşleme

Kişisel Verilerin Korunması Kanunu’nda, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması hali bir hukuka uygunluk sebebi olarak kabul edilmektedir. Belirtmek gerekir ki Avrupa Birliği Genel Veri Koruma Tüzüğü ve Yönerge kapsamında bu hukuka uygunluk sebebinin birebir karşılığı bulunmamaktadır. Yönerge’de⁸¹ özel nitelikli kişisel verilerin işlenmesi bakımından, yasal taleplerin tesisi, kullanılması veya savunulması için gerekli olması hali bir hukuka uygunluk sebebi olarak sayılmaktadır. Kişisel Verilerin Korunması Kanunu’nda ise söz konusu hakkın hukuki bir talep olması, sözleşmeden yahut bir kanun hükmünden doğması şartı aranmamaktadır. “Veri sorumlusunun hukuki yükümlülüğü” ve “kanunlarda açıkça öngörülme” hukuka uygunluk sebeplerinden farklı olarak bu halde tesis edilecek, kullanılacak yahut korunacak olan hakkın veri sorumlusuna mı yahut ilgili kişiye mi ait olacağına ilişkin ayırım yapılmamaktadır. Bu

⁸¹ Yönerge m. 8(2) e.

doğrultuda herhangi bir kişinin hakkının tesisi, kullanılması yahut korunması için gerekli bir kişisel veri işleme faaliyeti hukuka uygun kabul edilecektir. Kişisel Verilerin Korunması Kanunu'nun gerekçesinde⁸² bir şirketin kendi çalışanı tarafından açılan bir davada ispat için çalışanın kişisel verilerini kullanması veya kısıtlı bir kişinin haklarının korunması amacıyla vasiinin veya kayyımın, kısıtlının mali bilgilerine erişebiliyor olması söz konusu hukuka uygunluk sebebine örnek olarak verilmiştir. Bu kapsamda dava açılması, tescil işlemleri, her türlü tapu işlemi gibi bir hak tesisi, korunması yahut kullanılmasına ilişkin olarak o iş ile sınırlı bir şekilde kişisel verilerin işlenmesi hukuka uygunluk sebebi olarak kabul edilmelidir. Ancak belirtilmelidir ki söz konusu verilerin ölçülü olması ve işlem için zorunlu olması şartlarının sağlanması gerekmektedir.

3.2.4.8. Veri Sorumlusunun Üstün Meşru Menfaati

İlgili kişinin temel hak ve özgürlüklerine zarar vermemek koşulu ile veri sorumlusunun meşru menfaatleri doğrultusunda kişisel verileri işleminin hukuka uygunluk sebebi olarak kabul edilip edilemeyeceği hususu öğretice çokça tartışılmıştır. Söz konusu tartışmalar Kişisel Verilerin Korunması Kanunu'nun tasarı sürecinde gündeme gelmiştir. Öyle ki, Türkiye Cumhuriyeti Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü tarafından 18 Ocak 2016 tarihinde esas ve tali komisyona havale edilen, Bakanlar Kurulunca 04 Ocak 2016 tarihinde kararlaştırılan Kişisel Verilerin Korunması Kanunu Tasarısı metninde meşru menfaat hukuka uygunluk sebebi yer almasına rağmen Alt Komisyon tarafından kabul edilen metinde çıkarılmıştır. Daha sonrasında ise 12 Şubat 2016 tarihli Türkiye Büyük Millet Meclisi Adalet Komisyonu raporunda söz konusu hukuka uygunluk sebebinin maddeye eklenerek kabul edildiği belirtilmektedir⁸³. Kanun gerekçesinde işverenin çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, terfi, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işleminin meşru menfaat hukuka uygunluk sebebi altında

⁸² “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 9.

⁸³ “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 62.

değerlendirilebileceği belirtilmektedir. Ayrıca kişisel verilerin korunmasına ilişkin temel ilkelere uyulması ve veri sorumlusu ile ilgili kişinin menfaat dengesinin gözetilmesi gerektiği belirtilmiştir. Alt Komisyon ise “meşru menfaat” kavramının çok geniş bir istisnaya neden olması ve veri sorumlusunun meşru menfaati kavramının sınırlarının ve kapsamının neler olduğunun uygulamada ciddi sorun ve endişelere neden olabilmesi ihtimaline istinaden metin çıkarılarak kabul edilmesini teklif etmiştir⁸⁴. Adalet Komisyonu ise tekrar önünde gelen tasarıda somut olay bazında veri sorumlusunun meşru bir menfaatinin değerlendirilmesi gerektiği ve işlemenin bu meşru menfaat için zorunlu olması ve veri sorumlusunun gözetilen menfaatinin ilgili kişinin temel hak ve özgürlüklerine zarar vermemesi gerekliliklerinin hüküm kapsamında şart koşulmasının belirsizlik yaratmadığı gerekçesi ile ilgili hukuka uygunluk sebebini ekleyerek maddeyi kabul etmiştir⁸⁵. İlgili raporda yer alan muhalefet şerhinde ise meşru menfaat kavramının soyut ve sübjektif olması sebebi ile hukuka uygunluk nedenleri arasında yer alması, kişisel verileri kayıt almayı esas, korumayı ise istisna haline getirmesi yönünden eleştirilmiştir⁸⁶.

⁸⁴ a.e., s.24.

⁸⁵ a.e., s. 67.

⁸⁶ a.e., s. 84.

DÖRDÜNCÜ BÖLÜM

BÜYÜK VERİ UYGULAMALARI BAKIMINDAN KİŞİSEL VERİLERİN KORUNMASI

4.1. Genel Olarak

Bu çalışma kapsamında önceki bölümlerinde detaylıca açıklanmış olduğu üzere Avrupa Birliği ve onun bir yansıması olarak Türk hukukunda, kişisel verilerin işlenmesi kapsamında verisi işlenen gerçek kişinin menfaati üstün tutularak kişisel verilerin korunması bir kişilik hakkı olarak ele alınmaktadır. Her ne kadar verinin günümüzde bir ekonomik değer haline geldiği ve iktisadi değerinin engellenmemesi gerektiğine ilişkin bir görüş¹ olsa da açıklanan hukuki metinlerde de görüleceği üzere çatışan menfaatler arasındaki denge bireyler lehine kurulmuştur. Öyle ki bir reform ihtiyacı ile 5 senelik bir çalışma ürünü olarak 2018 yılının mayıs ayında uygulanmaya başlamış olan Avrupa Birliği Genel Veri Koruma Tüzüğü'nde, veri sorumlusunun arttırılmış yükümlülükleri ve genel ilkelere getirilen düzenlemeler, teknoloji karşısında bireylerin korunmasının daha önemli olduğunu işaret etmektedir. Bu başlık altında büyük veri uygulamalarının yarattığı iktisadi menfaat ve örnekleri açıklanarak birey merkezli Avrupa Birliği ve Türk veri koruma hukuku perspektifinden büyük veri uygulamalarının uygunluk sorunu ele alınacaktır.

4.1.1. Büyük Veri Uygulamaları ve İktisadi Menfaat

Büyük veri, terebayte'lar ve petabayte'lar² ile ölçülen, günlük kullanılan bilgisayar ve programlar ile analiz edilemeyecek kadar büyük ve hacimli, karmaşık veri setlerinden oluşmaktadır³. Büyük veri çok farklı kaynaklardan beslenerek, farklı veri grup ve kategorilerini bir araya getirerek sosyal medya paylaşımları, ziyaret bilgileri, davranış izlemeleri, kamera kayıtları, ağ günlükleri, fotoğraf ve videolar, telekomünikasyon

¹ Abu Bakar Munir, Siti Hajar Mohd Yasin, Firdaus Muhammad-Sukki, "Big Data: Big Challenges to Privacy and Data Protection", **World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering**, Cilt 9, Sayı 1, 2015, s. 361.

² Terebayt: 1 TB = 1099511531398.98 bayt = 1048575.91 megabayt = 1024 gigabayt; Petabayt: 1 PB = 1024 terebayt.

³ Necmi Gürsakar, **Büyük Veri**, 3. Baskı, Bursa, Dora Yayınları, 2017, s.9

operatörlerinden elde edilen arama kayıt bilgileri, yer ve konum bilgileri gibi çeşitli veri gruplarını anlamlı ya da anlamsız olarak barındırmaktadır. Örnek olarak bir internet sitesinde alışveriş yapıldığında kişiye atanan kod yahut sipariş numarası üzerinden alışverişin yapıldığı bilgisi anlamlı bir bilgi iken, kişinin alışveriş yapmasa bile site üzerinde gezinmesi, sayfada vakit geçirdiği alanlar, site kullanımları sırasında imleç hareketleri, ziyaret ısı haritaları, sayfa ziyareti öncesi gezindiği sayfalar gibi veriler daha sonra başka veri grupları ile birleştirilerek anlamlı sonuçlar elde etmek üzere büyük veri havuzuna aktarılmaktadır. Günümüzde veri saklamak ve işlemek için harcanan maliyetlerin düşmesi ise büyük veri ve büyük veri uygulamalarının kullanımını daha cazip hale getirmektedir.

Büyük veriyi besleyen kaynaklardan bazılarını, sosyal medya uygulamaları, sensör ağları, dijital görüntüler, videolar, cep telefonları, alışveriş kayıtları, kredi kartı işlemleri, tıbbi kayıtlar, arşivler, elektronik ticaret ve bilimsel araştırmalar, istatistiksel çalışmalar olarak örneklendirebilmek mümkündür. Bu veriler ilgili kişinin bizzat kendisinden onayı ile alınabileceği gibi, ilgili kişinin kullanımına bağlı olarak da elde edilebilmektedir. Örneğin, kişinin sosyal medya kullanımı sırasında bir içerik paylaşması, bir alışveriş yapması, internet üzerinden arama motoru aracılığı ile bir sorgu yapması, dijital asistanlar vasıtası ile ses kaydı ya da sesli sorgu yapması gibi örneklerde kişi temel olarak verilerini paylaştığının farkındadır. Bunun yanı sıra, sensörler, üçüncü taraf çerez uygulamaları, CCTV kameraları ile toplanan veriler kişinin fark edemeyeceği veri toplama yöntemleri olarak düşünülmelidir⁴. Ücretsiz olan uygulamalar içerisinde kullanıcılara gösterilen reklamlara kullanıcıların ilgi oranları, ilgili reklamı ziyaret edip etmediği, kaç saniye izlediği gibi veriler söz konusu uygulamalar açısından ekonomik bir değer ihtiva etmektedir. Tüm bu bilgilerin, yaklaşık 5 katrilyon veribayt boyutunda olduğu ifade edilmektedir⁵. Bilim insanları ise toplanan verinin 18 ayda bir ikiye katlanması istatistiğinden yararlanarak 2020 yılına

⁴ Supriyadi, “Personal and Non-Personal Data in the Context of Big Data”, s. 20.

⁵ Sadullah Çelik, “Büyük Veri Teknolojilerinin İşletmeler İçin Önemi”, **Social Sciences Studies Journal**, Cilt 3, Sayı 6, 2017, s. 873.

gelindiğinde, veri hacminin büyüklüğünün yaklaşık 40 zettabayt⁶ olacağını tahmin etmektedirler⁷.

Hızla büyüyen veri ve bu büyük veriyi işleyebilme teknolojisinin gelişmesi veri ekonomisini yaratmaktadır. Büyük veri ekonomisine ilişkin yapılan istatistik çalışmalarında yaratılan ekonominin hızla büyüdüğü ortaya konulmaktadır. 2017 yılında 23 milyar dolar geliri olan büyük veri pazarının 10 yıl içerisinde 100 milyar dolara ulaşması beklenmektedir⁸.

Geleneksel veri işleme yöntemlerinde göz ardı edilen ve biriken verilerin, yapay zeka ya da algoritmalar tarafından işlenmesi ile iş akışlarına değer katan sonuçlar elde edilebilmektedir. Büyük hacimli ve çeşitli olan, belirli bir kurala tabi olmaksızın toplanmış verilerin işlenmesi, anlamlı hale getirilmesi büyük veri uygulamaları ile gerçekleştirilebilmektedir. Büyük veri uygulamaları, geleneksel raporlamadan farklı olarak geçmiş “neden” ve “nasıl” soruları ile analiz edip modellemeler ve deneyime dayalı tasarımlar oluşturmak, güncel verilere bakarak mevcut durum içerisindeki en iyi seçeneği tespit etmek ve geleceğe yönelik olarak bir beklentiden çok daha fazlasını, en iyi ve en kötü senaryoları öngörü ile hesaplamak için kullanılmaktadır⁹. Büyük veri uygulamaları ile tasarruf, ekonomik yönlendirmeler ve karlılık yönetimi yapılabilmektedir. Şirketler ise ekonomik değeri yadsınamayacak olan büyük veri ve büyük veri uygulamalarından yararlanarak rekabet avantajı elde etmektedirler.

Büyük veri uygulamaları, fiyat politikalarını yönetmek ya da pazarlamada isabetli tahminler yapmak için kullanılabilmektedir. Elektronik ticaret ve perakende alanında büyük markalardan olan Wal-Mart, fiyat maliyet analizini büyük veri uygulamaları

⁶ Bir zettabyte, 1.180.591.620.717.410.000.000 bayt veya bilgi birimi demektir. Tek bir baytın, bir metin karakterine eşit olduğu düşünüldüğünde, 1,250 sayfalık Leo Tolstoy'un Savaş ve Barış'ı, 323 trilyon kez bir zettabyte'ye sığabilecektir. “2016: The Year of the Zettabyte,” Daily Infographic, 23 Mart 2013, (Çevrimiçi) <http://dailyinfographic.com/2016-the-year-of-the-zettabyte-infographic>, 18 Nisan 2018.

⁷ Vadim E. Kotov, “Big Data, Big Systems, Big Challenges: A Personal Experience”, **Perspectives of Systems Informatics**, ed. Andresi Voronkov, Irina Virbitskaite, Springer, Verlag Berlin Heidelberg, 2015, s. 42.

⁸ Big data market size revenue forecast worldwide from 2011 to 2027, (Çevrimiçi) <https://www.statista.com/statistics/254266/global-big-data-market-forecast/>, 14 Nisan 2018.

⁹ Thomas Davenport, Robert Morison, Jeanne Harris, **Analytics at Work: Smarter Decisions, Better Results**, Harvard Business Review Press, Şubat 2010, figure 1-1.

vasıtası ile yöneterek paydaşlarının kararlarına etki edebilmiş ve karlılığını arttırmıştır¹⁰. Amazon, Netflix, Target, LinkedIn gibi firmalar ise müşterilerinin alışveriş alışkanlıklarını analiz ederek yeni ürünler önermek için büyük veri uygulamalarından yararlanmaktadırlar. Amazon, satışlarının yaklaşık üçte birinin, Netflix ise kullanıcı seçimlerinin yaklaşık dörtte üçünün bu tavsiyeler sonucunda gerçekleştiği ifade etmiştir¹¹. Daha ziyade kişilerin, profesyonellik alanlarına göre ön plana çıktığı bir sosyal medya platformu olan LinkedIn ise “tanıyor olabileceğiniz kişiler” butonu için kullanmış olduğu büyük veri uygulaması ile yüzde 30’luk bir başarı yakalamıştır¹².

Büyük veri uygulamaları aracılığı ile sağlanan yararlar, sektörden sektöre değişiklik gösterebilmekle beraber uygulamaların genel olarak pazar gelişimi, operasyonel çalışmalar, talep öngörüler, karar alma ve müşteri bağlılığını sağlama noktasında şirket süreçlerine büyük katkı sağlayacağı düşünülmektedir¹³.

4.1.2. Büyük Veri Uygulamalarında Yer Alan Algoritmalar

Büyük veri uygulamalarının çalışma prensiplerini anlayabilmek için kısaca yürütülen algoritmalarla ilişkin açıklamalara yer vermek yerinde olacaktır. Basit bir ifade ile algoritma, verilere uygulanabilecek kurala bağlı bir dizi adım ve talimatı ifade etmektedir. Algoritmalar, veriyi filtrelemek, veri üzerinde çalışmak, davranışları ve ilişkileri aramak ya da genel olarak bilgi analizine yardımcı olmak için kategoriler oluşturmaktadır.

Büyük veri uygulamaları tarafından kullanılan veri setlerinin daha önceden kullanılan geleneksel veri setlerinden en önemli farkı veri toplama aşamasındaki davranışları

¹⁰ Fatima-Zahra Benjelloun, Ayoub Ait Lahcen, Samir Belfkih, “An overview of big data opportunities, applications and tools”, **Intelligent Systems and Computer Vision**, sunulmuş bildiri, IEEE, Mart 2015, s. 2-3.

¹¹ Eric Siegel, **Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die**, Jeopardy Productions, Canada, 2013.

¹² Şirketler tarafından kullanılan büyük veri uygulamaları ve sonuçlarına ilişkin daha detaylı bilgi için bkz. Bernard Marr, **Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results**, Wiley, Birleşik Krallık, 2016.

¹³ Şemsettin Çiğdem, Ibrahim H. Seyrek, “İşletmelerde Büyük Veri Uygulamaları: Bir Literatür Taraması”, **2. Ulusal Yönetim Bilişim Sistemleri Kongresi**, Erzurum, Kasım 2015, s. 9.

olarak ifade edilebilir. Geleneksel yöntemde kullanılan veri toplama metodu ilişkisel veri tabanı sistemine dayanmakta, bir başka deyişle henüz tasarım aşamasında hangi veri ya da veri gruplarının toplanacağını belirli olduğu veri tabanları kullanılmaktadır. Bu veri tabanlarında verilerin numerik ya da alfabetik olup olmayacağı da önceden belirlenmektedir¹⁴. İlişkisel veri tabanlarında kullanılmak üzere tasarlanmış tablolarda, ilgili kişi hakkında toplanması gereken bilgiler, örneğin; ad, soyad, yaş, e-posta, telefon, satın alınan ürünler olarak sınırlandırılır ve başkaca bir verinin giriş yapacağı alan olmadığı için, örneğin; ilgilendiği diğer ürünler, mağazada geçirdiği zaman gibi bilgilerin göz ardı edilmesi söz konusu olabilmektedir. Ancak büyük verinin odağında ise önceden belirlenmiş herhangi bir veri kategorisi yer almamaktadır. Her ne kadar bir veri tabanı için oluşturulacak sistemin başlangıçta bir amacı olsa da bu durum toplanacak veri kapasitesine ve çeşitliliğine ilişkin herhangi bir sınırlama getirmemektedir¹⁵. Bu doğrultuda belirlenen alanlar haricinde, kişinin başka marka tercihleri, medeni durumu, mesleği gibi doğrudan ya da dolaylı başka veriler de o an için ihtiyaç olmasa dahi tutulmaktadır. Büyük veri uygulamalarının bir diğer özelliği ise ilgili kişilerin doğrudan bilgisine sahip olmasa bile o bilgiye ulaşmak ya da bir kanaat oluşturmak için dolaylı bilgileri de kullanabilmesidir. Örneğin; mesleği bilinmeyen bir kişinin mesai saatleri içerisinde sürekli olarak avukatlar için düzenlenmiş bir platformu kullanıyor olması verisinden yola çıkarak bu kişi avukat olarak tahminlenebilecektir.

Bir algoritma tarafından atılan adımlar, tasarımcısının bilgisi, deneyimleri, güdüsü, önyargıları ve talepleri ile şekillendirilmektedir. Ancak yapay zekâ ile birlikte hayatımıza dâhil olan öğrenebilir algoritmalar, pek çok kaynaktan beslenerek veri setleri üzerinde çalışmakta ve her bir değere tasarımcısının öngörüsünden farklı bir ağırlık verebilmektedir. Yüksek teknoloji gerektiren bu algoritmalar otomatik karar mekanizmalarında kullanılarak profil oluşturmaya yönelik davranış çözümlemeleri, hedeflemeye yönelik davranış tahminleri veyahut bir puan oluşturarak ilgili kişiye yönelik olumlu ya da olumsuz sonuç elde etmek amaçlı olarak kullanılabilir.

¹⁴ Dale Neef, **Digital Exhaust: What Everyone Should Know About Big Data, Digitization and Digitally Driven Innovation**, PH Professional Business, Kasım 2014, s. 158.

¹⁵ Cenk Derinözlü, “Büyük Veri ve Mahremiyet Big Data and Privacy”, **TUBİTAK 1.Ulusal Bulut Bilişim ve Büyük Veri Sempozyumu B3S17 Sempozyumu Bildiri Kitabı**, 2017.

Bu algoritmaların en önemli yanı bilimsel bir nesnellik taşıdıkları için insana özgü önyargıları maskeleyebilme olanağına sahip olmalarıdır¹⁶. Ancak akıllı algoritmaların dahi insana özgü önyargıları öğrenmemelerinin bir garantisi bulunmamaktadır¹⁷.

4.1.3. Büyük Veri Uygulama Örnekleri

Telekomünikasyon, perakende, sigorta, finans ve bankacılık alanlarında faaliyet gösteren şirketler, rekabet avantajını koruyabilmek adına diğer iş analitiği çözümlerinde olduğu gibi, büyük veri alanında da yenilikleri hızla takip ederek, büyük veri uygulamalarını süreçlerine en hızlı entegre eden konumda bulunmaktadır.

İnternet 2.0 olarak anılan Wikipedia, Google, Facebook, YouTube, Blogger gibi sosyal paylaşım siteleri tarafından, bu platformlar üzerinden paylaşım yapan, içerik oluşturan yahut sadece sayfalar arasında gezinen kullanıcıların sağlamış olduğu verilerin, kullanıcı profillemeye, reklam gösterme gibi faaliyetler için işlenmesi büyük veri uygulamalarına örnek olarak gösterilebilmektedir. Twitter tarafından kullanıcı tweetlerini üç boyutlu bir harita üzerinde gösteren ve en çok hangi şehirden tweet atıldığını belirtmek amacı ile bir büyük veri projesi geliştirilmiştir¹⁸. AIDSVU Projesi¹⁹ ile Amerika Birleşik Devletleri eyaletlerinde HIV²⁰ taşıyan kişilerin yoğunlukta olduğu bölgeler bir harita üzerinde işaretlenmiştir. Uygulama dâhilinde söz konusu verilerin Amerika Birleşik Devletleri Sağlık Kontrol Merkezi'nden alındığı belirtilmiştir²¹. Yandex tarafından sunulan Yandex.Traffic projesi ile şehir içi

¹⁶ Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values", **The White House**, Washington, Mayıs 2014, s. 46.

¹⁷ 2016 yılının mart ayında, Microsoft tarafından bir chatbotu olarak geliştirilen Tay isimli yapay zeka, açık kaynaklardan ve kullanıcılar ile olan sohbetlerinden öğrenmek üzere tasarlanmıştır. Ancak twitter üzerinden açılan TayandYou hesabı kullanıcı beslemeleri ile 24 saatten kısa sürede ırkçı, cinsiyetçi ve küfürbaz bir bota dönüşmüştür. "Tay,Microsoft's AI chatbot, gets a crash course in racism from Twitter", **The Guardian** 24 Mart 2016, (Çevrimiçi) <https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter>, 18 Nisan 2018.

¹⁸ Söz konusu uygulamaya ilişkin detaylı bilgi için bkz. Uygulamanın resmi sayfası, (Çevrimiçi) https://blog.twitter.com/official/en_us/a/2013/the-topography-of-tweets.html, 4 Nisan 2018.

¹⁹ Proje adını Acquired Immune Deficiency Syndrome (AİDS), HIV etkeni nedeniyle insanlarda bağışıklık sisteminin çökmesine neden olan bulaşıcı bir hastalık türünden almıştır.

²⁰ Human Immunodeficiency Virus (HIV), sadece insanda hastalık yapan ve kişinin bağışıklık sistemini etkileyen bir virüstür.

²¹ Uygulamanın internet sitesi için bkz. (Çevrimiçi) <http://aidsvu.org/map/> 4 Nisan 2018.

çeşitli kaynaklardan ve kullanıcı cihazlarından toplanan verilere göre yol ve trafik durumunu gösteren haritalar ve kullanıcılara alternatif yol sunan yol tarifi uygulamaları üretilmiştir²². Anadolu Jet, uçuş rotalarının belirlenmesine ve maliyet fayda analizi yaparak bazı rotaların iptal edilmesine ilişkin hazırlamış olduğu proje kapsamında, Turkcell müşterilerinin verilerinden yola çıkarak, Turkcell'in sahip olduğu büyük veri kullanımı ile müşterilerin hareketliliklerini çıkartmış ve buna bağlı olarak rotalardan ne kadar verim alabileceği, hangi rotaların eklenmesi veya hangi rotaların çıkarılması gerektiği konusunda çıkarımlar yapılmıştır²³. Facebook tarafından tanıtılan DeepFace yazılımı ile bir kişiye ait iki farklı fotoğraf %97.35 başarı oranıyla eşleştirilebilmektedir²⁴. Yazılım başarısında en büyük etken ise hiç kuşkusuz kişilerin kendilerine ait yüklemiş olduğu fotoğrafların çok fazla olmasıdır.

Perakende sektöründe 2012 yılında yaşanmış bir örnek ise oldukça dikkat çekici olmuştur. Target isimli bir market müşterilerinin alışveriş alışkanlıklarını ve değişimlerini izleyerek çeşitli pazarlama stratejileri geliştirmektedir. Her bir müşteri için, müşteri adına, kredi kartına ya da e-posta adresine ilişkilendirerek misafir numarası atayan Target, bu numaralarla müşterilerinin alışverişlerini, doğrudan müşterilerinden aldıkları ya da başka kaynaklardan edindikleri demografik verileri eşleştirerek pazarlama faaliyetlerini yürütmektedir. Bunlardan biri ise belirli haftalardaki alışverişlerinden ve davranışlarından yola çıkarak, hamile olarak profillenen kadınlara yönelik olarak geliştirdikleri pazarlama stratejileridir. 2012 yılında, Target algoritması tarafından hamile olarak hedeflenerek, bebek kıyafetleri ve arabalarında kullanılmak üzere indirim kuponu alan kişinin babası, henüz kızının lise öğrencisi olduğunu belirterek, kızına gönderilen reklamların amacının kızını yönlendirmek olduğu iddiasıyla market yönetimini suçlamıştır. Market müdürü ile

²² Uygulamanın internet sitesini görmek için bkz. (Çevrimiçi) <https://yandex.com.tr/harita/?l=trf%2Ctrfe>, 4 Nisan 2018.

²³ Söz konusu projenin tanıtımı ve detali bilgi için bkz. "AnadoluJet uçuşlarını Turkcell ile planlayarak kaynaklarından maksimum verim sağlıyor", (Çevrimiçi) <https://www.turkcell.com.tr/kurumsal/isletmeler/basari-hikayeleri/anadolujet>, 4 Nisan 2018.

²⁴ Uygulamaya ilişkin daha fazla bilgi için bkz. (Çevrimiçi) <https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/>; işleyiş ve prensibi için bkz. Yaniv Taigman v.d., "DeepFace: Closing the Gap to Human-Level Performance in Face Verification", 2014, (Çevrimiçi) https://www.cs.toronto.edu/~ranzato/publications/taigman_cvpr14.pdf, 8 Nisan 2018.

baba arasında geçen görüşmede market müdürü bir yanlış anlaşılma olabileceğini ifade ederek özür dilediyse de gerçek birkaç hafta sonra ortaya çıkmıştır. Market müdürünü arayan baba, kızı ile görüştüğünü ve kızının hamile olduğunu öğrendiğini ifade ederek özür dilemiştir²⁵. Görülmektedir ki, büyük veri uygulamaları ile yürütülen kişisel veri işleme faaliyetleri başarılı olmakla birlikte bireyler tarafından rahatsız edici noktalara ulaşabilmektedir.

Büyük veri uygulamaları, sadece şirketler tarafından değil akademi tarafından da kullanılmaktadır. Örneğin, Stanford Üniversitesi'nde yürütülen bir yüksek lisans çalışmasında araştırmacı, internet siteleri, bloglar ve microbloglarda paylaşılan yazıları, çeşitli kongre ve konferanslarda yapılan konuşmaları, basın bültenlerini ve makaleleri otomatik olarak bilgisayarda analiz ederek, siyasi düşüncelerin nasıl yayıldığına ilişkin anlamlı sonuçlar elde etmeye çalışmıştır²⁶.

Telekomünikasyon ve internet sektöründe ise büyük veri uygulamalarına başta pazarlama amaçlı olmak üzere sıklıkla yer verilmektedir. Phorm, Front Porch ve NebuAd gibi hizmet sağlayıcı kuruluşlar, derin veri analizi²⁷ yöntemini kullanarak bilgisayarlara ve tarayıcılara yerleştirilen çerezler aracılığıyla, kullanıcılarının çevrimiçi hareketlerini kaydedip izleyebilmekte ve bunun sonucunda da davranışsal profiller oluşturabilmektedirler. Derin veri analizi yöntemi ile bütün trafik izlenebilmektedir. İzlenen ve profillenen kullanıcı ise daha sonrasında hedefleme yoluyla yapılan reklamcılık hizmetleri ile karşılaşmaktadır. Dolayısıyla büyük veri

²⁵ Kashmir Hill, "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did", **Forbes**, 16 Şubat 2012, (Çevrimiçi) <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teengirl-was-pregnant-before-her-father-did/> 16 Nisan 2018.

²⁶ Gürsakal, **a.g.e.**, s. 9.

²⁷ İngilizcesi **Deep Packet Inspection** olan Derin veri analizi yöntemi, internet üzerinden gönderilen verilerin içeriğinin okunması anlamında kullanılmaktadır. İletilen mesajlar karşısında tarafsız bir iletişim ortamı olarak tasarlanan internet veri ve mesaj iletimi için başlangıçta sadece adres bölümü internet hizmet sağlayıcıları tarafından okunmakta idi. Ancak güvenliğin sağlanması iddiası ile başlayan denetimler günümüzde ticari amaçlı olarak özel hayatın gizliliğini tehlikeye atma pahasına yürütülmektedir. Derin veri analizi yöntemine ve veri koruma hukuku bakımından etkisine ilişkin bkz. Robert Todd Graham Collins, "The Privacy Implications of Deep Packet Inspection Technology: Why the Next Wave in Online Advertising Shouldn't Rock the Self-Regulatory Boat" **Georgia Law Review**, Cilt 44, Sayı 2 2010, s. 558; Melih Kırıldoğan, Işık Barış Fidaner, Derin Veri Analizi: İnternetteki Temel Gözetim Aracı, XIV. Akademik Bilişim Konferansı, Uşak, 1-3 Şubat 2012, s. 967.

uygulamaları pazarlama ve reklamcılık sektörüne etki ederek geleneksel reklamcılık anlayışını değiştirmektedir.

Arama motoru üzerinden verilen reklamlarda da yine büyük veri uygulamaları kullanılmaktadır. Arama motoru sektöründe neredeyse tekel konumunda olan Google, Adwords ve Adsense isimli iki reklam platformu işletmektedir. 2000 yılından bu yana hizmet veren Adwords²⁸ isimli platform ile reklam verenlerin belirledikleri anahtar kelimeler vasıtasıyla reklamlarının gösterilerek ziyaretçi çekmeleri sağlanmaktadır. Google Adsense²⁹ hizmeti ise tüm internet sitesi yayıncılarının internet sitelerinde hedeflenmiş Google reklamlarını göstererek para kazanmalarını sağlayan ücretsiz ve kolay bir yöntem olarak tanımlanmaktadır. Her iki platform da hedefleme faaliyetlerini gerçekleştirirken büyük veri uygulamaları yürüten algoritmalar kullanmaktadır³⁰.

Telekomünikasyon şirketlerinin elde etmiş olduğu verilerin büyük veri uygulamaları ile bir araya getirilerek kullanılmasını sağlayan ve sadece bu işe özgülenmiş şirketler kurulmuştur. İspanya merkezli Telefónica, programatik reklamcılık firması Mobclix'i satın alarak Axonix'i³¹ bu amaçla kurmuştur. Telefónica 2015 yılında Birleşik Krallık'daki iştiraki O2 ile iş birliği yaptığı projede, O2 abonelerinin cihaz verilerini kullanarak Londra metrosunda yer alan reklam panolarında hedefli reklam servislerini kullanıma almıştır³².

Ülkemizde ise 2016 yılında Türk Telekom tarafından dijital reklam alanlarını otomatik olarak satın alma ve yönetme imkânı sağlayan pazarlama ürünü olan Programatik

²⁸ Platformun işleyişine ilişkin Google tarafından oluşturulmuş yardım sayfası için bkz. “Google AdWords Hakkında”, (Çevrimiçi) https://support.google.com/adwords/answer/6349091?visit_id=1-636591218437515651-1722933147&hl=tr&rd=1 , 8 Nisan 2018.

²⁹ Platformun işleyişine ilişkin Google Tarafından oluşturulmuş yardım sayfası için bkz. “Adsense Nasıl Çalışır”, (Çevrimiçi) <https://support.google.com/adsense/answer/6242051?hl=tr>, 8 Nisan 2018.

³⁰ Marcela Mattiuzzo, “Business Models and Big Data: How Google Uses Your Personal Information”, (Çevrimiçi) <https://itsrio.org/wp-content/uploads/2017/03/Marcela-Mattiuzzo-V-REVISADO.pdf>, 8 Nisan 2018.

³¹ Telefónica grup şirketleri bünyesinde yer alan Axonix, mobil reklamcılık sektöründe hedef kitle segmentleme hizmeti vermektedir. Telekomünikasyon verilerini konum ve diğer veriler ile eşleştirerek reklam verenler için nitelikli hedef kitleler oluşturmaktadır. İnternet sitesi için bkz. (Çevrimiçi) <http://axonix.com/> , 8 Nisan 2018.

³² İlgili haber metni için bkz. “Telefónica partners with advertising firm in UK big data Project”, 08 Haziran 2015, (Çevrimiçi) <https://www.eurocomms.com/industry-news/10746-telefonica-partners-with-advertising-firm-in-uk-big-data-project>, 8 Nisan 2018.

isimli servis, telekomünikasyon sektöründeki büyük veri uygulamalarına örnek olarak gösterilebilmektedir³³. Türk Telekom'un büyük veri uygulamaları kapsamında ilk girişimi ise 2012 yılında kişisel verilerin korunması kapsamında tepki çeken Phorm ve TTNET arasındaki iş birliği neticesinde şekillenen "Gezinti" hizmetidir. Hizmet kapsamında kullanıcıların internette ziyaret ettikleri sayfalardan yola çıkarak, genel ilgi alanlarının tespit edilmesi ve bu doğrultuda içerik ve reklam sunulması öngörülmüştür³⁴.

Büyük verilerinin yaygın olarak kullanıldığı bir diğer sektör ise bankacılık ve finans sektörüdür. Bankacılık ve finans sektörü piyasa verilerinin yanı sıra kullanıcılarının ya da müstakbel kullanıcılarının verileri ile de uzun bir süredir ilgilenmektedir. Kredi kartı harcamalarından herhangi bir kredi talebine kadar insanların yaptığı bütün bankacılık işlemleri analiz edilmektedir. Finans kurum ve kuruluşları, Bankalar, piyasadaki riski ve gelecek eğrisini öngörebilmek için büyük veri uygulamalarından faydalanmaktadır. Bununla birlikte finans sektörü sadece kendi sistemleri sırasında üretilen bankacılık hizmetlerinin kullanımına ilişkin verileri değil, Twitter, Facebook paylaşımları, Google sorguları vb. kaynaklardan elde ettikleri verileri de kullanarak piyasadaki diğer değişkenlerle ilişkilendirerek analiz çalışmalarını yürütmektedirler. Twitter haber akışı içerikleri ya da Twitter'dan elde edilen veriler ile hisse senedi piyasası arasındaki hareketlenme arasında bir ilişki olup olmadığı araştırılmıştır³⁵. İstatistikler uygulamalar dışında dolandırıcılığın önlenmesi ve doğru kredilendirme için bankalar büyük veri uygulamalarından yararlanmaktadır. Kredi başvurusu olan kişi hakkında açık kaynaklardan, sosyal medyadan veri toplayan kredi kuruluşları,

³³ Türk Telekom tarafından hizmetin duyurulduğu bültene ulaşmak için bkz. "Programattik" ile dijital reklamcılık alanında yeni bir dönem başlıyor!" 8 Nisan 2016, (Çevrimiçi) <https://www.turktelekom.com.tr/hakkimizda/medya-merkezi/basin-bultenleri/sayfalar/programattik-digital-reklamcilik.aspx>, 8 Nisan 2018.

³⁴ Keser Berber, **Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması**, s. 110.

³⁵ Venkata Sasank Pagolu v.d., "Sentiment Analysis of Twitter Data for Predicting Stock Market Movements", **International conference on Signal Processing, Communication, Power and Embedded System**, 28 Ekim 2016, (Çevrimiçi) <https://arxiv.org/pdf/1610.09225.pdf>, 18 Nisan 2018; R. Chen and M. Lazer, "Sentiment Analysis of Twitter Feeds for the Prediction of Stock Market Movement", **Stanford University**, 2013, (Çevrimiçi) <http://cs229.stanford.edu/proj2011/ChenLazer-SentimentAnalysisOfTwitterFeedsForThePredictionOfStockMarketMovement.pdf>, 18 Nisan 2018.

kurumları üzerinde doğabilecek riski en düşük seviyeye indirerek doğru karar alma mekanizmalarını işletmeyi hedeflemektedirler.

Büyük veri uygulamaları sadece özel sektör ya da teknoloji alanında değil politikada da kullanılmaktadır³⁶. Amerika Birleşik Devletleri 2012 yılı başkanlık seçimlerinde Obama'nın büyük veri uygulamaları aracılığı ile pek çok seçmene ulaşabildiği ve farklı kaynaklardan beslenen çok fazla verinin analiz edilerek doğru kampanya programının oluşturulduğu belirtilmektedir³⁷. Daha yakın bir örnekte ise Amerika Birleşik Devletleri 2016 seçimlerinde Trump'ın anlaşılmış olduğu şirket Cambridge Analytica'nın, Facebook üzerinden almış olduğu bireylerin özel nitelikli verileri de dâhil olmak üzere kişisel verilerini kullanarak siyasi yönelimleri doğrultusunda bireylere özelleştirilmiş programlar oluşturarak seçimleri manipüle ettiği iddia edilmiştir³⁸.

4.2. Büyük Veri Uygulamaları Kapsamında Kişisel Verilerin İşlenmesi

Büyük veri uygulamaların pek çoğu insan hayatına doğrudan etki etmekte ve kolaylaştırmaktadır. Avrupa Komisyonu, Dijital Tek Pazar Strateji Raporunda bulut hizmetler ve nesnelerin interneti³⁹ teknolojileri ile birlikte büyük verinin rekabet için

³⁶ Büyük veri uygulamalarının politika alanında kullanımına ilişkin olarak bkz. Çekin, **a.g.m.**, s. 631.

³⁷ “How Obama Used Big Data to Rally Voters”, (Çevrimiçi) <https://www.technologyreview.com/s/508836/how-obama-used-big-data-to-rally-voters-part-1/>, 18 Nisan 2018.

³⁸ Yoan Hermstruwer, “Contracting around Privacy: The (Behavioral) Law and Economics of Consent and Big Data”, **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, Cilt 8, Sayı 1, 2017, s. 9-26; Bkz. “Cambridge Analytica used data from Facebook and Politico to help Trump”, **The Guardian**, (Çevrimiçi) <https://www.theguardian.com/technology/2017/oct/26/cambridge-analytica-used-data-from-facebook-and-politico-to-help-trump>, 4 Nisan 2018.

³⁹ İngilizcede Internet of things ya da kısaca **IoT** olarak ifade edilen kavramın karşılığı olarak nesnelerin interneti terimi kullanılmaktadır. Nesnelerin İnterneti birbiri ile etkileşim halinde olan ya da bağlı cihazlarla ilgili bir terimdir. Nesnelerin interneti teknolojisinde algılayıcısı/sensörü olan her çeşit nesnenin internete bağlanarak birbiri ile haberleşmesi söz konusudur, Armağan Ebru Bozkurt Yüksel, “Nesnelerin İnternetinin Hukuki Yönden İncelenmesi”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt 17, Sayı 2, 2015, s. 113; nesnelerin interneti terimi ilk defa 1999 yılında Kevin Ashton tarafından yapılan bir sunumda kullanılmıştır, bkz. Kevin Ashton “That Internet of Things Thing”, **RFID Journal**, 22.06.2009, (Çevrimiçi) <http://www.rfidjournal.com/articles/view?4986>, 16 Nisan 2018

olan öneminin altını çizmiştir⁴⁰. Büyük veri, bulut hizmetler ve nesnelerin interneti teknolojilerinin Avrupa Birliğinin rekabetçiliğinin merkezini teşkil ettiği ifade edilmiştir. Adı geçen Rapor'da büyük veri uygulamalarının yılda yüzde 40 büyümeye gösterdiği ve bu rakamın bilgi teknolojileri pazarındaki büyümeden yedi kat daha fazla olduğu belirtilmiştir⁴¹. Bununla beraber insan kararlarının etkilendiği, hatta manipüle edildiği büyük veri uygulamaları kötü niyetli kişiler tarafından da işletilebilmektedir. Yukarıda da bahsedildiği üzere büyük veri oluşumunda tek bir kaynaktan alınan verilerden yararlanılmamaktadır. Büyük veri, veri alabildiği her bir kaynaktan beslenmeye açık olacak şekilde tasarlanmaktadır. Bu nedenle büyük veri içerisinde kişisel verilerin de yer alması kaçınılmaz olmaktadır. Article 29 Working Party, konuya ilişkin endişesini 2014 yılında kamu ile paylaşmış olduğu bir raporunda büyük veri uygulamalarının yaratmış olduğu gerçek değer hala ispata muhtaç olduğunu belirtilerek dile getirmektedir⁴². Bununla birlikte özellikle büyük veri uygulamalarının yaratmış olduğu ekonomik değer göz önünde bulundurularak veri koruma düzenlemelerinin çok sıkı olması halinde veri ekonomisinin engellenebileceği ve beklenen faydanın sağlanamayacağı endişesini taşıyan yazarlar da mevcuttur⁴³.

Hızla gelişen teknolojiler karşısında bireylerin temel hak ve özgürlüklerinin korumasız bırakılmaması adına kişisel verilerin korunması alanında yapılan çalışmalar büyük önem taşımaktadır. Avrupa Veri Koruma Denetmeni Giovanni Buttarelli, 11 Mayıs 2015 tarihinde Brüksel'de yapmış olduğu konuşmasında⁴⁴ veri koruma ilkelerinin; büyük veri uygulamaları, robotlar, nesnelerin interneti, yapay zekâ gibi son teknolojilere uygulanması için yeni bir yol bulunması gerektiğini belirtmiştir. Bu

⁴⁰ Avrupa Komisyonu, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe", Brüksel, 6 Mayıs 2015, (Çevrimiçi) <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN>, 8 Ağustos 2018.

⁴¹ **a.e.**, s. 14.

⁴² Article 29 Working Party, "Statement on Statement of the WP 29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU", WP 221, 16 Eylül 2014, s. 2.

⁴³ Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data", **Seton Hall Law Review**, Cilt 47, Sayı 4, 2017, s. 1002.

⁴⁴ Giovanni Buttarelli, "Big data, big data protection: challenges and innovative solutions" **ERA Conference on Recent Developments in Data Protection Law**, Keynote speech, Brüksel, 11 Mayıs 2015, Bölüm 9.

noktada *Buttalli*, şeffaflık, kullanıcı kontrolü ve hesap verilebilirlik ilkelerinin teknolojik gelişmelerin merkezine yerleştirilmesini önermektedir.

Günümüzde teknolojinin gelişmesiyle birlikte şekillenen ve yeniden yapılandırılan pazarlama ve reklamcılık sektörü başta olmak üzere büyük veri uygulamaları, doğrudan kişileri profillemeye ve hedefleme amaçlı olarak kullanılmakta ve bu amaç doğrultusunda otomatik karar alma mekanizmalarından yararlanılmaktadır. Bu kapsamda kişi için büyük önem arz etmeyen herhangi bir veri dahi büyük veri uygulamaları kapsamında şirketler için büyük bir değer arz edebilmektedir. Başka bir deyişle, büyük veri teknolojilerinin kullanımı ile farklı kaynaklardan gelen ve tek başına herhangi bir özellik yahut önem taşımayan veriler sentezlenerek paylaşılmamış kişisel verilere erişilebilmektedir. Özellikle çevrimiçi alanlarda anonim olarak gezinme ihtimali büyük veri uygulamaları ile giderek azalmaktadır⁴⁵. Örneğin; kullanılan internet tarayıcısında herhangi bir kullanıcı profili yahut hesabı açılmış olmasa da kullanıcı alışkanlıklarından ve hareketlerinden yola çıkarak tarayıcılar kişiyi yaklaşık olarak belirleyebilmektedir. Bununla birlikte büyük veri uygulamaları kapsamında çoğunlukla anonimleştirilmiş verilerin kullanıldığı iddia edilse de belirlenebilirlik unsuru sağlandığı sürece anonim bir veriden söz etmek mümkün gözükmemektedir⁴⁶. Büyük veri uygulamaları ise pek çok kaynaktan pek çok veriyi birleştirerek anonim olduğu iddia edilen veriyi belirli bir kişi ile ilişkilendirebilmektedir.

Büyük veri uygulamaları bakımından sıklıkla başvurulanan otomatik karar alma ve profillemeye faaliyetleri ise kişisel veriler bakımından temel tartışma noktasını oluşturmaktadır. Büyük veri uygulamaları ile yapay zekâ ve akıllı sistemler vasıtası ile

⁴⁵ Anonim veri, belirli veya belirlenebilir bir gerçek kişi ile ilgisi olmayan veya ilgili kişinin belirlenmeyeceği veya belirlenemeyeceği şekilde bir forma dönüştürülmüş verilerdir. Ancak günümüzde anonim verilerin teknolojik gelişmelerle birlikte geri döndürülmesi mümkün olduğu için özellikle büyük veri uygulamaları bakımından anonim verilerden söz etmek güçleşmektedir, Supriyadi, “Personal and Non-Personal Data in the Context of Big Data”, s. 36.

⁴⁶ New York Times gazetecileri, Amerika Birleşik Devletleri’nde kurulu kitle medya kuruluşlarından biri olan AOL tarafından “anonim” olarak paylaşılan veriler üzerinde yürütmüş oldukları çalışma neticesinde, kullanıcılara atanan numara ve yapılan sorgular üzerinden yapmış oldukları çalışmalar ile kullanıcıların bazılarının kimliğini tespit ederek kamu ile paylaşmışlardır. Sorgu sahipleri ise tespitleri doğrulamıştır, bkz. Michael Barbaro, Tom Zeller, “A face is exposed for AOL searcher Nr. 441749”, *New York Times*, 09 Ağustos 2006; Çekin, *a.g.m.*, s. 636.

kişiler profilenebilmekte ya da temel hak ve özgürlüklerini etkileyebilecek otomatik karar alma mekanizmalarına konu olabilmektedirler. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 11. maddesinin (g) fıkrasında münhasıran otomatik sistemler vasıtasıyla kişisel verilerin analiz edilerek ilgili kişi aleyhine sonuç doğurması halinde ilgili kişinin itiraz hakkı olduğu düzenlenmişse de profillemeye ve otomatik karar mekanizmalarına ilişkin detaylı bir açıklama ve düzenleme bulunmamaktadır. Bununla birlikte Avrupa Birliği Genel Veri Koruma Tüzüğü'nde hem profillemeye hem de otomatik karar alma mekanizmaları özel olarak düzenlenmiştir.

4.2.1. Otomatik Karar Alma Mekanizmaları

Günümüzde ağırlıklı olarak kredi kuruluşları, sigorta şirketleri, işe alım süreçlerinde işverenler ve reklam verenler tarafından profillemeye faaliyetleri yürütülmekte ve oluşturulan profillerden faydalanan otomatik karar alma mekanizmaları oluşturulmaktadır. Kredi notu hesaplanmasına ilişkin olan sistemler otomatik karar mekanizmalarından oluşmaktadır. Çok fazla sayıda iş başvurusu alan global şirketler etik kurallar çerçevesinde tarafsız olarak değerlendirme yapabilmek için söz konusu profil bilgilerinden yararlanan karar alma mekanizmaları ile ön değerlendirme gerçekleştirmektedir. Pazarlama alanında ise reklam verenler bütçelerini yönetebilmek adına tüketiciler hakkında oluşturulan profillere dayanarak hedeflemeye dayalı reklam gösterme uygulamalarını tercih etmektedirler⁴⁷. Sağlık ve eğitim sektörlerinde de profillemeye dayanan veri işleme faaliyetlerine bilimsel araştırmaları yürütmek amacıyla başvurulmaktadır.

Otomatik karar alma mekanizmaları insan faktörü bakımından profillemeye tanımından farklılaşmaktadır. Otomatik karar alma mekanizmalarında bir algoritmanın insan müdahalesi olmaksızın üretmiş olduğu nihai bir sonuç elde edilmektedir. Örneğin toplanan verilerden yola çıkarak otomatik olarak kişiye atanacak herhangi bir puan, not bu kapsamda değerlendirilebilecektir. Otomatik karar mekanizmasının sonucunda bir profil elde edilip edilmemesi önem teşkil etmemektedir. Genellikle profillemeye faaliyetleri kapsamında otomatik karar mekanizmalarında yararlanılmakla birlikte; otomatik karar mekanizması haricinde de bir profillemeye faaliyeti söz konusu

⁴⁷ Tikkinen-Piri, Rohunen, Markkula, **a.g.m.**, s. 141.

olabilecektir⁴⁸. Örnek olarak; otoyollarda bulunan kameraların otomatik olarak belirli bir aracın ortalama hızını hesaplayarak bir trafik cezası oluşturması herhangi bir profillemeye içermeyen otomatik karar mekanizması olarak kabul edilebilecektir. Bununla birlikte ilgili kişinin sürüş alışkanlıklarının zaman içinde izlenmesi durumunda profillemeye dayanan bir karar elde edilebilecektir. Uygulanan cezanın miktarı, sürücünün hız ortalaması, cezaya konu ihlalin tekrarlanan bir ihlal olup olmadığı veya sürücünün son zamanlarda başka trafik ihlalleri olup olmadığı gibi diğer faktörleri içeren bir değerlendirme sonucunda profillemeye yapılabilecektir.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nde Yönerge ile benzer şekilde⁴⁹ bireylerin otomatik karar mekanizmalarına konu olmayı reddetme hakkı düzenlenmiş⁵⁰ ve bu hakka istisna teşkil edecek hukuka uygunluk sebepleri belirtilmiştir⁵¹. Tüzük ile getirilmiş olan otomatik karar mekanizmalarına ilişkin bu düzenlemenin dar yorumlanarak, sıkı bir şekilde uygulanmasının büyük veri uygulamalarını engelleyebileceğine ilişkin endişelere yer veren görüşler bulunmaktadır⁵².

4.2.2. Profillemeye

Teknolojinin gelişmesi ile birlikte şirketler, devletler ve işverenler, kişisel verilerini işlemekte oldukları ilgili kişilerin davranışlarını ve tercihlerini öngörülebilir kılmak adına büyük veri uygulamalarından yararlanmaktadırlar. Bu uygulamalar profillemeye ve otomatik karar alma mekanizmalarına dayanmaktadır. Avrupa Birliği Genel Veri Koruma Tüzüğü'nde profillemeye, *“kişisel verilerin, gerçek bir kişiye ilişkin belirli kişisel özelliklerini değerlendirmek için kullanılması amacı ile otomatik vasıtalarla herhangi bir süreçle işlenmesi”* olarak tanımlanmıştır (m. 4/4). Bu kavram Tüzük'te, belirli kişisel özelliklerin değerlendirilmesi, çalışma performansı, sağlık, kişisel tercihler, ilgi alanları, güvenilirlik, davranışlar, konum veya hareketlere ilişkin hususların analiz edilmesi veya tahmin edilmesi olarak örneklendirilerek

⁴⁸ a.e., s. 141.

⁴⁹ Yönerge'de de ilgili kişinin her zaman belirli durumlarda kendi durumuna göre veri işlemenin konusu olmayı reddetme hakkı tanımlanmıştır. Yönerge m. 14-15.

⁵⁰ Tüzük, m. 22.

⁵¹ Düzenlemenin profillemeye ile birlikte değerlendirmesi ve detaylı bilgi için bkz. aşağıda 144.

⁵² Zarsky, a.g.e., s. 1017.

açıklanmıştır. Gerçekten de teknolojiadaki ilerlemeler ve büyük veri uygulamaları, yapay zekâ ve makine öğrenim olanakları, bireylerin hak ve özgürlüklerini önemli ölçüde etkileme potansiyeline sahip profilleri oluşturmayı ve otomatik karar mekanizmalarının kullanımını kolaylaştırmakta ve yaygınlaştırmaktadırlar⁵³.

Teknolojinin gelişmesi ile yaygınlaşan bu faaliyetler, 1990'lı yıllarda hazırlanmış olan Avrupa Birliği Veri Koruma Yönergesi'nde detaylı bir şekilde düzenlenmemiştir. Yönerge'den yola çıkarak hazırlanmış olan Kişisel Verilerin Korunması Kanunu'nda da özel olarak profillemeye tanımı yer almamaktadır. Avrupa Birliği Genel Veri Koruma Tüzüğü'nde ise sadece otomatik karar alma mekanizmaları ve profillemeye ilişkin sonuçlar değil, ayrıca profillerin oluşturulması için kişisel verilerin toplanması ve bu profillerin bireylere uygulanmasına ilişkin düzenlemeler de yer almaktadır⁵⁴.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nde yer alan tanımdan yola çıkarak profillemenin, **(i)** otomatik bir işleme olması⁵⁵, **(ii)** kişisel veri barındırması ve **(iii)** amacının gerçek bir kişinin kişisel yönlerinin değerlendirilmesi olması gerekmektedir. Ancak belirtmek gerekir ki, yer alan profillemeye tanımı uyarınca profillemenin *tamamen* bir otomatik işlemeye dayanması gerekmemektedir. Otomatik işlemeye ek olarak insan faktörünün ekleneceği profillemeye faaliyetlerinin de bu kapsamda değerlendirilmesi gerekmektedir.

Profillemeye faaliyetleri bu doğrultuda genel profillemeler, otomatik karar mekanizmalarından yararlanılan profillemeler ve sadece otomatik karar mekanizmalarından oluşan profillemeler olarak üç başlık altında incelenebilecektir. Profillemeye faaliyetinin otomatik karar mekanizmasına dayanması halinde insan faktörü sonucun belirlenmesinde etkindir. Ancak sadece otomatik karar mekanizmalarından yola çıkarak yapılan profillemeye faaliyetlerinde algoritma insan etkisi olmaksızın kararı oluşturmaktadır. Avrupa Birliği Genel Veri Koruma Tüzüğü'nde giriş bölümünde 71. paragrafta çevrimiçi kredi başvurularının

⁵³ Article 29 Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", WP 251, Rehber, 3 Ekim 2017, s. 5.

⁵⁴ **a.e.**, s. 6.

⁵⁵ Otomatik veri işleme tanımı ve açıklamaları için bkz. yukarıda, "3.2.2.2. Kişisel Verinin İşlenmesi".

reddedilmesi ya da elektronik işe alım uygulamaları otomatik ve insan etkisi olmaksızın gerçekleştirilen veri işlemlere örnek olarak verilmektedir.

Profilleme altında yer alan otomatik veri işlemlerin insan etkisi içerip içermemesine ilişkin bu ayrım Avrupa Birliği Genel Veri Koruma Tüzüğü'nün çizmiş olduğu hukuki çerçeve bakımından önem arz etmektedir. Avrupa Birliği Genel Veri Koruma Tüzüğü madde 22'de, profillemeye de dâhil olmak üzere sadece otomatik karar mekanizmaları sonucunda kişinin kendisi hakkında elde edilen ve hukuki olarak⁵⁶ ya da ciddi şekilde kendisini etkileyen⁵⁷ sonuca itiraz hakkı düzenlenmektedir. Bu doğrultuda herhangi bir insan görüşünün, yorum ve etkisinin dâhil olabileceği bir sonuç, sadece otomatik karar mekanizması nihai sonucu olarak değerlendirilemeyecektir. Veri sorumluları ilgili kapsamın dışına çıkmak için otomatikleşmiş insan müdahaleleri ekleyerek ilgili kişinin itiraz hakkı karşısındaki sorumluluklarını bertaraf edemeyeceklerdir. Örnek olarak; bir algoritma tarafından elde edilen sonucun, insan eliyle, ancak işlevsel herhangi bir müdahale olmaksızın kabul edilmesi nihai kararın otomatik karar mekanizması ile elde edilmiş olduğu sonucunu değiştirmeyecektir⁵⁸. Bir etkiyi insan müdahalesi olarak değerlendirebilmek için müdahalenin kararı değiştirmek için yetkiye sahip biri tarafından işlevsel ve anlamlı bir etki ile yapılması gerekmektedir.

Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında, profillemeye özgü birtakım düzenlemeler çeşitli maddelerde de yer almaktadır. Örneğin; 13 ve 14. maddeler uyarınca profillemeye faaliyetleri yürüten veri sorumlularına, bu türden profillemeye faaliyetinin öngörülen sonuçlarının yanı sıra profillemeye ilişkin yürütülen işlemlerin çalışma mantığı hakkında bireylere *anlamlı bilgileri*⁵⁹ sunma yükümlülüğü getirilmiştir. Benzer şekilde, 15. madde kapsamında da veri sorumlusunun ilgili

⁵⁶ Madde hükmünde yer alan “hukuki etki” ile ilgili kişinin hukuki bir hakkının, örneğin dava açma hakkı, seçme hakkı, bir derneğe katılma hakkı gibi hakkının etkilenmesi ifade edilmektedir. **a.e.**, s. 10.

⁵⁷ Madde hükmünde yer alan “ciddi şekilde etkileme” ibaresi maddenin uygulama alanını daralttığı iddiası ile eleştirilmiştir. Article 29 Working Party, “Opinion 01/2012 on the data protection reform proposals” s. 14.

⁵⁸ Article 29 Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, s. 10.

⁵⁹ İngilizce orijinal metinde “*meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*” ifadesi yer almaktadır, Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 13/2 (f).

kişinin talebi üzerine “profil oluşturma dâhil olmak üzere otomatik karar alma sürecinin varlığını” açıklaması gerekmektedir⁶⁰.

Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında ayrıca profillemeye faaliyetlerinin bireyler için risk oluşturduğu ifade edilmiştir. Veri koruma etki analizi⁶¹ yükümlülüğünün düzenlendiği 35. madde kapsamında açık bir şekilde, gerçek kişilerle ilgili, kişisel özellikler hususunda profil çıkarma da dâhil olmak üzere otomatik işlemeye dayalı olan ve gerçek kişi ile ilgili hukuki sonuçlar doğuran veya gerçek kişiyi ciddi bir şekilde etkileyen kararların konu olduğu sistemlere ilişkin düzenleme getirilmektedir. Madde kapsamında söz konusu faaliyetlerin sistematik ve kapsamlı değerlendirmeleri içermesi halinde veri sorumlularına yürütülen profillemeye ve otomatik veri işleme kapsamında veri koruma etki analizi yapma yükümlülüğü yer almaktadır.

4.3. Büyük Veri Uygulamalarının Kişisel Verilerin Korunması Hukuku Bakımından Değerlendirilmesi

Kişisel verilerin korunması hukuku çerçevesinde otomatik ya da yarı otomatik yollarla kişisel veri işleme faaliyeti yürüten veri sorumlularının; genel ilkelere uyma, hukuka uygunluk sebepleri kapsamında veri işleme ve aydınlatma yükümlülüğünü yerine getirme olmak üzere temel yükümlülükleri bulunmaktadır⁶². Veri sorumluları tarafından yürütülen kişisel veri işleme faaliyetinin genel ilkelere uygun olması gerekmektedir birlikte; yürütülen faaliyetin hangi hukuka uygunluk sebebi altında değerlendirileceği özellikle aydınlatma yükümlülüğü kapsamında büyük önem taşımaktadır. Bu bakımdan ikinci ve üçüncü bölümde anlatılmış olan hukuka uygunluk

⁶⁰ İngilizce orijinal metinde “*at least in those cases, meaningful information about the logic involved*” ifadesi yer almaktadır, Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 15/1 (h).

⁶¹ Avrupa Birliği Genel Veri Koruma Tüzüğü’nde “Data Protection Impact assesment” olarak geçen bu uygulama kapsamında veri sorumlularına getirilen arttırılmış yükümlülüklerden biridir. Bir çeşit erken uyarı mekanizması olarak değerlendirilebilecek olan bu yükümlülük kapsamında kişisel verilerin işleme yöntemine dayalı olarak muhtemel tehlikelerin asgari seviyeye indirilmesi amaçlanmaktadır.

⁶² Belirtmek gerekir ki veri sorumlularının yükümlülükleri bunlardan ibaret değildir. Kişisel verilerin güvenliğini sağlama, sicile kayıt olma, bildirim, ilgili kişinin taleplerini yanıtlama ve aktarıma ilişkin yükümlülükleri gibi Avrupa Birliği ve Türk hukuku mevzuatlarında tanımlanmış yükümlülükleri de bulunmaktadır.

koşullarının büyük veri uygulamaları bakımından tespiti önem arz etmektedir. Herhangi bir kişisel veri işleme faaliyetinin hukuka uygunluk sebeplerinden biri altında değerlendirilebilmesi için öncelikle amaç unsurunun netleştirilmesi gerekmektedir. Sonrasında ise uygunluk denetimi kapsamında, işlenen verilerin ve yürütülen veri işleme faaliyetinin; kapsamı, gerekliliği, ölçülülüğü değerlendirilmektedir. Bir başka deyişle hukuka uygunluk sebeplerinin büyük veri uygulamaları bakımından uygulama alanına değinebilmek için yürütülen kişisel veri işleme faaliyetinin kapsam ve amacının tespit edilerek, yürütülen faaliyetin genel ilkelere uygunluğunun değerlendirilmesi gerekmektedir. Nitekim hukuka uygunluk sebeplerinin sınırlarının belirlenmesinde ve somut olarak uygulanması bakımından genel ilkeler yol gösterici bir nitelik taşımaktadır.

Büyük veri uygulamaları bakımından açık rıza, sözleşmenin kurulması ya da ifası, kişisel verilerin ilgili kişinin kendisi tarafından alenileştirilmiş olması yahut veri sorumlusunun üstün meşru menfaati hukuka uygunluk sebepleri uygulama alanı bulabilecektir. Sayılan hukuka uygunluk sebeplerinin varlığına kanaat getirebilmek için öncelikle yürütülen faaliyetlerin genel ilkelere uygunluğunun değerlendirilmesi gerekmektedir. Nitekim hukuka uygunluk sebebinin uygulama alanı genel ilkeler ışığında değerlendirilebilecektir. Avrupa Birliği Veri Koruma Yönergesi ile Kişisel Verilerin Korunması Kanunu'nda belirlenmiş olan hukuka uygunluk sebepleri ve genel ilkelere ilişkin isimlendirmeler tümüyle aynı değildir. Çalışmanın bu bölümde başlıklandırmalar Avrupa Birliği ve Türk hukuku olarak ayrılmayacak olup her bir ilke ve hukuka uygunluk sebebi Kişisel Verilerin Korunması Kanunu'ndaki isimlendirmeden yola çıkarak tek bir başlık altında karşılaştırmalı olarak değerlendirilecektir.

4.3.1. Büyük Veri Uygulamaları ve Genel İlkelere Uygunluğu

Gerek uluslararası metinlerde gerekse Avrupa Birliği veri koruma hukuku ve Türk veri koruma hukuku çerçevesinde çalışmanın önceki bölümlerinde belirtildiği üzere paralel genel ilkeler benimsenmektedir. Bu başlık altında büyük veri uygulamaları; kişisel verilerin korunmasına ilişkin genel ilkeler olan **(i)** hukuka ve dürüstlük kurallarına uygun olma, **(ii)** doğru ve gerektiğinde güncel olma, **(iii)** belirli, açık ve meşru amaçlar

için işleme, **(iv)** işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve **(v)** ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ölçütleri bakımından değerlendirilecektir. Büyük veri uygulamaları bakımından hukuka uygunluk sebeplerinin varlığına kanaat getirebilmek için öncelikle yürütülen faaliyetlerin genel ilkelere uygunluğunun değerlendirilmesi gerekmektedir.

4.3.1.1. Hukuka ve Dürüstlük Kuralına Uygun Olma

Hukuka ve dürüstlük kuralına uygun olma ilkesi bakımından aranan temel koşul uyarınca veri sorumlusunun veri işleme amaçları doğrultusunda ilgili kişiyi açık bir şekilde bilgilendirmesi, yanıltıcı ve aldatıcı bilgi vermemesi gerekmektedir. Bu çerçevede bu ilkenin uygulanabilirliğinin denetlenebilmesi için büyük veri uygulamalarında kullanılan kişisel verilerin elde ediliş anlarına bakılması lazım gelir. Büyük veriyi besleyen her bir veri kanalı, aktardığı yahut büyük veri uygulamasına dâhil ettiği her bir kişisel veri bakımından ilgili kişiyi bu uygulamaya ilişkin bilgilendirmiş olmalıdır. Bir başka deyişle, ilgili kişi kişisel verilerini paylaşırken, bu paylaşımın sonuçlarını öngörebilir olmalıdır. İlgili kişinin kişisel verilerini paylaşması yahut veri sorumlusunun ilgili kişiden kişisel verileri doğrudan ya da dolaylı olarak elde etmesi anında ilgili kişinin kişisel verilerinin nasıl ve ne amaçla kullanılacağını bilmiyor olması ya da yanlış yönlendirilmesi halinde dürüstlük kuralına uygunluktan bahsedilemeyecektir. Bu durum ise büyük verinin tabiatı gereği mümkün olan her kaynaktan beslenmesine ilişkin yaklaşım ile tezat oluşturmaktadır⁶³. Nitekim büyük veri uygulamaları bakımından veriler çoğunlukla ilgili kişinin doğrudan kendisinden değil başka kanallar aracılığı ile elde edilmektedir⁶⁴.

Büyük veri uygulamalarının mantığında farklı veri kaynakları ve kümeleri arasında bir bağlantı oluşturarak yeni sonuçlara varmak yer almaktadır. Bu uygulamalar kapsamında kullanılan algoritmalar dâhilinde işlenen, kişisel veri olduğu kesin

⁶³ Çekin, **a.g.m.**, s. 635.

⁶⁴ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ’inde, kişisel verilerin ilgili kişiden elde edilmemesi halinde; **(i)** kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde, **(ii)** kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında, ya da **(iii)** kişisel verilerin aktarılabilecek olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada ilgili kişiyi aydınlatma yükümlülüğünün yerine getirilmesi gerektiği belirtilmektedir.

olmayan verilerin birleştirilmesi ile birlikte kişisel veri niteliği arz eden sonuçlar üretilebilecektir. Bu durum ise ilgili kişi bakımından çoğu zaman beklenmeyen bir işleme faaliyetidir. Örneğin; sigorta şirketleri tarafından yürütülen prim hesaplamalarında, bireyin araba kullanım alışkanlıkları göz önünde bulundurulabilmektedir. Bireylerin araba kullanım alışkanlıklarının değerlendirilmesi için sürüş mesafesi, güzergahlar, araç kullanım hızı, ani fren kullanıp kullanmaması gibi davranışları incelenmektedir. Aynı zamanda bu veriler hava koşulları, yol durumu gibi kişisel olmayan verilerle eşleştirilerek, sürücüye araba kullanımına ilişkin bir profil atanmaktadır.

Dünyada çeşitli kurumlar tarafından yapılan araştırmalarda bireylere kişisel verilerine ve işleme amaçlarına ilişkin olarak beklentileri ve görüşleri sorulmuştur. Uluslararası İletişim Enstitüsü tarafından yaptırılan araştırmalarda⁶⁵, insanların kişisel verilerini paylaşma istekliliğinin ve bu verilerin nasıl kullanılacağına ilişkin tutumlarının bağlama göre değişiklik arz ettiği sonucuna ulaşılmıştır. Örneğin; bireylerin kişisel verilerini paylaşmalarına ilişkin tutumlarında verilerini talep eden kurum ve kuruluşlara ne kadar güvendiği ve kurumlar tarafından hangi bilgilerin talep edildiği önemli bir etken olarak belirtilmektedir. Avustralya, Brezilya, Kanada, Çin, Fransa, Almanya, Hindistan, İtalya, Japonya, İspanya, Birleşik Krallık ve Amerika Birleşik Devletleri'nin dâhil olduğu 20 ülkede yapılan araştırmada⁶⁶ ise tüketicilerin %75'i için kişisel verilerinin gizliliği önemli bir konu olmakla beraber; 18-24 yaş arası bireylerin kişisel verilerine ilişkin olarak yeterince temkinli olmadığı tespit edilmiştir. Benzer ülkeler arasında yapılan daha güncel tarihli bir araştırmada ise bireylerin kişisel verilerine ilişkin tutumlarının veri türleri, veri kullanımı ve tüketici konumu gibi faktörlere bağlı olarak değiştiği, araştırmaya katılan kişilerin yaklaşık olarak %56'sının, şirketlerin kişisel verilerini nasıl kullandıklarıyla ilgili “endişe” veya “aşırı derecede endişe duyduğu” belirtilmektedir⁶⁷. Avrupa genelinde ise Avrupalıların

⁶⁵ International Institute of Communications, “Personal Data Management: the User’s Perspective”, Londra, Eylül 2012.

⁶⁶ John Rose, Christine Barton, Rob Souza, James Platt, “The Trust Advantage: How to Win with Big Data”, **The Boston Consulting Group**, Kasım 2013.

⁶⁷ KPMG, “Crossing the Line: Staying on the Right Side of Consumer Privacy”, **KPMG**, s. 29, Ocak, 2017, (Çevrimiçi) <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/crossingthe-line.pdf>, 08 Nisan 2018.

sadece %22'si arama motoru, sosyal medya ya da e-posta hizmeti sağlayıcısı şirketlere güvenirken; bu internet kullanıcılarının %72'si çevrimiçi olarak çok fazla kişisel verisi talep edilmesinden endişe duymaktadır⁶⁸.

Türkiye'de yapılan araştırmalarda ise internet siteleri ve sosyal paylaşım ağlarında kendini daha özgür hissedenlerin oranı %54 olarak yer almaktadır. Mahremiyet ihlalleri yaşanmasına rağmen internet ve sosyal medya kullanımını sürdürmeye devam edeceğini ifade eden kullanıcıların oranı %28 olarak ifade edilmektedir. Araştırmaya katılanların %51'i ise mahremiyetinden hiçbir koşulda taviz vermeyeceğini belirtmiştir. İlgili araştırmada bireylerin çevrimiçi gizlilik ve güvenlik ihlalleri karşısında farkındalık boyutunun yüksek olduğu; ancak internet kullanımlarının ihlallerden etkilenme oranının düşük olduğu ifade edilmiştir⁶⁹.

Bu doğrultuda kullanıcıların, büyük veri uygulamaları dâhilinde karmaşık algoritmaların üreteceği sonucu öngörebilmesini beklemek dürüstlük kuralına aykırı olarak değerlendirilebilecektir. Büyük veri uygulamalarının bu özelliği nedeniyle algoritmalar aracılığıyla yürütülecek kişisel veri işleme faaliyetleri dürüstlük kuralı açısından, Kişisel Verilerin Korunması Kanunu'nda sayılan açık rıza dışındaki diğer hukuka uygunluk sebepleri ile büyük oranda örtüşmemektedir. Ancak kişinin kendisine özel hedefleme yapılması üzerine bir programa kayıt olmak için sözleşme yapması ve bu pazarlama faaliyetini bir hizmet olarak alması durumunda sözleşmenin ifası hukuka uygunluk sebebi olarak değerlendirilebilecektir⁷⁰. Bu halde de yine büyük veri uygulama algoritmalarının ilgili kişiyle yapılan sözleşme ile sınırlı olarak işletilmesi halinde dürüstlük kuralının şartları sağlanmış olacaktır. Sözleşmenin kurulması yahut ifası hukuka uygunluk sebebine dayanarak kişisel verilerin işleniyor

⁶⁸ Avrupa Komisyonu, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe", Brüksel, 06 Mayıs 2015, s. 13.

⁶⁹ Malik Aslanyürek, "İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve Farkındalıkları", **Maltepe Üniversitesi İletişim Fakültesi Dergisi**, Sayı 3, 2016, s. 82-83.

⁷⁰ Sözleşmenin ifası hukuka uygunluk sebebine ilişkin detaylı açıklamalar açısından bkz. aşağıda "3.3.2.2. Sözleşmenin Kurulması veya İfası".

olabilmesi için en önemli ölçüt veri sorumlusu tarafından sunulan aydınlatma metninin açık, bilgilendirmeye dayalı ve mümkün olduğunca şeffaf olmasıdır⁷¹.

Hukuka ve dürüstlük kuralına uygunluk bakımından değerlendirilmesi gereken bir diğer husus ise büyük veri uygulamaları doğrultusunda yürütülen faaliyetlerin etki alanıdır. Karmaşık bir algoritma üzerinden sentezlenen pek çok veri ile elde edilen sonucun bireye etkisi önem teşkil etmektedir. Örneğin; sadece araştırma, kümülatif yönelimlerin ve kamusal hareketlerin herhangi bir bireye indirgenmeksizin tespit edilmesi amacıyla yürütülecek büyük veri uygulamalarının hukuka ve dürüstlük kuralına uygunluğu, doğrudan bireyler özelinde sonuç doğuran uygulamalara nazaran daha farklı değerlendirilebilecektir. Bireyin menfaatinin zarar görmemesi halinde bu uygulama veri sorumlusunun meşru menfaati kapsamında ele alınabilecektir⁷². Yine ham halde verilerin anonimleştirilerek istatistiki amaçla kullanılması bu kapsamda kabul edilebilecektir.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nde ayrıca *şeffaflık ilkesi* yer almaktadır⁷³. Şeffaflık ilkesi uyarınca veri sorumlusunun mümkün olduğunca anlaşılır ve açık bir şekilde kişisel verilerin işlenmesine ve amaçlarına ilişkin bilgileri ilgili kullanıcı ile paylaşması gerekmektedir. Bu durum özellikle büyük veri uygulamaları bakımından veri toplama anında işleme amacının henüz net olarak belirlenememiş olması sorun teşkil etmektedir. Ancak bu halde dahi ilgili kişilerin bilgilendirilmemiş olarak bırakılmaması gerekmektedir. Bu kapsamda kişisel verilerin daha sonraki olası amaçlar ile işlenebileceğine ilişkin bilgilendirmenin yanı sıra işlemenin şekli hakkında da ilgili kişiler bilgilendirilmiş olmalıdır⁷⁴. Bir başka deyişle, bilgilendirme yükümlülüğünün yerine getirilmesi amacı ile kullanılan gizlilik bildirimlerinin;

⁷¹ Information Commissioner Office, “Big Data and Data Protection”, 28 Temmuz 2014, s. 27-28, (Çevrimiçi) <https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220>, 18 Nisan 2018.

⁷² Çekin, **a.g.m.**, s. 636.

⁷³ Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 5/1.a “Lawful, fair and transparent”.

⁷⁴ Gloria González Fuster, Amandine Scherrer, “Big Data and Smart Devices and Their Impact on Privacy”, Directorate General For Internal Policies Policy Department C: Citizens' Rights And Constitutional Affairs Civil Liberties, **Justice and Home Affairs**, Brüksel, 2015, s. 30, (Çevrimiçi) [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU\(2015\)536455_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf) f 14 Nisan 2018.

otomatik karar mekanizmaları ve profillemeye de dâhil olmak üzere kişisel veri işleme faaliyetlerini açık ve basit bir şekilde anlatan, kapsamlı ve anlamlı bir metin olarak hazırlanmış olması gerekmektedir.

Büyük veri uygulamalarıyla yürütülen profillemeye faaliyetleri kapsamında kişisel verileri işlenen kişilere, veri sorumlusunun asgari ölçüde aşağıdaki hususları içerir şekilde bir bilgilendirme sunuyor olması gerekmektedir:

- i. Uygulama kapsamında yürütülen bir profillemeye faaliyeti olduğu,
- ii. Profillemeye faaliyetinin amaçları,
- iii. Profillemeye faaliyetinin sonuçları,
- iv. Profillemeye faaliyetinin altında yatan mantık (diğer bir deyişle kullanılan algoritma),
- v. İlgili saklama süreleri,
- vi. İnsan tarafından yeniden değerlendirilebilen otomatik bir karar mekanizmasının kullanıldığı.

Veri sorumlularının, aydınlatma metinlerini oluşturma ve ilgili kişilere etkili olarak sunma aşamasında da teknolojinin gelişiminden yararlanması gerektiği ifade edilmektedir. Bu doğrultuda Avustralya veri koruma otoritesi, veri sorumluları tarafından ilgili kişilerin bilgilendirilmesi adına daha teknolojik imkânlarla başvurularak dinamik, çok katmanlı ve kullanıcı merkezli gizlilik politikalarının oluşturulabileceğini belirtmiştir⁷⁵.

Teknolojik gelişmeler ışığında kanun koyucuların artan şeffaflık beklentisine tezat bir şekilde veri sorumluları, büyük veri uygulamalarının çalışma prensiplerine ilişkin açıklama yapmaktan ve ilgili kişilerin başvurularını yanıtlamaktan “ticari sır” iddiası ile kaçınmaya çalışmaktadır⁷⁶. Ticari sır kavramına ilişkin olarak açık bir tanım

⁷⁵ Office of the Australian Information Commissioner, “Consultation Draft: Guide to Big Data and The Australian Privacy Principles”, Mayıs 2016, s.13, (Çevrimiçi) <https://www.oaic.gov.au/engage-with-us/consultations/guide-to-bigdata-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacyprinciples>, 18 Nisan 2018.

⁷⁶ Örneğin, Facebook kullanıcısının kişisel verilerine erişim talebi facebook tarafından ticari sırların korunması gerekçesi ile geri çevrilmesi, Avrupa Veri Koruma Denetmeni olan Peter Hustinx tarafından örnek olarak verilmiştir, bkz. Avrupa Veri Koruma Denetmeni, “Opinion of the European Data Protection Supervisor, on the proposal for a directive of the European Parliament and of the Council on

mevzuatta yer almamaktadır. Ancak Bilgi Edinme Hakkı Kanunu’nun 23. maddesinde yer alan “Ticari Sır” başlıklı maddede “*Kanunlarda ticari sır olarak nitelenen bilgi veya belgeler ile, kurum ve kuruluşlar tarafından gerçek veya tüzel kişilerden gizli kalması kaydıyla sağlanan ticari ve mali bilgiler bu Kanun kapsamı dışındadır.*” hükmü yer almaktadır. Ticari Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısı⁷⁷ uyarınca ticari sır; “*Bir ticarî işletme veya şirketin faaliyet alanı ile ilgili yalnızca belirli sayıdaki mensupları ve diğer görevlileri tarafından bilinen, elde edilebilen, özellikle rakipleri tarafından öğrenilmesi halinde zarar görme ihtimali bulunan ve üçüncü kişilere ve kamuya açıklanmaması gereken, işletme ve şirketin ekonomik hayattaki başarı ve verimliliği için büyük önemi bulunan; iç kuruluş yapısı ve organizasyonu, malî, iktisadî, kredi ve nakit durumu, araştırma ve geliştirme çalışmaları, faaliyet stratejisi, hammadde kaynakları, imalatının teknik özellikleri, fiyatlandırma politikaları, pazarlama taktikleri ve masrafları, pazar payları, toptancı ve perakendeci müşteri potansiyeli ve ağırları, izne tâbi veya tâbi olmayan sözleşme bağlantılarına ilişkin veya bu gibi bilgi ve belgeleri*” ifade etmektedir.

Yargıtay kararlarında⁷⁸ “*ticari sır kavramının en önemli unsurunun toplumun bilgisi dâhilinde olmama veya ilgili alanda rakip firmalarca bilinmeme şartının olduğu*” ifadesi yer almaktadır. Belirtmek gerekir ki ticari sır kavramının en önemli özelliği, bilginin bir işletmeye ekonomik bir menfaat sağlamasıdır. Bu bakımdan iş ve işletme sırları, teknik sırlar ticari sır kapsamında değerlendirilmektedir⁷⁹. Bunun yanında

the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure” , 12 Mart 2014, (Çevrimiçi), https://edps.europa.eu/sites/edp/files/publication/14-03-12_trade_secrets_en.pdf, 8 Nisan 2018; Gianclaudio Malgieri, “Trade Secrets v Personal Data: a possible solution for balancing rights”, **International Data Privacy Law**, Cilt 6, Sayı 2, 2016, s.103.

⁷⁷ 21 Ekim 2011 tarihli ve 3336 sayılı Başbakanlık yazısı ile Türkiye Büyük Millet Meclisine iletilmiş olan “Ticari Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısı” henüz yasalaşmamıştır.

⁷⁸ Yargıtay 11. Hukuk Dairesi, Esas sayısı: 2004/7827, Karar sayısı: 2007/5755, Karar tarihi: 2 Haziran 2005.

⁷⁹ “*Bir gerçek veya tüzel kişi tacire, işletmeye, işletme faaliyetine, organizasyonuna, imalata veya ticarete dair sırlar genellikle ve en geniş anlamda ticari sır, ya da iş ve işletme sırrı kavramları ile ifade edilmektedir. Örneğin TK, m. 57/b. 7., 8. hükümlerinde yol gösterici şekilde, bir gerçek kişi veya tüzel kişi tacirin sahip olduğu ticaret ve imalat sırrından söz edilmektedir. Burada korunan sırrın kapsamına iş ve işletme sırları, teknik sır, imalat sırları, sınai ve ticari sırlarının tamamı girmektedir.*” bkz. Arslan Kaya, “4982 Sayılı Kanun Kapsamında Bilgi Edinme Hakkının Sınırlarından Olan 'Ticari Sır' ile Fikir

bilginin henüz kamuya açıklanmamış olması ve gizli kalmasına yönelik sahibinin iradesinin bulunması, ticari sır oluşturan bilgide bulunması gereken diğer unsurlardır. Ticari sır, ticari işletmelerin ve şirketlerin rekabet etmelerinde, piyasadaki güçlerini belirlemekde önemli bir etken olarak kabul edilmektedir⁸⁰. Bu açıdan ticari sırların saklanması ve korunması işletmeler ile şirketler açısından büyük önem taşımaktadır. Özellikle teknoloji şirketleri bakımından, kişisel verilerin işlenmesine ilişkin olarak algoritmalarının çalışma prensibi ve bir veriden nasıl yararlandıklarına ilişkin açıklamalar diğer paydaşlara karşı rekabet üstünlüğü yarattığı gerekçesi ile ticari sır olarak kabul edilebilecektir⁸¹. Ancak bu sorun veri koruma hukuku bakımından göz ardı edilmiş değildir. Avrupa Birliği Veri Koruma Yönergesi'nin giriş bölümü 41. paragrafta, otomatik karar mekanizmalarına ilişkin getirilmiş olan “ilgili kişinin mekanizmanın çalışma mantığına ilişkin bilgi alma hakkı” sınırlandırılmaktadır. İlgili kişinin sahip olduğu bu hakkın ticari sırları veya fikri mülkiyeti, özellikle yazılımı koruyan telif hakkını⁸² olumsuz yönde etkileyemeyeceği belirtilmektedir.

Belirtmek gerekir ki söz konusu sınırlandırmalar veri sorumlusuna ilgili kişinin talebini tamamen reddetme imkânı tanımamaktadır. Nitekim ilgili kişinin talebinin yerine getirilmesi halinde ticari sırlarının ifşa olacağını ispat yükü veri sorumlusuna yüklenmiştir. Büyük veri uygulamaları bakımından bir algoritmanın altında yatan mantığın açıklanması konusunda ticari işletme ve şirketler ile ilgili kişilerin menfaatlerinin arasında kolay çözülemeyecek bir menfaat çatışması olduğunun kabulü gerekmektedir. Ancak her halükârda gerek veri sorumlusunun aydınlatma yükümlülüğü kapsamında gerekse ilgili kişinin bilgi talepleri doğrultusunda veri sorumlularının, ilgili kişilerin menfaatlerini korumaya yönelik olarak makul bilgileri sağlamalarının önem arzettiğinin kabulü gerekecektir. Bilhassa veri sorumlusu

ve Sanat Eserleri”, **Bilgi Edinme Hakkı**, Türkiye Barolar Birliği Yayınlar no: 62, Ankara, Türkiye Barolar Birliği, Haziran 2004, s. 135.

⁸⁰ Neslihan Karataş Durmuş, “Ticari Sırların ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti”, **Türkiye Adalet Akademisi Dergisi**, Yıl 8, Sayı 31, Temmuz 2017, s. 383.

⁸¹ Gianclaudio Malgieri, “Trade Secrets v Personal Data: a possible solution for balancing rights”, **International Data Privacy Law**, Cilt 6, Sayı 2, 2016, s.103.

⁸² Bilgisayar programlarının fikri mülkiyet hukuku çerçevesinde korunmasına ilişkin detaylı bilgi için bkz. Mustafa Aksu, **Bilgisayar Programlarının Fikri Mülkiyet Hukukunda Korunması**, İstanbul, Beta Basım Yayım Dağıtım A.Ş., 2006, özellikle s. 107 vd.

tarafından yürütülen veri işleme faaliyetinin ilgili kişinin rızasına dayanıyor olması veya bir sözleşmenin kurulması ya da ifası kapsamında gerçekleştiriliyor olması halinde bu dengenin ilgili kişi lehine yorumlanması ilgili hukuka uygunluk sebebinin ispatı bakımından da önem taşımaktadır.

Kişisel Verilerin Korunması Kanunu kapsamında bu duruma ilişkin müstakil bir düzenlemeye yer verilmemiştir. Ancak özellikle şirketler bakımından, şirketlerin de gizlilik alanının bulunması gerektiği kabulüyle ticari ve sınai sırda ilişkin yukarıda açıklanan hususlar, her somut olayda göz önünde bulundurularak ilgili kişinin talebinin sınırlandırılması bakımından uygulama alanı bulabilecektir⁸³.

4.3.1.2. Doğru ve Gerektiğinde Güncel Olma İlkesi

Doğru ve gerektiğinde güncel olma ilkesi temel olarak büyük veri uygulamalarının sağlayıcıları tarafından da hedeflenen verimli sonuçlara ulaşma gayesine hizmet eden bir ilkedir⁸⁴. Ancak büyük veri uygulamaları kapsamında; çok fazla kaynaktan çok fazla veri toplanıp eşleştirileceği için bunlar arasında doğru olmayan ya da güncel olmayan veriler de yer alabilecektir. Bununla birlikte farklı kaynaklardan toplanan veriler birleştirilirken kişiye ait olmayan bilgilerin de toplanması suretiyle, kişiye ilişkin hatalı bir sonuca varılması mümkündür. Günümüzde büyük veri uygulayıcıları, yapay sinir ağları ile karmaşık algoritmaları çalıştırmakta ve veri kaynaklarını artırarak bu hata oranını düşürmeye çalışmaktadırlar. Ancak yine de büyük veri uygulamalarının çalışma prensipleri gereğince tamamen güvenilir, doğru ve gerçeğe uygun bir büyük veri yakalamak mümkün gözükmemektedir⁸⁵.

Otomatik karar mekanizmaları aracılığı ile yürütülen profillemeye faaliyetleri bakımından kişisel verilerin gerçeğe uygun ve güncel olması önem taşımaktadır. Özellikle bir sözleşmenin kurulması ya da ifası kapsamında kişi hakkında bir sonuca

⁸³ Avrupa Veri Koruma Denetmeni, “Opinion of the European Data Protection Supervisor, on the proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure”, s. 6.

⁸⁴ Küzeci, **a.g.e.**, s. 225.

⁸⁵ Giovanni Buttarelli, “Big Data, Big Data Protection: Challenges and Innovative Solutions” **ERA Conference on Recent Developments in Data Protection Law**, Keynote speech, Brüksel, 11 Mayıs 2015, Bölüm 9.

varmak amacı ile yürütülen otomatik karar mekanizmalarında kullanılan verilerin güncel ve gerçeğe uygun olmasını sağlamak veri sorumlusunun bir yükümlülüğüdür⁸⁶.

Avrupa Birliği üye devletleri mevzuatı açısından doğru ve gerektiğinde güncel olma ilkesi farklı yorumlanmıştır. Örnek olarak İsviçre⁸⁷ ve Almanya⁸⁸ veri koruma yasasında yalnızca “doğruluk” ifadesi kullanılmıştır. OECD Rehber İlkeleri’nde ise doğruluk ve güncelliğin yanı sıra verinin “bütün olması” da bir ilke olarak sayılmıştır. Kişisel Verilerin Koruması Kanunu’nda ise “*doğru ve gerektiğinde güncel*” ifadesi tercih edilmiştir. Bu ilkenin bağdaşması gereken bir diğer veri sorumlusu yükümlülüğü ise şüphesiz ilgili kişiye, kişisel verileri üzerinde kontrol sağlama imkânı sunulmasıdır. İlgili kişinin kişisel verilerine ulaşamaması halinde verilerin doğru ve güncel olup olmadığının tespit edilmesi pek mümkün görünmemektedir⁸⁹. Bu doğrultuda ilgili kişiye sağlanan bilgilerin yanı sıra bireylere kendilerine ilişkin kişisel verileri doğrulama, tamamlama imkânının sunuluyor olması önem teşkil etmektedir.

Kişisel verilerin güncelliğinin ve doğruluğunun kontrolü için geliştirilecek olan mekanizmalar ölçülülük ilkesine aykırı olmamalıdır. Başka bir deyişle, kişilere kişisel verilerinin doğrulanması ve tamamlanması imkânı sunulurken bu mekanizmalar gereğinden fazla kişisel veri toplamak için kullanılmamalıdır. Örnek olarak; bir kişinin teslimat adresi bilgisi bir elektronik ticaret sitesinin veri tabanında ilgili kişinin bir siparişini ulaştırma amacı ile daha önceden yer almış olabilir. Veri sorumlusu olan elektronik ticaret sitesinin, ilgili kişi başka bir sipariş kaydı oluşturmadığı sürece bu veriyi güncelleme ihtiyacının olmadığı kabul edilmesi gerekecektir⁹⁰. Diğer bir ifade ile söz konusu ilke, veri sorumlusunun sürekli olarak ilgili kişinin güncel durumunu araştırması olarak değerlendirilmemelidir. Nitekim ilkede yer alan “gerektiğinde” ifadesi bu duruma vurgu yapmaktadır.

⁸⁶ IT Governance Privacy Team, **EU General Data Protection Regulation: An Implementation and Compliance Guide**, IT Governance Publishing, United Kingdom, 2016, Bölüm. 3.

⁸⁷ Küzeci, **a.g.e.**, s. 225.

⁸⁸ Thomas Hoeren, “Big Data and Data Quality”, **International Journal of Law and Information Technology**, Oxford University Press, Sayı 25, 1 Mart 2017, s. 26–37.

⁸⁹ Küzeci, **a.g.e.**, s. 226.

⁹⁰ IT Governance Privacy Team, **a.g.e.**, Bölüm 3.

Doğru ve gerektiğinde güncel olma ilkesinin bir başka yansıması ile arşiv verilerinin zaman damgalı olarak tutuluyor olması halinde verinin güncel olması gerekliliği bertaraf edilebilecektir⁹¹. Nitekim tarihle beraber belirli bir durumu gösteren verinin doğruluk içerdiği sürece güncel olup olmaması önem taşımayacaktır. Ancak bu durumun, verilerin saklandığı yöntem ve veri tabanı bakımından anlaşılıyor olması gerekmektedir.

Büyük veri uygulamaları kapsamında özellikle otomatik karar mekanizmaları aracılığı ile kişilere atanacak profiller bakımından verilerin doğru olması, gerektiğinde güncel olması, verinin güncel olmaması durumunda bu verinin ne zamana ilişkin olduğuna dair kaydın algoritma tarafından göz önünde bulunduruluyor olması gerekmektedir. Örneğin; bankalar tarafından kredi verilmesi ya da herhangi bir yarar sağlanması amacı ile kullanılacak kişisel verilerin güncel olması önem taşımaktadır. Article 29 Working Party tarafından ise işverenlerin, çalışanlarına ait kişisel verileri güncel tutmaları, en azından güncel tutabilmek için gerekli önlemleri almaları gerektiği belirtilerek özellikle çalışanlara ilişkin sonuçlar doğuran raporlama ve veri işleme faaliyetleri bakımından güncel ve gerçeğe uygun kişisel verilerin işlenmesi gerektiği örnek olarak verilmektedir⁹².

Bu gereklilik büyük veri uygulamalarının dayanmış olduğu hukuka uygunluk sebepleri bakımından değişkenlik arz etmemektedir. Ancak özellikle Türk hukuku bakımından kişinin kendi isteği ile alenileştirmiş olduğu veriler bakımından veri sorumlusu güncel verilere ulaşarak işleme faaliyetlerini bu doğrultuda gerçekleştirmelidir.

Bu doğrultuda büyük veri uygulamalarını işleten veri sorumlularının ilgili kişilerin bilgilerine ulaşabileceği ve onları denetleyebileceği, güncelleyebileceği bir sistem

⁹¹ Taranto, **a.g.e.**, s. 90.

⁹² Article 29 Working Party, “Opinion 8/2001 on the processing of personal data in the employment context”, s. 3.

oluşturmaları halinde, veri işleme faaliyetleri, kişisel verileri doğru ve gerektiğinde güncel olarak işleme ilkesi ile bağdaşacaktır⁹³.

4.3.1.3. Belirli, Açık ve Meşru Amaçlar İçin İşlenme İlkesi

Kişisel verilerin korunmasına ilişkin olarak hazırlanmış metinlerin hemen hepsinde amaçla bağlılık ilkesi esas alınmaktadır. Avrupa Birliği Veri Koruma Yönergesi'nde kişisel verilerin toplanma amacının belirli ve açık olması ilkesi yer almaktadır. Keza Kişisel Verilerin Korunması Kanunu kapsamında da belirli, açık ve meşru amaçlarla kişisel verilerin işlenmesi gerektiği belirtilmektedir. Kişisel verilerin işlenme amacına yönelmiş olan ilke, veri sorumlularına, kişisel verileri işlemeye başlamadan önce meşru amaçlarını belirleme, bu amaçlarını açık bir şekilde ilgili kişiye bildirme yükümlülüğü getirmektedir.

Belirtmek gerekir ki, büyük veri uygulamaları bakımından veri toplama anında belirtilen amaçtan farklı olarak kişisel veri işleme amaç ve ihtiyaçları doğabilmektedir⁹⁴. Bu noktada bir amaç değişikliği sorunu gündeme gelebilecektir. Avrupa Birliği Veri Koruma Yönergesi'nde yer alan ilkenin yorumu sırasında da verilerin daha sonraki işleme amaçlarının toplama amaçları ile uygun olması şartı vurgulanmaktadır⁹⁵. Avrupa Birliği Genel Veri Koruma Tüzüğü'ne ilişkin Rapor⁹⁶ yayımlayan Avrupa Komisyonu bu ilkenin büyük veri uygulamalarını engelleyecek şekilde yorumlanmaması gerektiğini belirtmiştir. Ancak kişisel verileri elde etme amacından sonraki her bir amaç bakımından, orijinal amaç ile uyumluluk değerlendirmesinin yapılması gerektiğini de vurgulamaktadır. Yayımlanan Rapor'da sürücüsüz otomobiller üzerinden verilen örnekte, en çok kazaların nerede gerçekleştiğini ve gelecekteki kazaların nasıl önlenebileceğini analiz etmek için ham verilerin kullanılabilmesi ifade edilmiştir. Gerek kişisel verilerin işlenmesine ilişkin alınan açık rızaya ilişkin metinlerde gerekse aydınlatma yükümlülüğünün yerine

⁹³ Peter Carey, **Data Protection, A Practical Guide to UK and EU Law**, Oxford University Press, 2. Baskı, Büyük Britanya, 2004, s. 57.

⁹⁴ Çekin, **a.g.e.**, s. 48.

⁹⁵ Küzeci, **a.g.e.**, s. 218.

⁹⁶ Avrupa Komisyonu, Fact Sheet, “**Questions and Answers - Data Protection Reform**”, 21 Aralık 2015, (Çevrimiçi), http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm, 8 Nisan 2018.

getirilmesi adına hazırlanan belgelerde kişisel verilerin işleme amacının belirli ve açık olması aranmaktadır. Dolayısıyla bu metinlerde kişisel veri işleme amacının mümkün olduğunca net olarak ifade edilmesi gerekmektedir. Uygulamada söz konusu metinlerde sıklıkla yer verilen, “daha iyi hizmet verebilmek için”, “reklam ve pazarlama amaçlı”, “güvenliğiniz için” gibi genel ve somut olmayan ifadeler yetersiz olarak nitelendirilebilecektir⁹⁷. Belirtmek gerekir ki, bir taraftan bilgilendirme aşamasında geniş ifadelerin kabul edilmemesi bir taraftan da sonradan ortaya çıkan amaçlara karşın sıkı yorum yapılması, özellikle büyük veri uygulamaları önünde önemli bir engel teşkil etmektedir. Uygulamada bu duruma ilişkin olarak yaşanan sıkıntıları göz önünde bulunduran Avrupa Komisyonu, Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında amaç değişikliğini özel bir düzenlemeye tabi tutmuştur⁹⁸. Tüzük’te, Avrupa Birliği Veri Koruma Yönergesi’nde olduğu gibi sonradan ortaya çıkan amaç için tekrardan hukuka uygunluk sebepleri uyarınca bir denetim yapılması gerektiğine işaret edilmekle birlikte, ilgili kişiden rızası alınabiliyor ise bu uygunluk denetimine gerek olmayacağı düzenlenmiştir. Ancak ilgili kişinin rızası alınamıyor ise sonradan ortaya çıkan amaçlar için uygunluk denetiminin veri sorumlusu tarafından yapılması gerekmektedir.

Büyük veri uygulamaları, çoğunlukla veri setleri arasında bağlantılar kurarak bir sonuç üretme eğilimi taşımaktadır. Bu bakımdan çoğu zaman başlangıçta belirtilen amaçtan sapmalar gündeme gelebilmektedir. Bu doğrultuda büyük veri uygulamalarının genel mekanizmaları uyarınca muhtemel olarak belirlenen amaçtan sapma riski göz önünde bulundurulmalıdır. Article 29 Working Party, sonradan ortaya çıkan amaca ilişkin değerlendirmeyi yaparken göz önünde bulundurulması gereken kriterleri şöyle belirtmektedir⁹⁹: **(i)** kişisel verilerin toplandığı amaçlar ile sonraki işleme faaliyetinin amaçları arasındaki ilişki; **(ii)** kişisel verilerin toplandığı bağlam ve ilgili kişinin sonraki veri işleme faaliyetlerine ilişkin makul beklentileri; **(iii)** kişisel verilerin niteliği ve kişisel veri işleme faaliyetinin ilgili kişiye etkisi; **(iv)** veri sorumlusunun

⁹⁷ Çekin, **a.g.e.**, s. 46-47; The Article 29 Working Party, “Opinion 03/2013 on purpose limitation”, WP 203, Görüş, 2 Nisan 2013, s. 16, 52.

⁹⁸ Tüzük’te yer alan amaç değişikliği düzenlemesine ilişkin detaylı bilgi için bkz. Çekin, **a.g.e.**, s. 49 vd.

⁹⁹ The Article 29 Working Party, **a.g.e.**, s. 23 vd.

hukuka ve dürüstlük kuralına uygun olarak kişisel veri işleme faaliyetini sağlamak ve ilgili kişilerin üzerindeki herhangi bir olumsuz etkiyi önlemek için benimsediği güvenceler¹⁰⁰. Nitekim bu kriterler Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında da yer almaktadır¹⁰¹.

Bu doğrultuda büyük veri uygulamaları bakımından şu hususları göz önünde bulundurarak bir değerlendirme yapmak gerekmektedir:

“Önceki amaç ile yeni amaç arasındaki her türlü bağlantı” ile yeni ortaya çıkan amacın, ilk belirtilen amacın bir devamı görünümünde olması halinde bağlantının kabulü gerekmektedir. Bu doğrultuda alışveriş verilerinden yola çıkan büyük veri uygulamalarının, genel olarak popüler tercihleri belirlemek ve iş süreçlerini geliştirmek için herhangi bir bireye doğrudan etki etmeksizin veri sorumlusu tarafından araştırma amaçlı olarak işletilmesi bağlantılı olarak kabul edilebilecektir. Ancak sonraki amacın bireye doğrudan pazarlama yapılması amacı ile bir izleme ve profillemeye yönelik olması halinde ilk amaçla kurulacak olan bağlantı zayıflayabilmektedir¹⁰².

“Kişisel verilerin toplanma koşulları” göz önünde bulundurularak, hukuka ve dürüstlük kuralına uygunluk başlığı altında incelenmiş olan ilgili kişinin veri sorumlusuna karşı haklı beklentisinin somut olay bazında değerlendirilmesi gerekmektedir. Sonradan ortaya çıkan amacın ilgili kişiler bakımından beklenebilir olup olmadığı, veri sorumlusu ve ilgili kişi arasındaki ilişkinin denkliliği önem arz etmektedir¹⁰³.

“Kişisel verinin niteliği” bakımından yeni ortaya çıkan amaç bakımından söz konusu kişisel verinin, özel nitelikli kişisel veri olup olmadığı önem taşımaktadır. Nitekim büyük veri uygulamaları kapsamında işlenen veriler özel nitelikli kişisel veri kategorisinde yer almayacak olsa bile, elde edilecek sonuç, örneğin kişinin dâhil edileceği profil kategorisi özel nitelikli veri değeri arz edebilecektir. Bu durumda veri

¹⁰⁰ The Article 29 Working Party, “Opinion 03/2013 on purpose limitation”, s. 45.

¹⁰¹ Tüzük, m. 6/4.

¹⁰² a.e., s. 46-47.

¹⁰³ a.e., s. 24.

sorumlusunun veri niteliğini göz önünde bulundurarak bir denetim yapması gerekmektedir¹⁰⁴. Nitekim özel nitelikli kişisel verilerin işleme şartları daha ağırlaştırılmış olarak hem Türk hukukunda hem de Avrupa Birliği hukukunda düzenlenmektedir.

Veri sorumlusu, sonradan ortaya çıkan yeni ya da genişleyen amaç doğrultusunda “ilgili kişi açısından doğabilecek sonuçlar” itibariyle ilgili kişinin sonuçtan nasıl etkileneceğine ilişkin bir risk değerlendirmesi yapmalıdır. İlgili kişinin temel hak ve özgürlüklerine gelebilecek muhtemel zararları ve kapsamını öngörerek bu riski değerlendirmesi gerekmektedir¹⁰⁵. Bu doğrultuda yukarıda ifade edilen verilerin istatistiksel amaçlı olarak işlenmesi örneği, ilgili kişiye doğrudan bir etki oluşturmazken; kişinin profiltenerek ilgilendiği ürün nezdinde diğer kişilerden farklı fiyatlarla karşılaşması ilgili kişinin ekonomik menfaatini etkileyebilecektir.

“Diğer imkânlar” kriteri uyarınca, sonradan belirlenen amaç doğrultusunda kişisel verilerin işlenmesi ile ortaya çıkabilecek zararların asgari seviyeye indirilmesi için veri sorumlusunun gerekli önlemleri alması gerekmektedir. Bu bakımdan Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında kişisel verilerin şifrelenmesi, maskelenmesi ya da anonim hale getirilerek kullanılması önerilmektedir¹⁰⁶.

Kişisel Verilerin Korunması Kanunu’nda ise sonradan ortaya çıkabilecek olan amaçlar için böyle bir risk değerlendirme olanağı düzenlenmemiştir. Kanun uyarınca “işleme” olarak yer alan tanım kişisel veriye ilişkin her türlü faaliyeti kapsayacak şekilde hem toplama anını hem de sonraki faaliyetleri içermektedir. Bu doğrultuda kişisel verilerin

¹⁰⁴ a.e., s. 25.

¹⁰⁵ Çekin, a.g.e., s. 60.

¹⁰⁶ Günümüzde oldukça zorlaşan ve tartışmalı olan kişisel verilerin anonimleştirilmesine ilişkin olarak veri koruma otoriteleri rehberler yayınlamaktadır. Birleşik Krallık veri koruma otoritesi tarafından hazırlanmış olan rehber için bkz. Information Commissioner Office, “Anonymisation: managing data protection risk ”code of practice” Kasım 2012, (Çevrimiçi) <https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf> , 18 Nisan 2018; Article 29 Working Party tarafından hazırlanmış görüş için bkz. Article 29 Working Party, “Opinion 05/2014 on Anonymisation Technique” WP 216, Görüş, 10 Nisan 2014; Kişisel Verileri Koruma Kurumu tarafından hazırlanmış rehber için bkz. Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi**, Ankara, KVKK yayınları, Ocak 2018, (Çevrimiçi) <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf>, 18 Nisan 2018.

toplanmasından itibaren her aşama için belirli, açık ve meşru bir amaç bulunması gerekmektedir. Kural olarak, kişisel verilerin toplanma amacı ile işleme amacının uyumlu olması gerekmektedir. Türk kanun koyucu daha sonradan ortaya çıkan veri işleme ihtiyaçlarına yönelik olarak, veri işlemeye ilk kez başlanıyormuş gibi Kanun'un 5. maddesinde yer alan hukuka uygunluk sebeplerinin değerlendirilmesi şartını koşmaktadır¹⁰⁷. Kişisel Verileri Koruma Kurumu da kişisel verilerin kullanımına ilişkin ikincil amaçlar bakımından ayrıca açık rıza alınması gerektiğini belirtmiştir¹⁰⁸.

Büyük veri uygulamaları kapsamında yürütülen kişisel veri işleme faaliyetlerinin belirli, açık ve meşru olabilmesi için öncelikle veri sorumlusunun ilgili kişileri aydınlatması ve en başından veri işleme süreçlerini şeffaf hale getirmesi gerekmektedir. Bu durum hukuka ve dürüstlük kuralına uygun veri işleme ilkesi ile paralellik arz etmektedir. Bu doğrultuda, büyük veri uygulamalarının tasarım aşamasında mümkün olduğunca kişisel veri işleme faaliyetinin amaç unsurunun belirlenmesi için çaba sarf edilmelidir. Veri toplama aşamasında ise sadece belirlenmiş olan amaç unsurunu karşılayan kanallardan büyük veri uygulamasına veri akışı sağlanmalıdır. Herhangi bir amaçla toplanmış verilerin, veri simsarlarından satın alınması ile yürütülecek büyük veri uygulamaları söz konusu ilke ile bağdaşmayacaktır.

İlke uyarınca ayrıca kişisel verilerin işleme amaçlarının meşru olması gerekmektedir. Büyük veri uygulamaları bakımından hukuka uygunluk değerlendirmesine ilişkin açıklamalara aşağıda yer verilecektir.

4.3.1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi; belirli, açık ve meşru amaçlarla kişisel verilerin işlenmesi ilkesinin devamlılığını teminat altına alan bir ilke olarak yorumlanabilecektir. İşlenen verilerin, toplama anından itibaren belirlenen; belirli, açık ve meşru amaçların gerçekleştirilebilmesine elverişli olması ve bu amacın

¹⁰⁷ TBMM Başkanlığına 18 Ocak 2016 tarihinde Adalet Komisyonu'na sevk edilen 1/541 esas numaralı Kişisel Verilerin Korunması Kanunu Tasarısı, s. 8.

¹⁰⁸ Kişisel Verileri Koruma Kurumu, Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, s. 48.

gerçekleştirilmesiyle sınırlı olması gerekmektedir. Bir başka deyişle ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılması gerekmektedir¹⁰⁹. Avrupa Birliği Genel Veri Koruma Tüzüğü'nde¹¹⁰ de muhafaza edilen bu ilke temel olarak büyük veri uygulamalarının veri toplama prensibi ile uyuşmamaktadır¹¹¹. İlgili ilkenin temel motivasyonu “gelecekte kullanmak üzere aşkın veri toplama” faaliyetlerinin önüne geçmekken, büyük veri uygulamaları her türlü veriyi set halinde ileride çeşitli senaryolarda kullanmak üzere toplamaktadır¹¹². Birleşik Krallık, Fransa ve Almanya'daki işletmeler üzerinde yapılan bir çalışmada, şirketlerin %72'sinin kullanmadıkları verileri de topladıkları anlaşılmıştır¹¹³. Bu durum teorik olarak bu ilkenin ihlal edilmesi anlamına gelmektedir. Ancak söz konusu uygulama, pratik hayatta işletmelerin gerçekte ihtiyaç duydukları veriyi bulması ve üzerinde çalışması için büyük önem taşımaktadır. Bu ilkenin yorumlanmasında yukarıda incelenmiş olan hukuka uygunluk ve dürüstlük kuralı ilkesi göz önünde bulundurulmalıdır. Büyük veri analizi ile örneğin; insanların yaşam tarzları ve bunların kredi değerliliği hakkındaki veriler arasında beklenmedik ilişkiler tespit edilebilir. Ancak bu, kişilerin yaşam tarzlarına ilişkin bilginin kredi riskini değerlendirmek amacıyla kullanılmasının gerekli olduğu anlamına gelmeyecektir. Söz konusu ilişkinin kurulabilmesi için öncelikli olarak kişisel verilerin elde edilme anına ve amacına bakarak bir değerlendirme yapmak gerekmektedir¹¹⁴.

Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında verilerin sadeleştirilmesi ilkesine ayrıca vurgu yapılmıştır. Bu ilke büyük veri uygulamalarının dayanmış

¹⁰⁹ TBMM Başkanlığınca 18 Ocak 2016 tarihinde Adalet Komisyonu'na sevk edilen 1/541 esas numaralı Kişisel Verilerin Korunması Kanunu Tasarısı, s. 8.

¹¹⁰ Avrupa Birliği Genel Veri Koruma Tüzüğü'ne ilgili ilkenin birebir tercümesi, veri işlenmesi için gerekli amaç ile bağlantılı olarak yeterli, bağlantılı ve sınırlı olma şartı yer almaktadır. Bu durum “data minimisation” olarak kısaltılmıştır. Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 5(1)c.

¹¹¹ Michael Birnhack, “S-M-L-XL DATA: Big Data as a New Informational Privacy Paradigm”, **Big Data And Privacy Making Ends Meet**, Standford Law School, The Center for İnternet And Society, (Çevrimiçi) <https://fpf.org/wp-content/uploads/Big-Data-and-Privacy-Paper-Collection.pdf> , 18 Nisan 2018, s.8-9.; Zarsky, **a.g.e.**, s.1005.

¹¹² Zarsky, **a.g.e.**, s. 1009-1010.

¹¹³ Pure Storage. Big data's big failure. “The struggles businesses face in accessing the information they need. Pure Storage” Aralık 2015, (Çevrimiçi) http://info.purestorage.com/rs/225-USM292/images/Big%20Data%27s%20Big%20Failure_UK%281%29.pdf?aliId=64921319, 8 Nisan 2018.

¹¹⁴ Information Commissioner Office, **a.g.e.**, par. 86.

olduğu çok temel bir operasyon olan veri madenciliği ile çatışmaktadır. Veri madenciliği veri tabanları içerisindeki değerli bilgileri keşfetmek anlamında kullanılmaktadır. Bilhassa otomatik karar mekanizmaları tarafından veri madenciliğinden yararlanılmaktadır¹¹⁵. Veri madenciliği teknikleri, anlamlı alt gruplar oluşturmak için benzer olayları veya kişileri bir araya toplamak gibi sınıflandırma analizini veya büyük veri grupları içerisindeki olayların ve kişilerin birlikte ilişki analizini içerebilmektedir. Geleneksel bir veri işleme faaliyetinden farklı olarak veri madenciliği büyük hacimli ve karmaşık veri grupları içerisinden anlamlı sonuçlar çıkarabilmektedir. Bu doğrultuda verilerin sadeleştirilmesi ilkesi ile veri madenciliği uygulamasının bağdaşması çok kolay gözükmemektedir¹¹⁶. Veri sadeleştirilmesi ilkesi yerine verilerin suistimal edilerek kötü amaçlı kullanımına ilişkin bir sınırlama getirmenin büyük veri uygulamaları bakımından daha uygun olacağına ilişkin görüşler mevcuttur¹¹⁷. Bu görüş uyarınca mevcut veri koruma ilkeleri ile getirilen ve her olay bakımından uygulanması gereken verilerin sınırlandırılması ölçütünü somut olay bazında, verilerin kimler tarafından, hangi amaçla, hangi bağlamda işlendiği göz önünde bulundurularak değerlendirilmesi önerilmektedir.

Gerekliklik ölçütü ile kişisel veri işleme faaliyeti neticesinde güdülen amaç göz önünde bulundurularak, bu amaca yönelik asgari seviyede kişisel verinin toplanması gerektiği ifade edilmektedir. Büyük veri uygulamaları bakımından güç olan bu durum kişisel veri işlemenin önlenmemesi gerektiğini ifade eden ve verinin ekonomik bir olgu olduğunu savunan görüş bakımından eleştirilmektedir¹¹⁸. 2013 Dünya Ekonomik Forumu kapsamında Boston Consulting Group tarafından hazırlanan raporda¹¹⁹ değişen dünyaya uyum sağlayabilmek için verinin belirli bir amaçla bağlantılı olarak işlenmesi prensibine ilişkin geleneksel görüşün değişmesi gerektiği belirtilmiştir. Bu doğrultuda, veri setlerinin çaprazlanarak kullanılması ve sonraki veri işleme

¹¹⁵ Liane Colonna, **a.g.e.**, s. 20.

¹¹⁶ **a.g.e.**, s. 21.

¹¹⁷ **a.y.**

¹¹⁸ Zarsky, **a.g.e.**, s. 1008.

¹¹⁹ The Boston Consulting Group, “Unlocking the Value of Personal Data: From Collection to Usage”, **World Economic Forum**, 2013, s.7, (Çevrimiçi) http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf, 8 Nisan 2018.

faaliyetlerinin ekonomik bir değer ve yenilik getirdiği bakış açısıyla “belirli amaç ilkesinin” tekrardan yorumlanması gerektiği ifade edilmiştir.

Veri sorumlusu ve ilgili kişinin menfaatleri bu noktada çatışmaktadır. Tasarımdan itibaren veri koruma yaklaşımı uyarınca büyük veri uygulamalarının yazılım aşamasında, bu temel çatışmanın göz önünde bulundurularak algoritmalarının tasarlanması ve her bir somut olay açısından makul dengenin sorgulanması gerekmektedir¹²⁰. Örneğin; telefonda sadece hesap makinası olarak çalışacak bir uygulamanın kişinin telefon rehberine erişmesi gereklilik ve ölçülülük ilkesi ile bağdaşmamaktadır. Bu durum, “*kişinin mahrem fotoğraflarının belirli bir uygulamanın daha da iyi hale gelmesine hizmet edeceği hususunda ciddi tereddütler mevcuttur*” şeklinde eleştirilmektedir¹²¹.

Kişisel verilerin yalnızca somut bir amacın gerçekleştirilmesi için işlenmesi ve bu amaç yerine getirildikten sonra kişisel verilerin yok edilmesi gerekmektedir. Yeni amaçlar için verilerin tekrar kullanılabilmesi için sonraki amaç bakımından bir uygunluk denetiminin yapılması gerekmektedir. Söz konusu uygunluk denetimi ve kapsamına ilişkin tartışmalar sadece büyük veri uygulamaları bakımından yoğunlaşmamaktadır. Article 29 Working Party tarafından 2013 yılında yayınlanan görüşte¹²², sonradan ortaya çıkan kullanım amaçlarının her zaman uygunsuz olacağı kabulü ile bir değerlendirme yapılamayacağı her bir somut olay bazında sonraki amacın ilgili diğer koşullar uyarınca incelenmesi gerektiği belirtilmiştir.

Bununla birlikte ilgili kişilere ve amaca göre özelleştirilmemiş veri toplama kanalları söz konusu ilke bakımından ihlal niteliği taşıyabilecektir. Örneğin, insan kaynakları olarak hizmet veren bir şirketin bütün çalışan adaylarından aynı kapsamda bilgi toplamaya yönelik anket paylaşması özellikle işe kabul değerlendirmesinde önemli olmayan ölçüde sağlık durumuna ilişkin kapsamlı soruların sorulması ölçülülük ilkesi ile bağdaşmamaktadır. Yine acil durumlarda kullanılmak üzere işveren tarafından işyerinde tehlikeli iş ayrımı yapılmaksızın beyaz yaka çalışanlarının dahi kan

¹²⁰ Çekin, **a.g.m.**, s. 637.

¹²¹ **a.y.**

¹²² The Article 29 Working Party, “Opinion 03/2013 on purpose limitation”.

grubunun toplanması ölçölülük ilkesinin ihlaline örnek olarak verilebilecektir¹²³. Büyük veri özelinde ise örneğin bireylerin sadece gazlı içecek tercihlerine ilişkin bir profillemeye yönelmiş olan büyük veri uygulaması bakımından kişilerin içecek harici başka ürünlere ilişkin tercihlerinin de toplanması ölçölülük ilkesi ile bağdaşmayacaktır.

Büyük veri uygulamaları bakımından veri sorumlularının özellikle istatistiki amaçlı olarak kişisel veri işlemleri halinde faaliyetleri kapsamında gerçekten kişisel veri toplama ve işleme gerekliliğini açık bir şekilde ortaya koymalarının gerekli olduğu belirtilmektedir¹²⁴. Bu gerekliliğin açık bir şekilde ortaya konamıyor olması halinde büyük veri uygulamalarının anonimleştirilmiş verileri kullanmaları gerekmektedir. Bir başka deyişle, büyük veri uygulamaları ile elde edilmek istenen sonuç şayet anonim haldeki verilerin işlenmesi ile de karşılanabiliyor ise anonim verilerin tercih edilmesi gerekmektedir.

4.3.1.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre Kadar Muhafaza Edilme

Kişisel verilerin gerektiğinden uzun süre tutulmaması ilkesi, kişisel verilerin korunması düşüncesinin merkezinde yer almaktadır. Zira verilerinin silinmediğine inanan toplumlarda “yeri ve zamanı geldiğinde” kullanılmak üzere kendi verilerinin süresiz olarak saklandığını düşünen bireylerin bireysel özerklik, bireyin maddi ve manevi bütünlüğü ve özel yaşamın gizliliği gibi değerleri zarar görebilecektir¹²⁵. Bu halde, kişisel verilerin işlenmesi ile hedeflenen amacın gerçekleşmiş olması, amaca ulaşmak için kişisel verinin işlenmesinin gereksiz olduğunun anlaşılması ya da amacın ortadan kalmış olması halinde kişisel verilerin yok edilmesi gerekmektedir. Belirtmek gerekir ki, büyük veri uygulamaları bakımından, dijital verilerin saklama maliyetleri düştükçe kişisel verileri silmek yahut yok etmek bir o kadar maliyetli bir tablo

¹²³ Belirtmek gerekir ki Türk hukuku açısından sağlık verileri sözleşmenin kurulması ifası hukuka uygunluk sebebine dayanarak işlenememektedir. Bu durum eleştirilere konu olmaktadır, Yücedağ, **a.g.m.**, s. 772.

¹²⁴ Article 29 Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, s. 19.

¹²⁵ Küzeci, **a.g.e.**, s. 227.

çıkarmaktadır¹²⁶. Bununla birlikte dijital dünyada yedekleme faaliyetleri sebebi ile bir verinin geri döndürülemeyecek şekilde yok edilmesi güçleşmektedir¹²⁷.

İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi, temel olarak amaçla bağlantılı ilkesi ile benzeşmektedir. Söz konusu ilkenin temel unsurlarından biri, kişisel verilerin toplandığı amaçtan başka bir amaçla işlenmemesidir. Karmaşık algoritmalar kullanarak verilerin analiz edilmesine ve verilerin yeni amaçlar için kullanılmasına yol açabilecek beklenmedik eşleştirmelere neden olan süreçler meydana getiren büyük veri işleme faaliyetleri, temel olarak bu ilke ile bağdaşmamaktadır¹²⁸. Bulut sistemlerinin gelişmesi ile birlikte veri depolama maliyetleri düşerek büyük hacimde verilerin saklanmasına elverişli sistemler kullanıma açılmıştır. Bu doğrultuda şirketler ise sakladıkları veri boyutu bakımından bir tasarrufa gitme düşüncesinden günden güne uzaklaşmıştır. Bununla beraber çoğu zaman verileri silme ya da yok etmenin maliyeti saklamaktan daha yüksek olabilmektedir. Saklanabilen veri oranı arttıkça veriyi elinde bulunduran şirketler ise bu verilerden bir değer yaratma arayışına girmişlerdir. Büyük ölçüde maliyetlerle ilgili olan bu temel iki sebebin büyük veri uygulamalarının doğumunda büyük bir etken olduğu düşünülmektedir¹²⁹.

İlgili kişinin sahip olduğu kişisel verilerinin silinmesini talep etme hakkı, temel olarak bu ilkenin bir hak olarak tesis edilmiş halidir. Kişisel Verilerin Korunması Kanunu gerekçesinde bu ilke “*gelecekte kullanma ihtimalinin varlığına dayanarak veri saklanamayacaktır*” ifadesi¹³⁰ ile açıklanmaktadır. Bu ilke uyarınca, veri sorumlusunun kişisel verileri toplama yahut elde etme anında var olan amacı ortadan kalktığı noktada kişisel verileri silmesi, anonim hale getirmesi ya da yok etmesi gerekmektedir. Bu doğrultuda kişisel verilerin işlenmesine ilişkin olarak yukarıda

¹²⁶ Jim Sterne, “Is It Cheaper to Keep Than Delete?”, 10 Nisan 2014, (Çevrimiçi) <https://www.clickz.com/is-it-cheaper-to-keep-than-delete/32085/>, 18 Nisan 2018.

¹²⁷ Anonimleştirmeye ilişkin güçlükler için bkz. yukarıda dn. 98.

¹²⁸ Verilerin sadeleştirilmesi ilkesinin büyük veri uygulamaları ile tamamen ters düştüğüne ilişkin görüş için bkz. Çekin, **a.g.e.**, s. 638.

¹²⁹ Warner, Andrew, George Dyson seminar media, “The Long Now Foundation” 28 Mart 2013, (Çevrimiçi) <http://blog.longnow.org/02013/03/28/george-dyson-seminar-media/> 08 Nisan 2018.

¹³⁰ TBMM Başkanlığınca 18 Ocak 2016 tarihinde Adalet Komisyonu’na sevk edilen 1/541 esas numaralı Kişisel Verilerin Korunması Kanunu Tasarısı, s. 8.

bahsedilen hukuka ve dürüstlük kurallarına uygun olma, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkelerine uyum sağlayan bir veri sorumlusunun bu ilkeye uyum sağlaması kaçınılmazdır.

Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında müstakil bir hak olarak “unutulma hakkı” getirilmiştir (m. 17)¹³¹. Doğrudan bu ilke ile uyumlu olan bu hak temel olarak dijital çağın çok önemli bir gereksinimi karşılamaktadır. Nitekim günümüzde dijital dünyada gerçekleştirilen her hareket bir iz olarak sanal dünyada saklanarak kişilere değiştirilemez bir etiket yaratmaktadır. Bu doğrultuda unutulma hakkı bireysel özerkliğin korunması bakımından önem taşımaktadır. Nitekim bireyler geçmişlerinin kendilerini sürekli takip ettiği düşüncesiyle kendilerini geliştirme olanağından yoksun kalabileceklerdir.

Büyük veri uygulamaları bakımından problemli olan kısım çoğunlukla büyük veri kapsamında veri setleri içerisinde yer alan verinin temel olarak ne amaçla tutulduğunun tespitinin güç olmasıdır. Zira büyük veride set halindeki veri grupları eşlenerek yeni sonuçlar türetilmesi hedeflenmektedir. Bu bakımdan verinin mümkün olduğunca uzun süreli olarak saklanması büyük veri uygulamaları bakımından tercih edilmektedir. Ancak uzun yıllar saklanan verilerin hem doğru ve güncel olma ilkesi bakımından hem de büyük veri uygulamalarının beklediği doğru sonuçları yaratmak bakımından elverişsiz olduğunun esasen kabulü gerekmektedir. Bu doğrultuda veri sorumlularının kişisel verileri elde ederken ve işlerken dayanak aldığı hukuka uygunluk sebeplerini göz önünde bulundurarak kişisel verilerin saklanmasına ve imha edilmesine ilişkin politikalar geliştirmesi ve bu politikaları şirket departmanları içerisinde bir kültür olarak uygulaması önem arz etmektedir. IBM gibi büyük teknoloji şirketleri de büyük veriden elde edilen faydanın yüksek tutulması için temel

¹³¹ Avrupa Birliği hukukunda unutulma hakkının yargısal düzeyde en üst seviyede tanınmasına ilişkin olarak bkz. “Google Spain SL ve Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González” Adalet Divanı (Grand Chamber)’a karşı, Karar No C-131/1213, Karar Tarihi 13 Mayıs 2014.

yaklaşımların bu olması gerektiğine yönelik açıklamalara, çalışmalarında yer vermektedir¹³².

Büyük veri uygulamaları bakımından elde edilmek istenen menfaat için kişisel verilerin saklanması ve işlenmesinin zorunlu olup olmadığı tespit edilmelidir. Süreçler bakımından bir ayrıma gidilerek ilgili menfaati elde etmek için anonim verinin yeterli olması halinde kişisel verilerin anonimleştirilerek saklanması gerekmektedir.

Avrupa Birliği Genel Veri Koruma Tüzüğü ile silme ya da anonimleştirmeye alternatif olarak yer alan psödosomasyon ve şifreleme gibi yöntemler getirilmiştir. Türkçe bir karşılığı henüz öğretilen yer almayan psödosomasyon kavramı bulanıklaştırma olarak dilimize taşınabilecektir. Psödosomasyon yöntemi, kişisel verilerin ek bilgi kullanılmaksızın, ilgili kişiye ilişkin olmayacak biçimde işlenmesi anlamına gelmektedir. Avrupa Birliği Genel Veri Koruma Tüzüğü'nde ayrıca verinin bir kişiye ilişkin olabilmesi için gerek duyulan bilgilerin ayrı ayrı tutulması ve bu birleştirmenin yapılmaması için kapsamlı teknik ve idari önlemlerin alınması gerektiği ifade edilmektedir. Avrupa Komisyonu tarafından Veri Koruma Reformu hakkında soruları cevaplamak üzere yayınlanan Rapor'da¹³³ Avrupa Birliği Genel Veri Koruma Tüzüğü ile getirilen bu yeni kavramların, büyük veri uygulamalarını, anonimleştirme ve psödosomasyon işlemlerine maruz bırakılmış verilerin kullanımını teşvik etme amaçlı olduğu belirtilmiştir¹³⁴. Bu doğrultuda veri sorumlularının veri toplama anında söz konusu verinin anonim olarak kullanılıp kullanılmayacağına ilişkin bir değerlendirme yapması gerekmektedir. Adı geçen Rapor'da büyük veri uygulamaları tarafından, ham halde olan verinin; ilgili kişi tarafından beklenebilir ya da verilerin toplanma anında

¹³² IBM, “**Information lifecycle governance in a big data environment**” IBM Corporation, Ocak 2015, s.7, (Çevrimiçi) https://www-01.ibm.com/software/it/events/bigdata/pdfs/IBM_ILG_in_a_Big_Data_environment.pdf, 8 Nisan 2018.

¹³³ Avrupa Komisyonu, Fact Sheet, “Questions and Answers - Data Protection Reform”, Brüksel, 21 Aralık 2015

¹³⁴ Belirtmek gerekir ki psödosomasyon işlemlerine maruz bırakılmış kişisel veriler anonim olarak kabul edilmemektir. Psödosomasyon bir çeşit anonimleştirme yöntemi olmayıp, psödosomasyon işlemi uygulanmış veriler kişisel veri olarak değerlendirilmektedir. Psödosomasyon ve anonimleştirme işlemlerinin teknik olarak farklarına ilişkin bkz. Article 29 Working Party, “Opinion 05/2014 on Anonymisation Techniques”, s. 3, 20-25.

belirtilen orijinal amaçla uyumlu amaçlar için kullanılmak üzere saklanması uygun olabileceği belirtilmektedir.

Kişisel verilerin uzun süreler boyunca tutulması güvenlik açısından da bir risk oluşturmaktadır¹³⁵. Siber saldırı olaylarının yaygınlaştığı günümüzde özellikle dijital ortamda yer alan veri tabanlarını korumanın maliyeti artmaktadır. Veri sorumlusunun temel yükümlülüklerinden olan veri güvenliğinin sağlanması bakımından veri silme, imha etme politikalarını düzenleyerek, uygulanmasına ilişkin kontrolleri sağlamak yerinde olacaktır.

4.3.2. Büyük Veri Uygulamaları ve Hukuka Uygunluk Sebepleri

Kişisel veri işleme faaliyetinin meşru olabilmesi için kişisel verilerin korunmasına ilişkin ilgili düzenlemelerde öngörülüş, çalışmanın ikinci ve üçüncü bölümünde değinilen Avrupa Birliği ve Türk veri koruma hukukunda yer alan hukuka uygunluk nedenlerinin bulunması gerekmektedir. Büyük veri uygulamaları kapsamında kişisel verilerin işlenmesi faaliyetlerine ilişkin söz konusu hukuka uygunluk sebeplerinin değerlendirilmesi konusunda çeşitli tartışmalar öğretilde yer almaktadır. Bazı yazarlar¹³⁶ büyük veri uygulamalarının sadece açık rıza istisnası kapsamında gerçekleştirilebileceği savını ileri sürmektedir. Diğer bir görüş ise geçerli bir açık rızanın bulundurulması gereken unsurların büyük veri uygulamaları kapsamında sağlanmasının güç olması sebebi ile büyük veri uygulamaları bakımından, açık rıza hukuka uygunluk sebebinin uygulama alanı bulamayacağı ifade edilmektedir.

Bu başlık altında ilgili kişinin açık rızası, sözleşmenin kurulması ya da ifası için gerekli olması, kişisel verilerin ilgili kişinin kendisi tarafından alenileştirilmiş olması ve veri sorumlusunun üstün meşru menfaati hukuka uygunluk sebepleri bakımından büyük veri uygulamaları özelinde değerlendirmeler yapılacaktır.

¹³⁵ Zarsky, **a.g.e.**, s. 1010.

¹³⁶ Giuseppe D' Acquisto v.d., "Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies In The Era Of Big Data Analytics", **The European Union Agency for Network and Information Security (ENISA)**, Aralık 2015, s.46.

4.3.2.1. Açık Rıza

İlgili kişilerden alınan beyanın, geçerli bir açık rızanın unsurlarını taşıp taşımadığı sadece büyük veriler bakımından değil genel olarak veri koruma hukuku bakımından tartışmalı bir konudur. Büyük veri uygulamaları bakımından çevrimiçi ortamlar vasıtası ile alınan rıza kavramına ilişkin çekinceler Avrupa Komisyonu Raporu’nda belirtilmiştir¹³⁷. Söz konusu Rapor’da büyük veri uygulamalarına ilişkin olarak gizlilik politikalarının yeterince açık olmaması ve çevrimiçi davranışsal reklamcılık gibi alanlarda kullanıcıların tam olarak neye rıza verdiklerini anlayamamaları sorun olarak ifade edilmiştir. Birleşik Krallık veri koruma otoritesi, hazırlamış olduğu raporunda¹³⁸, büyük veri uygulamaları kapsamında alınan rızanın geçerli olarak kabul edilebilmesinin önünde çeşitli engellerin olduğunu; yenilikçi ve farklı bir yaklaşım ile bu sorunların çözülebileceğini belirtmiştir.

Günümüzde veri koruma hukuku alanında, “enformasyonel self-determinasyon”¹³⁹ hakkı temelli bir yaklaşım, baskın olarak yer almaktadır. Kişisel Verilerin Korunması Kanunu kapsamında Avrupa Birliği Veri Koruması Yönergesi’nde öngörülenden daha nitelikli bir rıza aranmaktadır. Avrupa Birliği Veri Koruma Yönergesi’nde özel nitelikli olmayan kişisel verilerin işlenmesi için ilgili kişinin rızası yeterli iken Kanun’da *açık rıza* aranmaktadır. Açık rıza ise Kanun’da “*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*” olarak tanımlanmıştır. Avrupa Birliği Genel Veri Koruma Tüzüğü’nde ise rızanın “*şüpheye yer vermeyecek şekilde*” ve ilgili kişinin “*açık bir hareketi*” ile gerçekleşmiş olma şartı aranmaktadır.

¹³⁷ Avrupa Komisyonu, “Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union”, s.9.

¹³⁸ Information Commissioner Office, “Big data, artificial intelligence, machine learning and data protection”, par. 55.

¹³⁹ “Kişinin kendisiyle ilgili kişisel verileri üzerindeki tasarruf hakkı” olarak nitelendirilebilecek “informational self- determination” hakkı ilk olarak Alman Federal Mahkemesi’nin Nüfus Sayımı Kararı’nda ortaya koyulmuştur, Karara ilişkin olarak bkz. yukarıda s. 26, 27. Yaklaşım ile bireylerin verilerinin kontrolünü ellerinde bulundurması gerektiği ifade edilmek istemiştir, Bart Custers, Helena Ursic, “Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection”, **International Data Privacy Law**, 2016, s. 11.

Bu bakımdan değerlendirilmesi gereken husus büyük veri uygulamaları kapsamında geçerli bir açık rızadan bahsedilmesinin mümkün olup olmayacağı sorunudur. Zira büyük veri uygulamalarında kullanılan algoritmaların karışık çalışma prensibi, çoğu zaman veri işleme faaliyetini anlaşılır bir şekilde açıklamaya elverişli değildir. Ancak büyük veri uygulamalarının karmaşık bir yapıya sahip ve farklı kaynaklardan besleniyor olması ilgili kişinin rızasına ilişkin gerekliliği bertaraf edecek bir mazeret olarak kabul edilmemektedir¹⁴⁰. Veri sorumlularının büyük veri uygulamalarının faydalarını açıklamak ve kullanıcılara işlevsel bir seçim sunmak üzere bir mekanizma bulması gerektiği ve yürütülecek kişisel veri işleme faaliyetlerinde bu seçime saygı göstermeleri gerektiği belirtilmektedir. Bu doğrultuda veri sorumlularının algoritmalarını planlarken hangi amaçla ve hangi verileri işleyeceğini baştan tespit etmiş olması gerekmektedir.

Bir servis ya da hizmet sunmanın ön koşulu olarak kişisel veri işlemeye ilişkin rızanın ön şart olarak dayatılıp dayatılamayacağı da tartışmalı bir konudur. Kişinin rızasını vermesine ilişkin bir seçme imkânının olmaması ya da rızasını istediği zaman geri alamaması veri koruma düzenlemelerinde yer alan asgari rıza koşullarını sağlamama gerekçesiyle eleştirilmektedir¹⁴¹. Büyük veriye en çok katkı sağlayan kaynakların başında şüphesiz ücretli yahut ücretsiz çevrimiçi mobil uygulamalar gelmektedir. Kullanıcıların çevrimiçi ortamlardaki uygulamalardan yararlanmak üzere kişisel verilerinin işlenmesine ilişkin olarak vermiş oldukları rıza, özgür irade unsuru bakımından tartışmalıdır. Örneğin; fotoğraflar üzerinde düzeltme ve oynama yapılmasını sağlayan bir mobil uygulama, kullanıcılarından konum bilgilerini ve davranışsal reklamcılık faaliyeti kapsamında diğer verilerini uygulamanın kullanılması için ön koşul olarak talep etmektedir. Bu kapsamda fotoğraf düzenlemesine ilişkin bu uygulamanın sağlamış olduğu hizmet ile konum bilgisi talebi ve davranışsal reklamcılık faaliyeti uyusmamaktadır. Kişinin, bu verilerin paylaşılmasına izin vermediği halde uygulamayı kullanamayacak olması rızanın özgür iradeye dayalı olarak kabul edilmesi önünde engel teşkil etmektedir¹⁴².

¹⁴⁰ Information Commissioner Office, “Big data and data protection”, par. 60.

¹⁴¹ Information Commissioner Office, “Big data and data protection”, par. 58.

¹⁴² Article 29 Working Party, “Guidelines on consent under Regulation 2016/679”, s. 6.

Veri sorumlusu her zaman rızanın geri alınabilmesi için elverişli yolları ilgili kişi bakımından ulaşılabilir tutmakla yükümlü olup, bu doğrultuda ilgili kişinin rızasını geri alması halinde rızaya dayalı veri işleme faaliyetlerini durdurması gerekmektedir¹⁴³. Bir başka deyişle, yeterli değerlendirme yapmaksızın sözleşmenin ifası, meşru menfaat gibi başkaca hukuka uygunluk sebepleri olmasına rağmen ilgili kişiden onay almayı tercih eden veri sorumlusu, ilgili kişiyi bu amaçlar için bilgilendirmediğinden rızasını geri çekmesi halinde kişisel verileri işleyemeyecektir. Rızanın ilgili kişi tarafından geri alınabileceği, Avrupa Birliği Veri Koruma Tüzüğü kapsamında açık ve net bir şekilde yer almaktadır. Tüzük ile rızanın koşullarının ağırlaştırılmış olması ve ilgili kişinin rızasını her zaman geri alabilecek olması, büyük veri uygulamaları bakımından açık rıza hukuka uygunluk sebebine dayanarak veri işleme faaliyetlerini yürütmeyi elverişsiz hale getirdiği görüşü ile eleştirilmektedir¹⁴⁴. Türk hukuku bakımından da

Büyük veri uygulamaları kapsamında genellikle veriler elde edilme anında belirtilen amaçtan başka, sonraki bir amaç için işlenebilmektedir. Amaçla bağlantılılık ilkesi gereğince bu durum genel ilkelere aykırılık teşkil edecektir. Uygulamada büyük veri uygulamaları kapsamında kişisel verilerin işlenmesi için sıklıkla açık rıza hukuka uygunluk sebebine başvurulmaktadır. Ancak belirtmek gerekir ki geçerli bir rızanın en temel iki koşulu rıza metninin açık ve spesifik olmasıdır. Uygulamada ise mümkün olduğunca geniş kapsamlı olarak internet ortamında hizmet verenler ilgili kişilerin açık rızalarını sormaktadırlar. Avrupa Birliği’nde bulunan veri koruma otoriteleri bu tür geniş kapsamlı ve ucu açık rıza beyanlarını kabul etmemektedir. Fransız veri koruma otoritesi, gizlilik politikasında amaçların net bir şekilde belirlenmemiş olması ve

¹⁴³ Online olarak kişisel verilerin işlenmesine ilişkin olarak verilen rızanın sadece mesai saatlerinde açık olan çağrı merkezi üzerinden geri alınabileceğine ilişkin mekanizma kurgulayan veri sorumlusunun dürüstlük ilkesine uygun davranmadığına ilişkin örnek için bkz. Article 29 Working Party, “Guidelines on consent under Regulation 2016/679”, s. 20.

¹⁴⁴ Viktor Mayer-Schönberger, Yann Padova, “Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation” **The Columbia Science & Technology Law Review**, Cilt 17, s. 315-335, Bahar 2016, s. 326.

gizlilik sözleşmesinin kapsamının çok geniş olması sebebi ile 2014 yılında, veri sorumlusu hakkında para cezası yaptırımında bulunmuştur¹⁴⁵.

Büyük veri uygulamaları kapsamında alınacak olan rızanın, mevcutta uygulanan geleneksel modellerin ötesine geçmesi gerektiği belirtilmektedir. Bu görüş uyarınca rızanın ilgili kişiden alınması aşamasında ve geri çekilmesinde daha fazla otomasyon sağlanması gerekmektedir. Ancak bu durumda da belirli uygulamaların ilgili kişi adına rıza veren ajan yazılımları, büyük veri uygulamaları bakımından riskli bir alan oluşturmaktadır.

Çevrimiçi ortamlar haricinde büyük veri uygulamasına veri akışı sağlayan sensörler, nesnelerin interneti ve akıllı cihazlar aracılığı ile toplanan kişisel veriler ayrı bir risk alanı teşkil etmektedir. Söz konusu teknolojiler ile çok fazla veri toplanabilmekte ve bu verilerin veri madenciliği gibi diğer analiz yöntemleri ile ilgili kişiler hakkında bireylerin öngöremeyeceği kadar çeşitli veriler üretilebilmektedir¹⁴⁶. Bu tür sistemler için yaratıcı rıza alım süreçlerinin kurgulanması gerektiği belirtilmektedir. İlgili kişinin jestleri, davranış kalıpları ve hareketlerinin otomatik olarak analiz edilebileceği sistemler örnek olarak verilmektedir¹⁴⁷.

Geçerli bir rızanın kademeli olması gerektiğine ilişkin görüşler de bulunmaktadır¹⁴⁸. Buna göre ilgili kişi bir sisteme dâhil olmadan önce önüne getirilen ve geniş kapsamlı bir metin içerisinde, bütün veri işleme faaliyetlerine ilişkin rıza vermek durumunda bırakılmamalıdır. Bu doğrultuda örneğin bir sosyal medya platformuna giren kişi, başlangıçta sadece sisteme giriş için gerekli olduğu ölçüde verileri talep edilmelidir. Daha sonrasında ise hukuka uygunluk sebeplerinin bulunmaması halinde rızası alınmalı ve üçüncü taraflara veri paylaşım faaliyetlerinin amaçları ve etkisi anlatılarak ayrıca paylaşım faaliyetine ilişkin rızası sorulmalıdır.

¹⁴⁵ Commission Nationale de l'Informatique et des Libertés, Fransız Veri Koruma Otoritesi, Yaptırımlar Komitesi, No. 2013-420, 3 Ocak 2014, (Çevrimiçi) <https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000028450267>, 7 Haziran 2018.

¹⁴⁶ Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values", Giriş Bölümü.

¹⁴⁷ Giuseppe D' Acquisto, Josep Domingo-Ferrer, Panayiotis Kikiras, Vicenç Torra, Yves-Alexandre de Montjoye, Athena Bourka, **a.g.e.**, s. 46.

¹⁴⁸ Information Commissioner Office, "Big data and data protection", par. 57.

Büyük veri uygulamaları bakımından bir başka sorun ise, büyük veri uygulamalarına kaynaklık eden kişisel verilerin çoğunlukla ilgili kişilerin doğrudan kendilerinden toplanmıyor olmasıdır. Bu şekilde üçüncü taraf uygulamaları ya da veri sorumluları aracılığı ile toplanan veriler büyük veri havuzuna dâhil edilerek işlenmektedir. Uygulamada veri ticaretini ekonomik gelir modeli olarak kullanan veri simsarları büyük veri setlerini satmaktadırlar. Bu halde veri satın alan kurum ya da kuruluş, elde etmiş olduğu veriler bakımından bireylere karşı veri sorumlusu sıfatıyla sorumlu olacaktır. İlgili kişilerin, kişisel verilerinin işlenmesine ilişkin olarak rızalarının olmadığı beyan etmeleri, haklarına ilişkin başvuruda bulunmaları halinde, verileri satan kişi ile birlikte veri setini satın alın kişi, kurum ve kuruluşlar beraber sorumlu tutulacaktır. Bu nedenle üçüncü taraf uygulamalar, kişi ya da kurumlardan elde edilen kişisel verilerin veri koruma düzenlemelerine uygun edinilmiş olması ve yürütülecek faaliyetin de ilgili kullanıcıdan alınan rıza kapsamında yer alması önem taşımaktadır. Uygulamada, rıza metinlerinde yer verilen “*kişisel verileriniz üçüncü kişiler ile paylaşılabılır*” ifadesi bu doğrultuda yeterli kabul edilmemektedir¹⁴⁹. Hem Tüzük hem de Kişisel Verilerin Korunması Kanunu, verilerin paylaşılacağı üçüncü kişiler bakımından aydınlatma yahut rıza metninde asgari seviyede bir grupta aramaktadır.

Yukarıda açıklandığı üzere veri sorumluları tarafından kişisel veri işleme faaliyetini, bireyin rızası hukuka uygunluk sebebi uyarınca gerçekleştiriyor olmak büyük veri uygulamaları itibarıyla risk taşımaktadır. Öncelikle veri işleme faaliyeti bakımından ilgili kişinin rızasının gerekip gerekmediği doğru bir şekilde değerlendirilmelidir. Nitekim, esasen başka bir hukuka uygunluk sebebi bulunmasına rağmen kullanıcının onayının sorulması kullanıcıyı yanıltıcı nitelikte olabilecektir. Uygulamada sıklıkla başvurulmuş bir hizmet ya da servisin sağlanması için kişisel verilerin işlenmesine ilişkin onayın şart koşulması, kullanıcının özgür olarak rıza göstermesi önünde engel teşkil edebilecektir¹⁵⁰.

¹⁴⁹ Information Commissioner Office, “Direct marketing”, 6 Mart 2018, (Çevrimiçi) <https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf>, 18 Nisan 2018, par. 89.

¹⁵⁰ Lucas Bergkamp, Jan Dhont, **a.g.e.**, s. 78.

Türk hukuku bakımından Nisan 2016, Avrupa Birliği için ise 25 Mayıs 2018 itibari ile itibari ile uygulanmaya başlayan açık rıza düzenlemesi kapsamında ilgili otoritelerin yorumları uygulamada yol gösterici olabilecektir. Ancak bilhassa büyük veri uygulamaları bakımından, veri işleme faaliyetlerinin her bir somut olayda farklı sonuçlar üretecek şekilde algoritmalar çalıştırması, açık rıza hukuka uygunluk sebebinin belirlilik ve bilgilendirmeye dayalı olma unsurları bakımından sorun yaratmaktadır. Bu bakımdan kişisel verilerin işlenmesine ilişkin rızanın gerekliliği diğer hukuka uygunluk sebepleri göz önünde bulundurularak değerlendirilmelidir¹⁵¹.

4.3.2.2. Sözleşmenin Kurulması veya İfası Kapsamında Gerekli Olma

Hem Avrupa Birliği Veri Koruma Yönergesi hem de Kişisel Verilerin Korunması Kanunu'nda bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması hali hukuka uygunluk sebebi olarak yer almaktadır. Belirtmek gerekir ki genel olarak büyük veri uygulamaları, sözleşmenin kurulması yahut ifasından ayrı olarak bir sözleşme ilişkisi çerçevesinde toplanan verileri, sözleşme kapsamı dışında başka amaçlarla işlemektedir. Böyle bir uygulama olduğunda söz konusu hukuka uygunluk sebebinin varlığından bahsedilemeyecektir. Zira belirli ve meşru amaçlar için işleme ilkesi kişisel verilerin toplanma anında güdülen amaç ile uyumlu işleme faaliyetlerini aramaktadır.

Büyük veri uygulamaları kapsamında, kişisel verilerin işlenmesinin bir sözleşmenin kurulması yahut ifası için gerekli olduğunun ispatı çoğunlukla kolay olmamaktadır¹⁵². Sözleşme öncesi önlemler deyimi ile madde kapsamı genişliyor olsa da Kişisel Verilerin Korunması Kanunu kapsamında mümkün olduğunca bireylerin korunması ilkesi gereği, dar yorumlamak esas alınmalıdır. Bu nedenle sözleşme öncesi önlemler ile genel olarak bir sözleşmenin kurulması amaçlanıyorsa, kurulma aşamasına kadar taraflarca alınan önlemler ifade edilmektedir¹⁵³.

¹⁵¹ **a.e.**, s. 81.

¹⁵² Information Commissioner Office, “Big data, artificial intelligence, machine learning and data protection”, par. 54.

¹⁵³ Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin, 2004, s. 41.

Söz konusu hukuka uygunluk sebebi, sözleşme yapmak amacı ile görüşmeye başlayan taraflar arasında, tarafların birbirlerinin kişisel verilerini işlemesini mümkün kılmaktadır. Düzenleme ile veri sorumlusunu, sözleşme ilişkisinde olduğu ya da olması muhtemel olan kişilerin verilerini sözleşme kapsamı ile sınırlı olarak işlemesi halinde bir hukuka uygunluk zemini tesis edilmesi amaçlanmaktadır. Ancak belirtmek gerekir ki sözleşmenin kurulmamış olması sonucunda veri sorumlusunun verileri imha etmesi veya ilgili kişiye iade etmesi gerekmektedir¹⁵⁴. Örneğin; bir satış sözleşmesinin kurulması amacı ile toplanan iletişim bilgilerinin sözleşmenin kurulmaması halinde bu verilerin daha sonradan pazarlama amaçlı olarak bir veri tabanına kaydedilerek bireye talep etmediği bir hizmet yahut mala ilişkin olarak teklif gönderilmesi bu kapsamda değerlendirilmeyecektir. Yahut mal ve hizmete ilişkin bir sözleşme kurulmuş olsa dahi başkaca hizmet ve ürün teklifi için pazarlama amaçlı söz konusu verilerin kullanılması, kişi ile iletişim kurulması ölçülülük ilkesine aykırı olacağından yine bu kapsamda değerlendirilmeyecektir.

Bu bakımdan elektronik ticaret sitelerinde yer alan kullanıcı davranışlarını izleme ve profilleyerek bu doğrultuda öneride bulunmaya ilişkin büyük veri uygulamaları sözleşmenin kurulması hukuka uygunluk sebebi altında değerlendirilemeyecektir.

Büyük veri uygulamaları bakımından, kişinin bir büyük veri uygulamasının hizmetlerinden yararlanmasına yönelik iradesi ile kurulmuş bir sözleşme kapsamında bu hukuka uygunluk sebebinin işletilmesi mümkün gözükmektedir. Büyük veri uygulamaları, veri sorumlusunun otomatik karar mekanizmalarından yararlanarak insan etkisi ve ön yargısı gibi etkenleri bertaraf etmek istediği durumlarda kullanılmaktadır. Örneğin kredi sözleşmesi gibi geri ödemeli sözleşmelerin kurulması için müşterisinin ödemeleri karşılayamama riskini azaltmak isteyen kurum ve kuruluşlar otomatik karar mekanizmalarında yararlanmaktadır. Büyük veri setleri söz konusu olduğunda kısa sürede pratik olarak sonuç elde etmek isteyen şirketler de yine

¹⁵⁴ Develioğlu, a.g.e., s. 61.

büyük veri uygulamalarına başvurmaktadır¹⁵⁵. Bu kapsamda otomatik iş başvurusu değerlendirme sistemleri örnek olarak verilebilecektir.

Kişiye özel bir sonucun elde edilmesinin, bir ürün yahut hizmetin kişi için özelleştirilmesinin ifa için gerekli olduğu bir sözleşme kapsamında da büyük veri uygulamaları kullanılabilir. Ancak bu halde dahi kişi sözleşmenin ifası için işlenebilecek kişisel verilerinin neler olduğunu ve nasıl işleneceklerini önceden biliyor olmalıdır. Banka sektöründe kredi notu hesaplaması için kullanılan büyük veri uygulamaları bu duruma örnektir. Kişi kredi notunun hesaplanması için kuruluşa başvurduğunda pek çok kurum ve kuruluştan veriler toplanarak bir sonuç elde edilmektedir. Bu doğrultuda kişinin doğru kredi notunun hesaplanabilmesi için her ne kadar açık rızası gerekmeseyse de kişinin kredi notunun hangi kaynaklardan elde edilen hangi verilerle hesaplanacağını başvurmadan önce bilmesi gerekmektedir¹⁵⁶. Ancak bir büyük veri uygulamasının herhangi bir sözleşmenin ifası için *kesinlikle* gerekli olma durumu oldukça istisnai olabilecektir¹⁵⁷. Günümüzde sadece bankalar ve kredi kuruluşları değil müşteri portföyünü ve ortaklık ilişkilerini doğru yönetmek isteyen gerçek ya da tüzel kişiler de, muhatap oldukları kişilerin “notlanmasını” talep edebilmektedir. Bu bakımdan söz konusu kurulacak olan ilişki göz önünde bulundurularak talep edilen “notlandırmanın” sözleşmenin kurulması için gerekli olup olmadığının değerlendirilmesi gerekmektedir.

Sözleşmenin kurulması için talep edilen veriler, amaçla bağlantılılık ilkesine riayet edilerek toplanmalıdır. Örneğin; herhangi bir üyelik talep etmeksizin bir elektronik ticaret sitesi vasıtası ile alışveriş yapan bir kişi için sözleşmenin ifası kapsamında, ödeme yapmak için kredi kartı bilgileri ve ürünü teslim etmek için ilgili kişinin adresinin işlenmesi gereklidir. Sözleşmenin tamamlanması, kullanıcının beğenilerinin ve yaşam tarzı seçimlerinden yola çıkarak bir profil oluşturmaya bağlı değildir.

¹⁵⁵ Article 29 Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, s. 12.

¹⁵⁶ **a.e.**, s. 12.

¹⁵⁷ Information Commissioner Office, **a.g.e.**, par. 73.

Profillemenin, sözleşme içeriğinde özellikle belirtilmiş olması, tek başına, bu faaliyetin “gerekli” olmasını sağlamayacaktır¹⁵⁸.

Profilleme olarak nitelendirilebilecek bu tür büyük veri uygulamalarına ilişkin olarak Kişisel Verilerin Korunması Kanunu kapsamında doğrudan ve açık bir düzenleme bulunmamasına karşın, Avrupa Birliği Genel Veri Koruma Tüzüğü’nde profilleme tanımına yer verilerek ayrıca düzenlenmiştir. Avrupa Birliği Veri Koruma Tüzüğü’nde profilleme, kişisel verilerin, bireye ilişkin belirli kişisel yönlerini değerlendirmek amacı ile kullanılmasından oluşan, herhangi bir şekilde otomatik olarak işlenmesi olarak tanımlanmaktadır¹⁵⁹. İlgili kişinin bilgilendirilmesi ve kişisel verilere erişim hakkına ilişkin madde kapsamında profilleme yapan veri sorumlusunun ek yükümlülükler getirilmiştir. Madde uyarınca veri sorumlusunun, ilgili kişinin otomatik veri işlemeye ve profillemeye konu olması halinde (m. 13/2.f); otomatik karar alma sürecinin varlığı (m. 14/2.g), işlemenin mantığı, söz konusu işlemin önemi ve ilgili kişi için öngörülen sonuçları hakkında (m.15/1.h.) ilgili kişiye bilgi vermesi gerekmektedir.

Avrupa Birliği Genel Veri Koruma Tüzüğü’nde profilleme ve otomatik karar mekanizmalarına ilişkin olarak yer alan hükümde ilgili kişinin kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen profil çıkarma da dâhil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı sınırlandırılmıştır. Söz konusu faaliyetin sözleşmenin kurulması yahut ifası için gerekli olma hali madde kapsamından istisna tutulmuştur¹⁶⁰. Ancak bu halde dahi ilgili kişiye kendi görüşünü ifade hakkı ve çıkan sonuca itiraz hakkının tanınması gerektiği belirtilmiştir.

Sözleşmenin ifası hukuka uygunluk sebebi, akıllı cihazların kullanımının artması ve nesnelerin interneti teknolojilerinin yaygınlaşması ile daha sık uygulama alanı bulabilecektir. Nitekim internete erişim sağlamak için bireyler veya kurumsal kurumlar tarafından kullanılan router ve switch gibi ürünlerin üreticisi Cisco,

¹⁵⁸ Article 29 Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation”, s. 20.

¹⁵⁹ Profillemeye ilişkin olarak bkz. yukarıda “4.2.2. Profilleme”.

¹⁶⁰ Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 22/2.a.

nesnelerin internetinin “her şeyin interneti”ne dönüşerek, 2020'ye kadar 37 milyar akıllı cihazın internete bağlanacağını öngörmektedir¹⁶¹. 2012 yılında 2000 yılına nazaran on iki kat artan bir internet trafiğinden ve 2016 yılında ise 2015 yılına kıyasla iki kat artmış olan bir mobil veri trafiğinden bahsedilmektedir¹⁶². Gerçek zamanlı veya yakın zamanlı olarak elde edilen verileri işlemek için geliştirilen yüksek performanslı büyük veri uygulamalarının, düşük maliyetli hale getirilmeye çalıştığı belirtilmiştir. Bu noktada yakın gelecekte gündelik hayata entegre olacak olan akıllı cihazların sayısı arttıkça, kullanıcı taleplerini karşılayabilmek için cihazlar arası iletişim ve veri akışları sözleşmenin ifası kapsamında değerlendirilebilecektir.

4.3.2.3. Kişisel Verinin İlgili Kişi Tarafından Alenileştirilmesi

Kişisel verilerin ilgili kişinin kendisi tarafından alenileştirilmiş olması hukuka uygunluk sebebi ile hukuka ve dürüstlük kurallarına uygun olma ve amaçla bağlantılı olma genel ilkeleri yakın ilişki içerisinde düşünülmelidir. Veri sorumlusu yahut veri işleyenin ilgili kişi tarafından kişisel verinin alenileştirilme sebebini makul düzeyde araştırması gerekmektedir. Söz konusu hukuka uygunluk sebebinin amaçla bağlantılılık ilkesinden ayrı düşünülmesi ilgili kişinin aleyhine sonuç doğurabilmektedir. Kabul etmek gerekir ki ilgili kişinin kişisel verilerini alenileştirmesindeki amaç her zaman kolay belirlenebilir olmayabilir. Bu konuda İtalya veri koruma otoritesi, internette kolayca bulunabilecek olan ya da kurumsal internet sitelerinde yer alan kişilere ait elektronik posta adreslerinin pazarlama amaçlı iletişim için kullanılarak reklam iletilmesinin amaçla bağlantılılık ilkesi ile bağdaşmayacağını belirtmektedir¹⁶³. Örnek olarak ise bir üniversitenin internet

¹⁶¹ Dave Evans, “How the Internet of Everything Will Change the World for the Better #IoE [Infographic]”, **Cisco Blogs**, 7 Kasım 2012, (Çevrimiçi) <https://blogs.cisco.com/digital/how-the-internet-of-everything-will-change-the-worldfor-the-better-infographic> , 18 Nisan 2018.

¹⁶² Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021, White Paper, 28 Mart 2017, (Çevrimiçi) <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html> , 18 Nisan 2018.

¹⁶³ Maria Roberta Perugini, “Personal Data Made Public by the ‘Data Subject’ and Use Of Information Published On Social Networks: Early Observations Of GDPR Art. 9, Para. 2, Letter E”, 31 Ekim 2016, s. 52. (Çevrimiçi) <http://europriacy.info/2016/10/31/italiano-dati-personali-resi-manifestamente-pubblici-dallinteressato-e-uso-di-dati-pubblicati-su-social-network-prime-osservazioni-allart-9-co-2-lett-e-gdp/>, 4 Nisan 2018.

sitesinde yer alan akademik personelin iletişim bilgilerinin sadece kurumsal ve akademik amaçlı iletişim için kullanılabileceği belirtilmektedir.

Özellikle sosyal medya uygulamaları aracılığı herkeşe açık olarak bireyler tarafından paylaşılan veriler büyük veri uygulamalarına katıldıkları için söz konusu istisna önem teşkil etmektedir. Kişisel Verileri Koruma Kurumu¹⁶⁴ tarafından hazırlanan yayında, kişinin herkesin erişimine açık bir şekilde sosyal medya hesabında kişisel verisini paylaşması alenileştirme olarak kabul edilmektedir. Ancak bu örneklemenin yerinde olabilmesi için kişinin herkeşe açık olarak paylaşmış olduğu kişisel verileri, ne amaçla paylaşmış olduğunun incelenmesi gerekmektedir. Kişisel Verilerin Korunması Kanunu'nun tasarı metninde düşülen muhalefet şerhinde¹⁶⁵ söz konusu hukuka uygunluk sebebi, alenileştirme kavramının belirsiz olması sebebi ile eleştirilmiştir. Sosyal medyada birtakım bilgilerini paylaşan kişi ya da bir konferansta fikirlerini belirli bir grupla paylaşan kişinin bu bilgileri alenileştirmiş sayılıp sayılmayacağının belirli olmaması ve ilgili hukuka uygunluk sebebinin Avrupa Birliği Veri Koruma Yönergesi'nde yer almaması sebebi ile tasarı metninden çıkarılması teklif edilmiştir.

İtalya veri koruma otoritesi, sosyal medya profilinde yer alan iletişim bilgilerinin de pazarlama amaçlı reklam gönderilmesi için kullanılmaması gerektiğini ifade etmektedir¹⁶⁶. Article 29 Working Party ise, kişisel verilerin bir biyografi, basılı bir yayın yahut kamuya açık bir internet sitesi üzerinden paylaşılması halinde ilgili kişinin alenileştirme niyetinin açık olduğunu belirtmektedir. Öte yandan, özellikle sosyal medya mecralarından kişisel verilerini platformun gizlilik sözleşmesini kabul ederek paylaşan kişilerin niyetleri hakkında ise karar vermenin güç olduğunu ifade etmiştir¹⁶⁷.

Bu doğrultuda ilgili kişi tarafından alenileştirilmiş olması sebebine dayanarak yürütülecek kişisel veri işleme faaliyetleri bakımından, ilgili kişinin söz konusu kişisel

¹⁶⁴ Kişisel Verileri Korunma Kurumu, “Kişisel Verilerin Korunması Kanunu ve Uygulanması”, s. 26.

¹⁶⁵ “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 83-84.

¹⁶⁶ İtalyan veri Koruma Otoritesi, Tanıtım Faaliyetleri Ve Spam Hakkında Uygulamalara İlişkin Rehber (Linee guida in materia di attività promozionale e contrasto allo spam), 4 Temmuz 2013, par. 6.1, (Çevrimiçi) (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2542348>), 22 Mart 2018.

¹⁶⁷ Article 29 Working Party, “Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)”, WP 258, Görüş, 29 Kasım 2017, s. 10.

verileri alenileştirme bağlamı ve amacı göz önünde bulundurularak bir değerlendirme yapılması gerekmektedir. Bağlamın önemine istinaden örnek olarak bir kişinin hem Facebook hem de LinkedIn profili üzerinden herkese açık bir şekilde meslek durumunu “belirli bir şirkette çalışıyor” şeklinde düzenlediğini varsayalım. Bu doğrultuda kişinin belirli bir şirkette çalıştığına ilişkin söz konusu veri Facebook ile paylaşılırken, platformun niteliği itibarı ile o iş yerinde çalışan kişilerle iletişim kurmak, arkadaş olmak yönünde bir irade bulunduğunun kabulü gerekmektedir. Ancak LinkedIn üzerinden söz konusu verinin paylaşılması bir iş tecrübesinin paylaşılması olarak nitelendirilebilecektir. Bu doğrultuda söz konusu veri kişiye yeni iş tekliflerin iletilmesi amacı ile kullanılabilir. İlgili kişinin söz konusu kişisel verilerini bilerek ve isteyerek kamu ile paylaşmış olması gerekmektedir¹⁶⁸.

Büyük veri uygulamaları bakımından kişisel verilerin toplandığı en önemli kaynaklardan biri de kamuya açıklanmış bir başka deyişle ilgili kişi tarafından alenileştirilmiş kişisel verilerdir. Günümüzde sosyal medya platformları üzerinden kullanıcıların sıklıkla “herkese açık” olarak paylaşımlarının bu kapsamda değerlendirilip değerlendirilemeyeceği tartışmalıdır¹⁶⁹. Yargıtay 12. Ceza Dairesi, herkese açık olarak paylaşılmış bir profil fotoğrafının üçüncü bir kişi tarafından kullanılmasına ilişkin şikâyet kapsamında, Facebook profil resminin ilgili kişi tarafından başkalarınca görülmesi ve bilinmesi istenmeyen, hukuk tarafından gizliliği ve korunması temel bir şahsiyet hakkı kabul edilmiş özel yaşam alanına ilişkin görüntü olarak değerlendirmemiştir¹⁷⁰. Ancak yine Yargıtay 12. Ceza Dairesi bir başka olayda, herkese açık olan profil fotoğrafının alınarak başka bir profilde paylaşılmasında hukuka uygunluk nedenlerinin bulunmamasından dolayı verileri hukuka aykırı olarak verme veya ele geçirme suçunun oluştuğuna kanaat getirmiştir¹⁷¹.

¹⁶⁸ Yücedağ, **a.g.e.**, s. 779.

¹⁶⁹ Türkiye’de sosyal medya platformlarında bireylerin paylaşımlarına ilişkin gizlilik tercihlerine ilişkin örnek çalışma için bkz. Özgür Külcü ve Türkay Henkoğlu, “Sosyal Paylaşım Ağlarında Gizlilik: Facebook İncelemesi”, **Bilgi Dünyası**, Cilt 15, Sayı 2, 2014, s. 231-252.

¹⁷⁰ Yargıtay 12. Ceza Dairesi, Esas Sayısı: 2014/4081, Karar sayısı: 2014/19490, Karar tarihi: 13 Ekim 2014.

¹⁷¹ Yargıtay 12. Ceza Dairesi, Esas Sayısı: 2016/9759, Karar sayısı: 2017/10938, Karar tarihi: 26 Aralık 2017.

Büyük veri uygulamaları tarafından özellikle internet ortamında bireylerin herkese açık paylaşmış olduğu veriler, algoritmaları besleyen bir kaynak olarak kullanılmaktadır. Örneğin; bu durum Facebook Gizlilik Politikası'nda yer almaktadır. Facebook Gizlilik Politikası'nda, herkese açık, herkesle paylaşılan bilgilerin veya bir Facebook sayfasında ya da herkese açık başka bir forumda paylaşılan içeriklerin internet arama motorları, uygulama sağlayıcılar ve internet dışı televizyon gibi kanallara açık ve bu kanallar aracılığıyla görülebilir veya erişilebilir olduğu belirtilmektedir¹⁷².

İlgili kişi tarafından alenileştirilerek herkese açık olarak paylaşılan verilerin büyük veri uygulamaları ile pazarlama, bankacılık, güvenlik ve sigorta alanlarında sıklıkla kullanıldığı bilinmektedir. Evrensel olarak bilgi güvenliği sorunlarının tartışıldığı RSA Konferansları kapsamında 2012 yılında konuşmacı olarak davet edilen Microsoft kurumsal ilişkiler başkan yardımcısı Scott Charney tarafından büyük veri uygulamalarının sektörel kullanımları hakkında çarpıcı örnekler sunulmuştur¹⁷³. Charney, voleybol maçı sırasında fotoğrafı çekilen ve sosyal medya üzerinden paylaşılan kişiye ait fotoğrafın sigorta şirketi tarafından primleri artırmak için kullanılıp kullanılamayacağına ilişkin tartışmaları konuşmasına taşırken bu konuda faaliyet gösteren şirketlerin bulunduğuna ilişkin haberlere dikkat çekmiştir¹⁷⁴. Benzer büyük veri uygulamalarının bankalar ve kredi derecelendirme şirketleri tarafından da yürütüldüğü çeşitli haberlere konu olmaktadır¹⁷⁵. Kredilendirmenin yanı sıra finans kuruluşları tarafından müşterilerinin beklentileri, zevkleri ve tercihlerinin anlaşılacak

¹⁷²Facebook, Veri İlkesi, "Bu Bilgiler Nasıl Paylaşılır?", 29 Eylül 2016, (Çevrimiçi) <https://www.facebook.com/privacy/explanation>, 8 Nisan 2018.

¹⁷³ Matthew Smith, Benjamin Henne, Christian Szongott ve Gabriele von Voigt, "**Big data privacy issues in public social media**". 2012 6th IEEE International Conference on Digital Ecosystems Technologies, Haziran 2012, s. 1.

¹⁷⁴ "Are insurance companies spying on your Facebook page?" 7 Kasım 2011, (Çevrimiçi) <http://abc7.com/archive/8422388/>, 8 Nisan 2018.

¹⁷⁵ Stephanie Armour, "**Regulators Have Concerns About Lenders' Use of Facebook, Other Sites**", 08 Ocak 2014, (Çevrimiçi) <https://www.wsj.com/articles/borrowers-hit-socialmedia-hurdles-1389224469?tesla=y>, 08 Nisan 2018.

ürün geliştirilmesi bakımından veri kaynağı sosyal medya olan büyük veri uygulamaları kullanılmaktadır¹⁷⁶.

Belirtilen örneklerden yola çıkarak kişisel verilerin korunması hukuku kapsamında büyük veri uygulamalarının yürütmüş olduğu kişisel veri işleme faaliyetleri bakımından ikili bir ayrım üzerinden değerlendirme yapılabilecektir. Bu doğrultuda ilk olarak söz konusu uygulamaların kişisel verileri elde etme faaliyeti bir veri işleme, elde edilen veriler üzerinde yürütülen faaliyetler ise ikinci bir veri işleme faaliyeti olarak değerlendirmeye konu edilmelidir. Kişinin paylaşımlarını herkese açık yapması ile bu bilgilerin herkes tarafından erişilebileceğini öngörmesi beklenebilecekken bu verilere erişen kişilerin daha sonraki veri işleme faaliyetleri günümüz teknolojisi itibari ile kişi öngörüsünü aşabilecektir. Bu bakımdan her ne kadar ilgili kişi tarafından alenileştirilmiş bir kişisel veri olsa da büyük veri uygulamaları bakımından bu kişisel veriler üzerinde yürütülecek veri işleme faaliyetleri için diğer hukuka uygunluk sebeplerinin aranması gerekmektedir¹⁷⁷.

Article 29 Working Party, kişinin sosyal medya platformları ile alenileştirmiş olduğu kişisel verisinin, alenileştirme amacının saptanmasının güçlüğüne dikkat çekmektedir. İtalyan Veri Koruma Otoritesi ise konuya ilişkin yayınlamış olduğu rehber kapsamında sosyal medya aracılığı ile herkese açık olarak paylaşılan kişisel verilerin sınırsız şekilde kullanılmaması gerektiğini ifade etmektedir¹⁷⁸. Birleşik Krallık veri koruma otoritesi tarafından ise, ilgili kişiye ait kişisel verilerinin herkes tarafından görülebilecek olmasının, söz konusu verilerin herkes tarafından sınırsız olarak herhangi bir amaç doğrultusunda kullanılabileceği başka bir deyişle erişimi olan

¹⁷⁶ Billie Anderson ve J. Michael Hardin, “Credit Scoring in the Age of Big Data” **Encyclopedia of Business Analytics and Optimization**, ed. John Wang, IGI Global, Hershey Pennsylvania, 2014, s. 550-552.

¹⁷⁷ Joint Committee Discussion Paper, par. 24, (Çevrimiçi) https://esas-joint-committee.europa.eu/publications/discussion%20paper/jc-2016-86_discussion_paper_big_data.pdf , 4 Nisan 2018.

¹⁷⁸ Garante per la protezione dei dati personali, Tanıtım Faaliyetleri ve Spam Hakkında Uygulamalara İlişkin Rehber (Linee guida in materia di attività promozionale e contrasto allo spam), 4 Temmuz 2013, par. 6.1, (Çevrimiçi) (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2542348>), 22 Mart 2018.

herkesin herhangi bir amaçla söz konusu verileri işleme hakkına sahip olduğu anlamına gelmeyeceği belirtilmektedir¹⁷⁹.

4.3.2.4. Veri Sorumlusunun Üstün Meşru Menfaati

Büyük veri uygulamaları kapsamında yürütülen kişisel veri işleme faaliyetleri için sıklıkla dayanak olarak gösterilen veri sorumlusunun meşru menfaati hukuka uygunluk sebebi doktrinde pek çok tartışmaya konu olmaktadır¹⁸⁰. İkinci ve üçüncü bölümde detaylı olarak değinilen, veri sorumlusunun meşru menfaati hukuka uygunluk sebebine dayanarak yürütülecek olan veri işleme faaliyetleri kapsamında ilgili kişinin temel hak ve özgürlükleri bakımından bir menfaat dengesinin her zaman aranması gerekmektedir. Bahsedilen menfaat dengesinin araştırılması, her bir büyük veri uygulaması özelinde ve işlenen veri kategorisi göz önünde bulundurularak, son derece hassas bir şekilde yapılmalıdır. Nitekim işlenen yahut işlenecek olan kişisel veri niteliği itibari ile ilgili kişinin kişilik hakkının özüne yaklaştığı derece ve ölçüde veri sorumlusunun söz konusu veriyi işlemekle elde edeceği menfaat aranmalıdır¹⁸¹.

Şirketler; pazarlama, dolandırıcılığın önlenmesi, hizmetlerin suistimal edilmesinin önlenmesi, fiziksel ya da bilgi teknolojileri güvenliğinin sağlanması amacı ile büyük veri uygulamalarına başvurabilmektedirler. Ancak sayılan bu amaçların meşru bir menfaat olması tek başına yeterli değildir. Veri sorumlusu, bu uygulamalar kapsamında kişisel verilerin işlenmesi faaliyetini yürütebilmeleri için gereklilik unsuruna kaynaklık teşkil edecek gerekçelerini ispat etmelidir. Bu doğrultuda büyük veri uygulamalarının potansiyel bir menfaat için kullanılması yahut söz konusu

¹⁷⁹ Information Commissioner Office, “Big data, artificial intelligence, machine learning and data protection”, par. 64.

¹⁸⁰ Otomatik veri işleme ve profillemeye dayanan büyük veri uygulamaları bakımından veri sorumlusunun sadece meşru menfaatini ortaya koymasının ilgili hukuka uygunluk nedenine dayanmak için yeterli olmadığı, veri sorumlusunun ayrıca ilgili kişinin çıkarları veya temel hak ve özgürlüklerinin de zarar görmediğini ispat edip bir denge testi yapması gerektiği Article 29 Working Party tarafından hazırlanan rehberde belirtilmiştir. İlgili rehber için bkz. Article 29 Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”.

¹⁸¹ Çekin, **a.g.e.**, s. 8.

menfaatin kişisel verileri işlemekten de elde edilmesinin mümkün olması halinde ilgili hukuka uygunluk sebebi dayanak olarak gösterilemeyecektir¹⁸².

Açık rızanın bir alternatifi olarak büyük veri uygulamalarını yürüten şirketlerin kişisel veri işleme faaliyetlerini meşrulaştırmak amacı ile sıklıkla başvurdukları bir hukuka uygunluk sebebi olan meşru menfaat, esasen veri sorumlularına büyük bir sorumluluk getirmektedir. İlgili kişinin açık rızasına dayanarak yürütülen veri işleme faaliyetlerinde veri sorumlusunun yükümlülüğü temel ilkelere uyumun sürdürülmesi ile sınırlı iken meşru menfaat hukuka uygunluk sebebine dayanarak kişisel verileri işleyen büyük veri uygulamalarının, ilgili kişinin hak ve çıkarlarına ilişkin olarak yürütmüş olduğu faaliyet ve elde etmiş olduğu menfaat bakımından sürekli olarak bir değerlendirme yapması gerekmektedir.

Belirtilmelidir ki Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında ilgili kişiye, veri sorumlusundan kişisel verilerini işleme faaliyetini kısıtlama veya askıya alma talep hakkı tanınmıştır(m. 18/1.d). İlgili madde uyarınca; bireylerin, veri sorumlusunun meşru gerekçelerinin kendi gereklerine ağır basıp basmadığı kesinleşene kadar veri işleme faaliyetine itiraz etme hakkı olduğu belirtilmektedir. Bu hakkın büyük veri uygulamaları arasında önemli bir yer ihtiva eden profillemeye ve otomatik veri işleme faaliyetleri bakımından da uygulama alanı bulacağına kabulü gerekmektedir. Avrupa Birliği Genel Veri Koruma Tüzüğü ile profillemeye de dâhil olmak üzere kişisel verilerin, veri sorumlusunun meşru menfaatine dayanılarak işlenmesi haline özel olarak ilgili kişiye tanınmış olan itiraz etme hakkı söz konusu hukuka uygunluk sebebini rıza gerekliliğine yaklaştırmaktadır. Bu düzenleme özellikle doğrudan pazarlama faaliyetleri bakımından önem taşımaktadır. Türkiye’de ise kişisel verilerin pazarlama amaçlı işlenmesinin veri sorumlusunun meşru menfaati kapsamında değerlendirilip değerlendirilemeyeceğine ilişkin açık bir düzenleme yer almamaktadır. Ancak Avrupa Birliği Veri Koruma Tüzüğü giriş bölümünde kişisel verilerin doğrudan pazarlama amacı ile işlenmesi hallerinin meşru menfaat kapsamında değerlendirilebileceği belirtilmiştir¹⁸³.

¹⁸² Information Commissioner Office, **a.g.e.**, par. 67.

¹⁸³ Avrupa Birliği Genel Veri Koruma Tüzüğü, Giriş par. 47.

Büyük veri uygulamalarından profillemeye dayalı çevrimiçi davranışsal reklamcılık faaliyetlerinin veri sorumlusunun meşru menfaati doğrultusunda gerçekleştirilip gerçekleştirilemeyeceğinin değerlendirilmesi gerekmektedir. Avrupa Birliği Genel Veri Koruma Tüzüğü'nde açıkça doğrudan pazarlama kapsamında yürütülen kişisel veri işleme faaliyetlerinin veri sorumlusunun meşru menfaati olarak değerlendirilebileceği belirtilmektedir. Ancak çevrimiçi izleme ve büyük ölçüde ve çeşitli veri toplayarak kişinin ilgi alanlarına göre reklam segmenti oluşturan uygulamalar için bir açıklık bulunmamaktadır. Belirtmek gerekir ki çevrimiçi davranışsal reklamcılık faaliyetleri sadece pazarlama yahut bir ürün gösterme olarak düşünülmemelidir. Çevrimiçi davranışsal reklamcılık faaliyetlerini yürüten büyük veri uygulamaları, bireylerin internet kullanımlarını izleyerek pek çok yerden veri almakta ve profillemeye faaliyeti yürütmektedir.

Bireylerin internet faaliyetlerinin, takip edilerek ilgi alanlarına yönelik olarak hedefli bir başka deyişle özelleştirilmiş reklamların çeşitli araç ve platformlar aracılığı ile gösterilmesini sağlayan çevrimiçi davranışsal reklamcılık uygulamalarının ekonomik bir yarar taşıdığı kişisel verilerin korunmasına ilişkin çalışmalar yürüten kurumlar tarafından da vurgulanmaktadır¹⁸⁴. Temel olarak iki önemli ekonomik fayda yaratmaktadır; ilk olarak çevrimiçi davranışsal reklamcılık uygulamaları, potansiyel alıcıları belirlemek ve sınıflandırmak üzere çalıştıkları için reklam verenler bakımından bir tasarruf imkânı sağlamaktadır. İkincil olarak ise sadece tercihlerine uygun ürün ve hizmetlere ilişkin iletiler alan tüketiciler, ilgi alanları dışındaki ürün ve hizmetlere dair alakasız içeriklerden korunmakta ve zaman kaybetmemektedirler¹⁸⁵. Ekonomik bir önem ihtiva eden çevrimiçi davranışsal reklamcılık uygulamalarının bu özelliği yadsınamayacak olsa da kişisel verilerin korunmasına ilişkin olarak “veri sorumlusunun meşru menfaati” hukuka uygunluk sebebi altında değerlendirilemeyeceğine ilişkin eleştiriler mevcuttur. Bu eleştiriler, çevrimiçi davranışsal reklamcılık uygulamalarını yürüten şirketlerin menfaatlerini kabul etmekle birlikte, bu faaliyetlerin bireylerin temel hak ve özgürlüklerine ve çıkarlarına

¹⁸⁴ Article 29 Working Party, “Opinion 2/2010 on online behavioural advertising”, WP171, Görüş, 22 Haziran 2010, s.3.

¹⁸⁵ David S. Evans “The Online Advertising Industry: Economics, Evolution and Privacy” **Journal of Economic Perspectives**, Cilt 23, Sayı 3, 2009, s.37.

etkisine odaklanmaktadır¹⁸⁶. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün kabulünden önce yayınlanmış olan Article 29 Working Party görüşünde, pek çok farklı kaynaktan toplanan veriler doğrultusunda ilgili kişiye, kendisine özel kampanya ya da teklif oluşturulmasına ilişkin hedefleme faaliyetlerinin veri sorumlusunun meşru menfaati kapsamında değerlendirilemeyeceği belirtilmiştir¹⁸⁷.

Avrupa Veri Koruma Denetmeni ise büyük veri uygulamaları bakımından veri sorumlusunun meşru menfaati ve ilgili kişinin temel hak ve özgürlüklerine ilişkin dengenin sağlanmasının güç olduğunu belirtmiştir¹⁸⁸.

4.3.3. Büyük Veri Uygulamalarına Getirilen Düzenlemeler

Büyük veri uygulamaları bakımından kişisel verilerin korunması hukuku kapsamında yaşanan sorunlar, büyük ölçüde büyük verinin hacim, çeşitlilik ve hız özelliklerinden kaynaklanmaktadır. Ancak kişisel verilerin korunması hukuku bakımından esas sorun ise kişisel verilerin korunması alanında belirlenmiş olan genel ilkeler çerçevesinde günümüzde hızla gelişen teknolojiler ve getirdiği ekonomik yarar ile bireylerin menfaatlerinin dengelenmesi konusudur. Bu noktada günümüzdeki hâkim veri koruma ilkeleri ve kişisel verilerin korunmasına ilişkin olarak oluşturulmuş hukukun, fiziksel dünyanın özelliklerinden kaynaklanan analog verilere dayandığının kabulü gerekmektedir. Günümüzde ise dijitale aktarılacak çeşitlenen veri kaynakları ve işleme gücü büyük veri sorununu yaratmaktadır¹⁸⁹. Büyük veriyle ilgili endişeler, toplanan verilerin miktarındaki önemli artışlara ve büyük veri uygulamaları bakımından öngörülemeyen, çeşitli ve belirsiz veri işleme amaçlarına odaklanmaktadır. Yukarıda da anlatılmış olduğu üzere veri koruma hukukunun genel ilkeleri ile büyük veri uygulamalarını uzlaştırmak pek kolay olmamaktadır. Bu nedenle Avrupa Birliği veri

¹⁸⁶ Article 29 Working Party, “Online Behavioural Advertising: Industry Proposed Solutions Inadequate”, Basın Açıklaması, Brüksel, 15 Aralık 2011 (Çevrimiçi) http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2011/20111215_press_release_oba_final.pdf, 22 Mart 2018, s.1.

¹⁸⁷ Article 29 Working Party, “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”, s. 32, 62.

¹⁸⁸ Avrupa Veri Koruma Denetmeni, “Meeting the challenges of big data”, Sayı 7/2015, 19 Kasım 2015, (Çevrimiçi) https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf, 8 Nisan 2018.

¹⁸⁹ Büyük verinin sunmuş olduğu yararlar karşısında yaratmış olduğu etik problemler ve hukuki boyutuna ilişkin bir değerlendirme için bkz. Mehmet Bedii Kaya, **a.g.e.**, s. 182.

koruma hukuku çerçevesinde Mayıs 2018’de uygulamaya girmiş olan Avrupa Birliği Genel Veri Koruma Tüzüğü çerçevesinde teknolojik gelişmeler göz önünde bulundurulmaya çalışılmıştır. Kişisel verilerin korunmasına ilişkin düzenleme yaparken ne yazık ki Türk kanun koyucusu ise Tüzük’ün geçersiz kılacağı Avrupa Birliği Veri Koruma Yönergesi’ni temel almıştır. Getirilen düzenlemenin uygulamada somut olaylar bakımından değerlendirileceği ve temel kuralların uygulanmasına ilişkin olarak ilerleyen süreçte sektörel düzenlemelere yer verileceği öğretilde belirtilmektedir¹⁹⁰.

Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında büyük veri uygulamaları bakımından doğrudan uygulama alanı bulabilecek olan “hesap verilebilirlik”¹⁹¹, “veri koruma etki analizi ve ön değerlendirme”¹⁹², “tasarımdan itibaren ve varsayılan ayarlar veri koruması” gibi yeni yükümlülükler yer almaktadır. Teknolojinin gelişmesi ile beraber, veri sorumlularına gelişen teknolojileri ürünleştirirken veri koruma ilkelerini göz önünde bulundurma zorunluluğu getirilmiştir. Erken aşamalardan itibaren veri korumaya ilişkin güvencelerin sağlanmasına ilişkin bu düzenlemeler hukuk ile teknik ve teknolojinin kaynaşması bakımından önem arz etmektedir. Avrupa Birliği Genel Veri Koruma Tüzüğü ile getirilen yenilikler ve düzenlemeler, geleneksel veri işleme metotlarının yanı sıra büyük veri uygulamalarına da uygulanabilir bir yaklaşım ortaya çıkarmaktadır¹⁹³. Getirilen yeni yaklaşımlar geleneksel hukuk düzeninin temel işleme prensibi olarak, meydana gelen olumsuz sonuca ilişkin olarak telafi imkânlarının sunulması anlayışından ziyade, ihlalin oluşumunu baştan önlemeyi hedeflemektedir¹⁹⁴. Kişisel verilerin korunması

¹⁹⁰ Kişisel Verilerin Korunması Kanunu kapsamında benimsenen sisteme ilişkin açıklama ve görüş için bkz. Elif Küzeci, **Kişisel Verilerin Korunması**, yenilenmiş ve gözden geçirilmiş 2. Baskı, Ankara, Turhan Kitabevi, 2018, s. 314-318.

¹⁹¹ İngilizce Orijinal metinde “accountability” olarak yer almaktadır, bkz. Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 5(2).

¹⁹² İngilizce Orijinal metinde “Data protection impact assessment and prior consultation” olarak yer almaktadır bkz. Avrupa Birliği Genel Veri Koruma Tüzüğü, m. 35, 36.

¹⁹³ Schönberger, Padova, **a.g.e.**, s. 335.

¹⁹⁴ Çekin, **a.g.e.**, s. 12.

ilkelerinin bir yükümlölükten ziyade bir kültür haline getirilmesini amaçlayan bu düzenlemelere Türk hukuku bakımından yer verilmemiş olması eleştirilmektedir¹⁹⁵.

4.3.3.1. Veri Koruma Etki Analizi ve Ön Değerlendirme

Avrupa Birliğı Genel Veri Koruma Tüzüğü ile veri sorumlularına kendilerini değerlendirme ve denetleme yükümlölüğü getirilmiştir. Günümüzde teknolojinin artan hızı karşısında hukuk düzenlemeleri geride kalabilmektedir. Bu nedenle gelişen teknoloji karşısında her daim uygulanabilir düzenlemeler yapmak yerinde olmaktadır. Bununla birlikte ayrıntılı düzenlemeler ve kesin kurallar getirmek de günümüz şartlarında etkili olmayan ve teknolojiyi engelleyen bir yaklaşım barındırmaktadır. Bu bakımdan Avrupa Birliğı Genel Veri Koruma Tüzüğü kapsamında veri sorumlularına getirilmiş olan kişisel verilerin işlenmesinden doğan tehlikeleri tespit etme ve bunları önlemek adına gerekli yöntemleri belirleme yükümlölüğü hukuk ile teknolojinin uzlaştırılması bakımından oldukça önemlidir. Sorumluluk ve hesapverilebilirlik ilkesinin bir görünümü olan bu yükümlölük kapsamında veri sorumlusu kişisel verilere ilişkin olarak bireyler nazarında oluşabilecek tehlikeleri henüz ortaya çıkmadan önlenmesi için uygun tedbirleri belirleme ve uygulama yükümlüğü altındadır¹⁹⁶.

Avrupa Birliğı Genel Veri Koruma Tüzüğü kapsamında özellikle yeni teknolojiler kullanan işletmeler bakımından yürütülecek olan veri işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir risk alanı oluşturmasının muhtemel olduğu hallerde veri sorumluları veri koruması etki analizi yapmakla yükümlü kılınmıştır. Tüzük kapsamında ayrıca özellikle veri koruması etki analizi yapmakla yükümlü olanlar belirtilmiştir. Profillemeye de dâhil olmak üzere otomatik işlemeye dayanan ve gerçek kişilere ilişkin hukuki ya da ciddi derecede etkisi bulunan sistematik ve kapsamlı veri işleme faaliyetleri yürüten veri sorumluları yükümlüler arasında sayılmıştır. Bu ifade itibari ile özellikle profillemeye ve otomatik karar mekanizmalarına ilişkin yürütülen büyük veri uygulamalarının bu kapsamda değerlendirileceğı açıktır¹⁹⁷. Günümüzde özellikle kişisel verilerin kümeler halinde ve

¹⁹⁵ Küzeci, **a.g.e.**, s. 319.

¹⁹⁶ Çekin, **a.g.e.**, s. 116.

¹⁹⁷ Information Commissioner Office, “Big data, artificial intelligence, machine learning and data protection”, par. 159.

öngörülemeyen sonuçlar üretecek şekilde algoritmalar tarafından işlenmesi artık sadece bir mahremiyet sorunu teşkil etmemektedir. Büyük veri uygulamaları bakımından oluşturulan özellikle profillemeye ilişkin sonuçlar kişiler nezdinde sosyal, ekonomik ve manevi açıdan riskler yaratmaktadır. Bu bakımdan büyük veri uygulamalarını hayata geçirmeden önce yapılacak olan veri koruma etki analizi bireyler aleyhine oluşabilecek sonuçları öngörerek önlem alabilmek adına büyük önem taşımaktadır. Büyük veri uygulamaları bakımından genellikle büyük veri ekibi tarafından faaliyetin etik değerlendirme kapsamında analiz edildiği argümanı ileri sürülmektedir. Ancak Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında veri koruma etki analizi bir yükümlülük olarak getirilmiş olup içeriği düzenlenmiştir ve sadece etik konuları içermemektedir. Yapılacak olan büyük veri uygulamasının veri koruma hukukunun genel ilkeleri ve faaliyet kapsamında yer alan amaçlarının hukuka uygunluk nedenleri kapsamında analiz edilmesi hedeflenmektedir. Bu bakımdan büyük veri uygulamaları kapsamında veri koruma etki analizi yapılmasının gerekli olup olmadığına ilişkin olarak üç soru ortaya atılmıştır¹⁹⁸:

- i. Büyük veri uygulaması kapsamında kullanılan kişisel veriler elde edilme amacından farklı bir amaç ve yolla kullanılmakta mıdır?
- ii. Büyük veri uygulaması kapsamında özel hayatın gizliliğine etki edebilecek yeni bir teknoloji kullanılmakta mıdır?
- iii. Büyük veri uygulaması neticesinde verilen bireylere ilişkin kararlar ya da atılan adımlar bireyleri ciddi ölçüde etkilemekte midir?

Belirtmek gerekir ki söz konusu soruların cevabını büyük veri uygulamalarına ilişkin projelerin başlangıç aşamasında vermek güç olabilmektedir. Nitekim büyük veri uygulamalarında yer alan algoritmalar, veri setleri arasında beklenmedik bağlantılar kurarak sonuçlar çıkarabilmektedir. Bu bakımdan Birleşik Krallık veri koruma otoritesi soruların cevaplanamaması yahut emin olunamaması halinde her halükârda analize başlanması gerektiğini ifade etmiştir¹⁹⁹. Büyük veri uygulamaları bakımından

¹⁹⁸ Information Commissioner Office, “Big data, artificial intelligence, machine learning and data protection”, s. 101.

¹⁹⁹ a.e., s. 102.

kişisel verilerin korunması adına makul önlem ve adımların atılması adına söz konusu risk analizinin yapılması önerilmektedir²⁰⁰.

Tüzük kapsamında analize esas alınacak olan hususlar ile asgari içerik belirlenmiştir. Bu doğrultuda denetleme kurumuna sunulacak olan veri koruma etki analizi raporu asgari olarak aşağıdaki hususları içermelidir:

- i. Uygulama kapsamında öngörülen işleme faaliyetleri ve işleme amaçlarına ilişkin sistematik bir açıklama,
- ii. Kişisel veri işleme faaliyetlerinin amaçla bağlantılı olarak gerekliliği ve orantılılığına yönelik bir analiz,
- iii. İlgili kişilerin temel hak ve özgürlüklerine ilişkin bir risk analizi,
- iv. İlgili kişilerin ve diğer kişilerin hakları ve meşru menfaatleri dikkate alınarak, kişisel verilerin korunmasının sağlanması ve Tüzük'e uygun hareket edildiğinin gösterilmesiyle ilgili güvenceler, güvenlik tedbirleri ve mekanizmalar da dâhil olmak üzere risklerin ele alınması hususunda öngörülen tedbirler.

Belirtmek gerekir ki, yukarıda sayılan hususlara ek olarak, veri sorumlusunun yürüteceği faaliyet uyarınca daha başka noktalara yer vermesi gerekebilecektir. Sayılan hususların, bilhassa kişisel veri işleme faaliyetlerine ve amaçlarına ilişkin sistematik açıklamaların, veri sorumlusu ve ilgili kurumların veri işleme faaliyetinden doğabilecek risklerin öngörülmesine elverişli şekilde veri koruma etki analizi raporunda yer alması gerekmektedir. Bu bakımdan büyük veri uygulamaları kapsamında yürütülecek olan faaliyetin doğrudan bireyleri etkilemesi halinde bu faaliyetin ihtiva ettiği risk oranında analizin detaylı olması beklenecektir²⁰¹.

Veri koruma etki analizi raporu sonucunda yürütülecek olan veri işleme faaliyetinin önemli risklere yol açacağının ortaya konması halinde veri sorumlusunun faaliyetine başlamadan önce denetim makamının görüşüne başvurması yükümlülüğü ayrıca Tüzük'te ön değerlendirme başlığı altında düzenlenmiştir. Ön değerlendirme'ye

²⁰⁰ Office of the Australian Information Commissioner, "Guide to big data and the Australian Privacy Principles", Mayıs 2016, s. 8.

²⁰¹ Çekin, **a.g.e.**, s. 118.

başvuran veri sorumluları, veri koruma etki analizi uyarınca ayrıca, kendisi ve kendisi ile müteselsil sorumlu olan kişileri ve veri işleyenlerin sorumlularını, planlanan işlemin amaçlarını ve vasıtalarını, öngörülen tedbir ve güvenceleri, veri koruma görevlisinin irtibat bilgilerini, veri koruma etki analizi ve denetim makamı tarafında talep edilecek diğer belgeleri sunmakla yükümlüdür.

4.3.3.2. Tasarımdan İtibaren ve Varsayılan Ayarlarla Veri Koruması

Uzunca bir süredir uygulamada veri koruma otoriteleri tarafından önerilen ve mahremiyeti teşvik eden teknolojiler²⁰² olarak desteklenen yaklaşım, “*tasarımdan itibaren ve varsayılan ayarlarla veri koruması*” yükümlülüğü olarak Avrupa Birliği Genel Veri Koruma Tüzüğü’nde yer almaktadır. Her ne kadar veri koruması ve büyük veri uygulamaları temelleri itibari ile birbirleriyle çatışan kavramlar olarak değerlendiriliyor olsa da tasarımdan itibaren ve varsayılan ayarlarla veri koruması yaklaşımı büyük veri çağında, bireyleri güçlendirerek veri sorumlularının sorumluluğunu ve güvenini destekleyen bir veri koruma enstrümanıdır²⁰³. Tasarımdan itibaren veri koruması ile, teknolojik bir uygulamanın geliştirme aşamasında veri koruma ilkelerinin göz önünde bulundurulması hedeflenmektedir. Veri koruma ilkelerinin bir sistemin kuruluş anında değerlendiriliyor olması sonraki aşamalardaki “uyumlu hale getirme” sorununu bertaraf etmektedir.

Büyük veri uygulamaları bakımından tasarımdan itibaren veri koruması yükümlülüğü, kişisel verileri varsayılan olarak koruma için gerekli kontrollerin erken uygulanmasını sağladığı için oldukça yararlı olarak değerlendirilmektedir. Ancak büyük veri kapsamında işlenmekte olan verinin büyüklüğü, çeşitliliği ve neredeyse gerçek zamanlı olarak elde edilmesi bazı zorluklar ortaya çıkmaktadır. Büyük veri uygulamaları bakımından tasarımdan itibaren veri koruması yükümlülüğünün yerine

²⁰² Orijinal kullanımı “Privacy Enhancing Technologies” (“PET”) olan ve verilerin daha ileri düzeylerde işlenmesini mümkün olduğunca aza indirmek olan teknolojik çözüm araçları anlamına gelen kavramın öğretilde “Mahremiyeti Teşvik Eden Teknolojiler” olarak tercüme edilmiştir, Çekin, **a.g.e.**, s. 12

²⁰³ Giuseppe D’ Acquisto, “Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies In The Era of Big Data Analytics”, s. 21.

getirilmesinde, kişisel veri işleme süreçlerin belirli ve açık olmaması bir başka engel olarak gösterilmektedir.

Tasarımdan itibaren veri korumanın yedi ilkedен oluştuđu ifade edilmektedir²⁰⁴:

- i. Cezalandırıcı değil önleyici olma: Yaptırım mekanizmalarından ziyade veri korumanın önleyici ve danışmanlık yanını öne çıkarmaktadır. Bu ilke uyarınca kurum içi ya da kurum dışı veri koruma görevlilerinin yeni teknolojilerin kullanıldığı proje ekiplerine tasarım aşamasında dâhil olmaları gerekmektedir.
- ii. Varsayılan veri koruma: Sağlanması gereken maksimum veri koruma yaklaşımını vurgulamaktadır. Oluşturulacak her bir sistem için kişisel veri işlemeyecek şekilde bir kurgunun temel alınması gerekmektedir. Bu ilke uyarınca ilgili kişinin sessiz kalması halinde kişisel verilerinin işlenmesine ilişkin olarak rıza vermediği kabul edilmelidir.
- iii. Veri koruma içeren tasarım: Tasarımı bütünsel olarak ele alarak her aşamasında devam eden bir veri korumanın tesisi gerekmektedir. İlke uyarınca başlangıçtan itibaren ve eklenecek olan yeni süreçlerde de devam eden şekilde tarafların çıkarlarının bütünleştirilmesi amaçlamaktadır.
- iv. Tam işlevsellik: Kişisel verilerin korunması ve veri güvenliği ikileminden arı bir şekilde veri işleme faaliyetinin bütün aktörleri için eşit ve geçerli bir korumanın tesisi amaçlanmaktadır.
- v. Uçtan uca güvenlik: Bir kurum ya da kuruluş içerisindeki kişisel verinin yaşam döngüsü kapsamında, toplamadan imha aşamasına kadar, veri koruma genel ilkeleri ile uyumlu işlenmesini ifade etmektedir. Bu ilke veri güvenliği ile ilgili olan uçtan uca şifreleme ve diğer teknolojiler ile karıştırılmamalıdır. İlke uyarınca güvenlikle beraber genel ilkelerin dikkate alınması gerekmektedir.
- vi. Görünürlük ve şeffaflık: Kişisel verilerin işlenmesinde yer alan sistemleri ve süreçleri doğrulamaya dayanmaktadır. Kurum ya da kuruluş bünyesinde gerçekleşen süreçlerin şeffaf bir şekilde yürütülmesi ve teknik sistemlerin denetime açık olması gerekmektedir.

²⁰⁴ Martin Rost, Kirsten Bock, “Privacy by Design and the New Protection Goals,” İngilizce çevirisinden yararlanılmıştır, “Privacy by Design und die Neuen Schutzziele”, **Datenschutz und Datensicherheit**, Cilt 35, Sayı 1, 2011, s. 32; Lambert, **a.g.e.**, 330.

- vii. Kullanıcı kişisel verilerine saygı: Kişisel veri işleme süreçlerinin birey merkezli olmasını ve bireye kişisel verileri üzerinde kontrol imkânı tanınmasını ifade etmektedir.

Sayılan ilkelerden de görüleceği üzere tasarımdan itibaren ve varsayılan ayarlarla veri koruması yükümlülüğü temelde veri koruma ilkelerini içermekte ve bu ilkelerin süreçlerin en başından itibaren göz önünde bulundurularak uygulanması gerekliliğini ihtiva etmektedir.

Tasarımdan itibaren ve varsayılan ayarlarla veri koruması yükümlülüğü, Avrupa Birliği Genel Veri Koruma Tüzüğü'nde de belirtilmiş olduğu üzere, anonim halde ya da psödosomasyon işlemlerine maruz bırakılmış verileri kullanma ve veri sadeleştirilmesi ilkeleri ile ilişkilidir. Ancak tasarımdan itibaren ve varsayılan ayarlarla veri koruması yükümlülüğü daha geniş teknik gereklilikler barındırmaktadır. Bu teknikler uluslararası geçerliliği olan otoriteler tarafından tavsiye niteliğinde yayımlanan pek çok metinde örneklenmiştir²⁰⁵. Buna göre, verilerin kötüye kullanılmasının önlenmesi için erişim kontrolleri, şifreleme ve denetim kayıtları gibi güvenlik tedbirlerinin alınması; veri sadeleştirilmesinin sağlanması adına sadece gerekli olan değerlendirme ve işlemler kapsamında gerekli olduğu ölçüde verilerin işlenmesi; amaçla bağlantılılık ilkesi uyarınca veri işleme, veri saklama yöntemlerinin sınıflandırmaya dayalı olarak yapılması; bireylerin tercihlerine ve şirket kurallarına ilişkin olarak sıkı politikaların geliştirilmesi tasarımdan itibaren ve varsayılan ayarlarla veri koruması yükümlülüğüne ilişkin örnek olarak verilmektedir.

Büyük veri uygulamaları bakımından ise aşağıda açıklanan, tasarımdan itibaren ve varsayılan ayarlarla veri koruması stratejilerinin, verilerin toplanmasına ve işlenmesine yönelik olarak sistemlerin kurgu ve tasarım aşamasından itibaren göz önüne bulundurularak uygulanması gerekmektedir:

- i. Sadeleştirme: Kişisel verilerin miktarı mümkün olduğunca en düşük seviyede tutulmalıdır.

²⁰⁵ Giuseppe D' Acquistio, "Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies In The Era Of Big Data Analytics", s. 22; Information Commissioner Office, "Big data, artificial intelligence, machine learning and data protection", s. 73.

- ii. Gizleme: Kişisel veriler, herkes tarafından erişilebilir olmaması adına gizlenmelidir. Kurum içi erişim sınırlamaları getirilmelidir.
- iii. Ayırıştırma: Kişisel veriler, mümkün olduğunda ayrı bölümlerde dağıtılmış şekilde işlenmelidir.
- iv. Kümeleme: Kişisel veriler, mümkün olduğunca toplu olarak ayrıntıları ön plana çıkarılmadan işlenmelidir.
- v. Bilgilendirme: İlgili kişiler, yeterli seviyede şeffaf bir şekilde bilgilendirilmelidir.
- vi. Kontrol: Kişisel verilerin kontrolü bireylere, ilgili kişilere bırakılmalıdır.
- vii. Yürürlük: Yasal gerekliliklerle uyumlu bir gizlilik politikası yürürlükte olmalı ve uygulanmalıdır.
- viii. Hesap verilebilirlik: Veri sorumluları yürürlükteki yasalara ve gizlilik politikalarına uygun olduklarını gösterebilmelidir.

Büyük veri uygulamaları bakımından tasarım aşamasında bu yaklaşımın göz önünde bulundurularak sayılan hususların uygulanması, veri işleme aşamasında yaşanacak sorunları asgari seviyeye düşürecektir. Kişisel verilere ilişkin olarak barındırdıkları riskler göz önünde bulundurulduğunda büyük veri uygulamaları için kanuni bir zorunluluk olsun olmasın pek çok veri koruma otoritesi bu uygulamaların tasarımdan itibaren ve varsayılan ayarlarla veri koruması prensibi ile hayata geçirilmesini tavsiye etmektedir²⁰⁶. Bireylerin kendilerini güvende hissettiği ve verilerinin kontrolünü elinde bulundurduğu bir ekosistem, büyük veri uygulamaları bakımından da avantaj sağlayabilecektir.

Bununla birlikte tasarımdan itibaren ve varsayılan ayarlarla veri koruması safi veri koruma hukukundan kaynaklanan bir yükümlülük olarak düşünülmemelidir. Özellikle

²⁰⁶ Office of the Australian Information Commissioner, “Guide to big data and the Australian Privacy Principles”, Mayıs 2016, s. 9.; Ann Cavoukian, Jeff Jonas, “Privacy by Design in the Age of Big Data”, **Information and Privacy Commissioner**, Ontario, Canada, Haziran 2012, s. 12-13 (Çevrimiçi) <https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf>, 18 Nisan 2018; Fuster, Scherrer, **a.g.e.**, s. 32.

tüketicie yönelik olan ürün ve hizmetler bakımından şeffaflık ve dürüstlük sağlayan bu yükümlölük rekabet avantajını da beraberinde getirmektedir²⁰⁷.

Öte yandan yaptırma dayalı bir hukuk mekanizması yerine, veri sorumlularının kendi risk alanlarını belirleyerek veri korumayı bir kültür olarak operasyonlarının en başından itibaren içselleştirmelerini bekleyen bu tür düzenlemeler uygulamada daha rahat karşılık bulabilecektir.



²⁰⁷ Kişisel verilerin korunması konusunun yaratmış olduğı rekabet avantajına ilişkin çalışma için bkz. Alessandro Mantelero, “Competitive value of data protection: the impact of data protection regulation on online behaviour”, **International Data Privacy Law**, Cilt 3, Sayı 4, s. 229-238, 1 Kasım 2013.

SONUÇ

Sanayi 4.0'ın getirmiş olduğu teknolojilerden, büyük veri uygulamaları kapsamında yürütülen *kişisel veri işleme faaliyetlerinin barındırmış olduğu risklerin mümkün olduğunca tespit edilmesi ve bunların kişisel verilerin korunması hukuku bakımından değerlendirilmesi* işbu çalışmanın konusunu oluşturmaktadır.

Büyük veri yaratmış olduğu veri ekonomisi ile çok yönlü bir değer taşımaktadır. Öte yandan nesnelerin interneti ve yapay zekâ gibi teknolojiler geliştikçe, büyük veri, sürekli ilerleyerek bireylerin davranışsal modellerini oluşturmakta ve belirli profilleri tespit etme eğilimi geliştirmektedir. Bununla birlikte profillemeye ve otomatik karar mekanizmaları ile birlikte yürütülen davranış yönlendirme faaliyetleri kişinin kendisini geliştirme ve ifade etme olanağını kısıtlamaktadır. Belirtilmelidir ki bu uygulamaların kişiler özelinde yaratmış olduğu sorunlar güncel veri koruma hukuku ve kanun koyucuları tarafından göz ardı edilmemektedir. Beş yıllık bir çalışmanın ürün olarak Mayıs 2018'de yürürlüğe girmiş olan Avrupa Birliği Genel Veri Koruma Tüzüğü bu konudaki en güncel örnek olarak bu çalışma kapsamında ayrıntılı olarak başlı başına değerlendirilmiş, ayrıca Türk hukukunda kişisel verilerin korunması açısından temel düzenleme niteliğindeki Kişisel Verilerin Korunması Kanunu'ndaki düzenlemeler Tüzük ile karşılaştırmalı olarak incelenmiştir. Bu temel metinlerde yer alan genel ilkeler ve hukuka uygunluk sebepleri, veri sorumlusunun veri işleme faaliyetinin çerçevesini somutlaştırmak açısından ve yükümlülükleri bakımından büyük önem taşımaktadır. Bu nedenle bu çalışma kapsamında özel olarak kişisel verilerin işlenmesinde öngörülmüş olan hukuka uygunluk sebepleri ayrıca genel ilkeler ışığında da incelenmiştir. Son bölümde ise büyük veri uygulamaları açıklanan genel ilkeler ve hukuka uyumluluk sebepleri bakımından ayrıca değerlendirilmiştir.

Bu çerçevede çalışmada detaylı bir şekilde açıklanmış olan büyük veri uygulamaları bakımından ortaya çıkan sorunlar şu şekilde özetlenebilecektir:

- Temel işlevi ve hedefi veri setleri arasında ilişki kurarak yeni anlamlı sonuçlar yaratmak olan bu algoritmaların, çalışma yönteminin ve amacının açık bir şekilde verilerin toplanma anında ilgili kişiye sunulması mümkün

olmayabilmektedir. Ya da bilgilendirme metinleri bireyler için uzun ve anlaşılmaz olabilmektedir. Bu durum ise *hukuka ve dürüstlük kurallarına uygun olma ilkesi* bakımından sorun teşkil etmektedir.

- Kişilere, büyük veri uygulamalarında yer alan verileri görüntüleme ve düzeltme imkânının sunulamıyor olması ve bu verilerin bireylerin kontrolü dışında toplanması, *doğru ve gerektiğinde güncel olma ilkesinin* ihlali anlamına gelmektedir.
- *Belirli, açık ve meşru amaçlar için işleme ilkesinin*, büyük veri uygulamalarının içerdiği veriler için her an yeni bir kullanım amacı yaratabilecek algoritmalar çalıştırması sebebiyle büyük veri uygulamalarıyla bağdaştırılması zor gözükmemektedir. Avrupa Birliği Genel Veri Koruma Tüzüğü'nde yer alan verilerin toplama amacından farklı olarak başka bir amaçla işlenmesinden önce ilgili kişinin bilgilendirilerek tekrardan onayının alınmasına ilişkin düzenleme ise hayatın olağan akışına uygun olmadığı sebebi ile eleştirilmektedir.
- Büyük veri uygulamaları gerçekte ihtiyaç duydukları veriyi bulmak ve üzerinde çalışabilmek için çok fazla kaynaktan, çok fazla veriyi toplamaktadır. Bu nedenle çoğu zaman toplanma amaçlarını aşan veriler bireylerden talep edilmektedir. Bu durum ise *amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi* kapsamında bir sorun teşkil etmektedir.
- Bulut sistemler aracılığı ile veri saklama maliyetlerinin düşmesi ve dijital dünyada verinin silinmesinin güçleşmesi gerekçeleri ile büyük veri uygulamalarının verileri silmek ya da yok etmek için herhangi bir politika geliştirmemesi ve kişisel verilerin süresiz olarak saklanması *gerekli olan süre kadar muhafaza edilme ilkesi* ile bağdaşmamaktadır.
- Büyük veri uygulamaları bakımından genellikle kullanılan verilerin üçüncü taraf uygulamalardan sağlanıyor olması veya veri sorumlularının büyük veri uygulamalarında çalıştırdıkları algoritmaların çalışma prensiplerini tam olarak açıklamamaları, *uygulamaların şeffaflık ve hesap verilebilirlik ilkesi* ile ters düşmesine sebep olabilmektedir. Güçlü algoritmalar, işletmelere sunulan geniş bilgi birikimindeki değeri açığa çıkarmakta ve tüketicilerin lehine sonuçlar

üretebilmektedir. Ancak aynı zamanda otomatik karar mekanizmaları bireylere yönelik ekonomik, sosyal ve manevi açıdan ayrımcılığı gündeme getirebilmektedir.

- Belirlilik ve amaçla bağlantılı olma ilkesinin büyük veri uygulamaları bakımından kolay bir şekilde sağlanamaması sebebiyle ilgili kişinin *açık rızası* ve *sözleşmenin kurulması ya da ifası* hukuka uygunluk sebebine dayanılarak kişisel verilerin işlenmesi *tartışmalı* olarak değerlendirilmektedir.
- *İlgili kişi tarafından alenileştirilmiş olan kişisel veriler* bakımından ise ilgili kişinin alenileştirme amacının tespit edilmesinin güç olması ve büyük veri uygulamaları tarafından söz konusu açık veriler üzerinden ilgili kişinin öngöremeyeceği veri işleme faaliyetlerinin yürütülmesi hukuka ve dürüstlük kurallarına uygun ve amaçla bağlantılı olma ilkesi bakımından sorunlu görülmektedir.
- Bir tarafta ilgili kişinin başta temel hak ve özgürlükleri olmak üzere menfaati diğer tarafta ise *veri sorumlusunun meşru menfaati* arasındaki dengenin sağlanması çeşitli güçlükler barındırmaktadır. Bu bakımından her zaman için bu dengenin gözetilerek yürütülen kişisel veri işleme faaliyetinin genel ilkelere uygunluğunun denetlenmesi gerekmektedir.

Büyük veri uygulamalarının beraberinde getirdiği bu sorunlar, veri koruma hukukunun genel ilkeleri ve düzenlenen hukuka uygunluk sebepleri kapsamında gündeme gelmektedir. Çalışmada büyük veri uygulamaları sorunlarına yönelik olarak özellikle Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında doğrudan uygulama imkânı bulacak olan düzenlemeler de ayrıca açıklanmış ve değerlendirilmiştir.

Belirtmek gerekir ki günümüzde birey ve kişisel verilerin korunması odaklı yaklaşımlar getiren veri koruma hukuku düzenlemeleri, taşıdığı ekonomik değeri açık olan büyük veri uygulamaları önünde bir engel teşkil edebilmektedir. Genel ilkelerin çok sıkı yorumlanması, risk değerlendirmesi yapmaksızın *safî veri koruma odaklı bir yaklaşım bireylerin korunması bakımından da etkisiz* olabilecektir. Bu katı yaklaşım, büyük veri uygulamalarının korsan olarak artması sonucunu doğurabilecektir. Çalışmanın son bölümünde açıklandığı üzere bilhassa genel ilkeler ile büyük veri uygulamalarının çalışma prensibi arasında uzlaştırması güç bir çatışma bulunmaktadır.

Belirtmek gerekir ki kişisel verilerin korunması kapsamında bireylerin etkili bir biçimde korunması için kanun koyucuların kesin ve ayrıntılı düzenlemelerden ziyade teknolojik gelişmeleri göz önünde bulunduran ve geleceğe uygulanabilir düzenlemeleri benimsemeleri yerinde olacaktır.

Mayıs 2018’den itibaren Avrupa Birliği üye devletleri içerisinde doğrudan uygulanmaya başlayan *Avrupa Biliği Genel Veri Koruma Tüzüğü* ve Nisan 2018’de bütün hükümleri ile yürürlüğe girmiş olan *Kişisel Verilerin Korunması Kanunu* uygulaması ışığında, bu çalışma kapsamında açıklanan genel ilkeler ve hukuka uygunluk sebeplerinin büyük veri çerçevesinde nasıl yorumlanacağı ve uygulanacağı önümüzdeki dönemde veri ekonomisinin şekillenmesi sağlanacaktır.

KAYNAKÇA

I. Kitap ve Makaleler

- Akgül, Aydın: “Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi” **Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, (yayınlanmamış doktora tezi)**, Kocaeli, 2013.
- Akıncı, Ayşe Nur: **Çalışma Raporu 6**, “Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi”, Türkiye Cumhuriyeti Kalkınma Bakanlığı, Yayın No 2968, 2017.
- Aksoy, Hüseyin Can: “Kişisel Verilerin Korunması”, **Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk (Medeni Hukuk) Anabilim Dalı Yüksek Lisans Tezi**, Ankara, 2008.
- Aksu, Mustafa: **Bilgisayar Programlarının Fikri Mülkiyet Hukukunda Korunması**, İstanbul, Beta Basım Yayın Dağıtım A.Ş., 2006.
- Alsenoy, Brendan Van: “Reconciling the (extra)territorial reach of the GDPR with public international law”, **Data Protection and Privacy Under Pressure Transatlantic Tensions: EU Surveillance, and Big Data**, Editörler: Gert Vermeulen, Eva Lievens, Antwerp, Belçika, 2017.
- Anderson, Billie / Hardin, J. Michael: “Credit Scoring in the Age of Big Data”, **Encyclopedia of Business Analytics and Optimization**, Editör: John Wang, IGI Global, Hershey Pensilvanya, 2014, s. 550-552.
- Araslı, Oya: **Özel Yaşamın Gizliliği Hakkı ve TC Anayasasında Düzenlenişi**, (yayınlanmamış doçentlik tezi), Ankara Üniversitesi, Ankara, 1979.
- Ashton, Kevin: “That Internet of Things Thing”, **RFID Journal**, 22.06.2009, (Çevrimiçi) <http://www.rfidjournal.com/articles/view?4986>, 16 Nisan 2018
- Aslanyürek, Malik: “İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve

- Farkındalıkları”, **Maltepe Üniversitesi İletişim Fakültesi Dergisi**, Sayı 3, 2016, s. 80-106.
- Aybay, Rona: **Açıklamalı İnsan Hakları Evrensel Bildirisi**, Türkiye Barolar Birliği İnsan Hakları Uygulama ve Araştırma Merkezi, Türkiye Barolar Birliği Yayınları: 113, Türkiye Barolar Birliği İnsan Hakları Uygulama ve Araştırma Merkezi no: 7, 1. Baskı, Ankara, Aralık 2006.
- Başalp, Nilgün: “Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt 21, Sayı 1, İstanbul, 2015.
- Barbaro, Michael / Zeller, Tom: “A face is exposed for AOL searcher Nr. 441749”, **New York Times**, 09 Ağustos 2006.
- Başalp, Nilgün: **Kişisel Verilerin Korunması ve Saklanması**, Yetkin, Ankara, 2004.
- Benjelloun, Fatima-Zahra / Lahcen, Ayoub Ait / Belfkih, Samir: “An overview of big data opportunities, applications and tools”, **Intelligent Systems and Computer Vision**, (sunulmuş bildiri) IEEE, Mart 2015.
- Bennett, Colin J.: **Regulating Privacy**, Cornell University, New York, 1992.
- Bergkamp, Lucas / Dhont, Jan: “Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide” Web, **The Edi Law Review, Legal Aspects of Paperless Communication**, Cilt 7, Sayı 2-3, Kluwer Law International, 2000.
- Birnhack, Michael: “S-M-L-XL DATA: Big Data as a New Informational Privacy Paradigm”, **Big Data And Privacy Making Ends Meet**, Stanford Law School, The Center for Internet And Society, (Çevrimiçi) <https://fpf.org/wp-content/uploads/Big-Data-and-Privacy-Paper-Collection.pdf> , 18 Nisan 2018.
- Booth, Sharon / Jenkins, Richard / Moxon, David / Semmens, Natasha / Spencer, Christopher / Taylor, Mark / Townend, David: “What are ‘Personal Data’?: A Study conducted for the UK Information Commissioner”, **The University of Sheffield**, 2004, (Çevrimiçi) https://www.frareg.com/cms/wp-content/uploads/personal_data.pdf , 18 Nisan 2018.

- Bozkurt Yüksel, Armağan Ebru Bozkurt Yüksel, “Nesnelerin İnternetinin Hukuki Yönden İncelenmesi”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt 17, Sayı 2, 2015, s. 113-139.
- Buttarelli, Giovanni: “Big data, big data protection: challenges and innovative solutions” **ERA Conference on Recent Developments in Data Protection Law**, Keynote speech, Brussel, 11 Mayıs 2015.
- Bygrave, Lee A.: **Data Protection Law: Approaching Its Rationale, Logic and Limits**, Kluwer Law International, Hollanda, Amerika Birleşik Devletleri, 2002, s. 58.
- Carey, Peter: **Data Protection, A Practical Guide to UK and EU Law**, 2. Baskı, Oxford University Press, United Kingdom, 2004.
- Cavoukian, Ann / Jonas, Jeff: “Privacy by Design in the Age of Big Data”, **Information and Privacy Commissioner**, Ontario, Canada, Haziran 2012, (Çevrimiçi) <https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf>, 18 Nisan 2018.
- Charlesworth, Andrew: “Clash of the Data Titans? US and EU Data Privacy Regulation”, **European Public Law**, Cilt 6, Sayı 2, Hollanda, 2000, s. 256-257.
- Charlesworth, Andrew: “The Governance of the Internet in Europe”, **The Internet, Law and Society**, haz: Yaman Akdeniz, Clive Walker, David Wall, Pearson Education Limited, United Kingdom, 2000.
- Chen, Ray / Lazer Marius: “Sentiment Analysis of Twitter Feeds for the Prediction of Stock Market Movement”, **Stanford University**, 2013, (Çevrimiçi) <http://cs229.stanford.edu/proj2011/ChenLazer-SentimentAnalysisOfTwitterFeedsForThePredictionOfStockMarketMovement.pdf>, 18 Nisan 2018.
- Collins, Robert Todd Graham : “The Privacy Implications of Deep Packet Inspection Technology: Why the Next Wave in Online Advertising Shouldn't Rock the Self-Regulatory Boat” **Georgia Law Review**, Cilt 44, Sayı 2 2010, s. 545-580.

- Colonna, Liane: “Mo’ Data, Mo’ Problems? Personal Data Mining and the Challenge to the Data Minimization Principle”, **Big Data And Privacy Making Ends Meet**, Stanford Law School, The Center for Internet And Society, (Çevrimiçi) <https://fpf.org/wp-content/uploads/Big-Data-and-Privacy-Paper-Collection.pdf>, 18 Nisan 2018.
- Custers, Bart/ Ursic, Helena: “Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection”, **International Data Privacy Law**, 2016.
- Çekin, Mesut Serdar: **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu**, 1. Baskı, İstanbul, On İki Levha Yayıncılık, Ocak 2018.
- Çekin, Mesut Serdar: “6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt LXXIV, Sayı 2, İstanbul, 2016, s. 629-644.
- Çelik, Sadullah: “Büyük Veri Teknolojilerinin İşletmeler İçin Önemi”, **Social Sciences Studies Journal**, Cilt 3, Basım 6, 2017, s. 873-883.
- Çiğdem, Şemsettin / Seyreki İbrahim H.: “İşletmelerde Büyük Veri Uygulamaları: Bir Literatür Taraması”, **2. Ulusal Yönetim Bilişim Sistemleri Kongresi**, Erzurum, Kasım 2015.
- Çubukçu, Faruk: **Bilgisayar Terimleri Sözlüğü**, 1. Baskı, Ankara, V Yayınları, 1987.
- D’ Acquisto, Giuseppe / Domingo-Ferrer, Josep / Kikiras, Panayiotis / Torra, Vicenç / Montjoye, Yves-Alexandre de / Bourka, Athena: “Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies In The Era Of Big Data Analytics”, **The European Union Agency for Network and Information Security (ENISA)**, Aralık 2015.
- Davenport, Thomas / Morison, Robert / Harris, Jeanne: **Analytics at Work: Smarter Decisions, Better Results**, Harvard Business Review Press, Şubat 2010.
- Derinözlü, Cenk: “Büyük Veri ve Mahremiyet Big Data and Privacy”, **TUBİTAK 1.Ulusal Bulut Bilişim ve Büyük**

Veri Sempozyumu B3S17 Sempozyumu Bildiri Kitabı, 2017.

- Develioğlu, Hüseyin Murat: **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, 1. Baskı, İstanbul, On İki Levha Yayıncılık, 2017.
- Diebold, Francis X.: “A Personal Perspective on the Origin(s) and Development of “Big Data”: The Phenomenon, the Term, and the Discipline, Second Version”, PIER Working Paper No. 13-003, University of Pennsylvania, Department of Economics, **National Bureau of Economic Research**, Pennsylvania, 26 Kasım 2012.
- Dural, Mustafa / Öğüz, Tufan: **Kişiler Hukuku: Türk Özel Hukuku**, Cilt 2, İstanbul, Filiz Kitabevi, 2017.
- Dural, Mustafa / Sarı, Suat: **Türk Özel Hukuku: Temel Kavramlar ve Medeni Kanunun Başlangıç Hükümleri**, Cilt 1, 10. Baskı, İstanbul, Filiz Kitabevi, 2015.
- Dülger, Murat Volkan: **Bilişim Suçları ve İnternet İletişim Hukuku**, 6. Baskı, Ankara, Seçkin Yayıncılık, 2015.
- Dülger, Murat Volkan: “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”, **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt 3, Sayı 2, İstanbul, 2016, s. 101-167.
- Evans, David S.: “The Online Advertising Industry: Economics, Evolution and Privacy” **Journal of Economic Perspectives**, Cilt 23, Sayı 3, Sidney, 2009.
- François, Jean / Kombe, Akandji: **Avrupa İnsan Hakları Sözleşmesi kapsamında pozitif yükümlülükler: Avrupa İnsan Hakları Sözleşmesinin Uygulanmasına İlişkin Kılavuz Kitap**, çev: Özgür Heval Çınar ve Abdulcelil Kaya, Belçika, 1. Baskı, 2008,
- Fuster, Gloria González: **The Emergence of Personal Data Protection as a Fundamental Right of the EU**, Springer Science & Business, Belgium, 28 Nisan 2014.
- Fuster, Gloria González/ Scherrer, Amandine: “Big Data and Smart Devices and Their Impact on Privacy”, Directorate General For Internal Policies

- Policy Department C: Citizens' Rights And Constitutional Affairs Civil Liberties, **Justice and Home Affairs**, Brüksel, 2015, (Çevrimiçi) [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU\(2015\)536455_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf) 14 Nisan 2018.
- Garfinkel, Simson: **Database Nation: The Death of Privacy in the 21st Century**, Amerika Birleşik Devletleri, O'Reilly, 2000.
- Gemalmaz, Mehmet Semih: **İnsan Hakları Belgeleri/Human Rights Instruments**, Cilt 4, İstanbul, Boğaziçi Üniversitesi Yayınevi, 2004
- Gemalmaz, Mehmet Semih: **İnsan Hakları Belgeleri/Human Rights Instruments**, Cilt 1, İstanbul, Boğaziçi Üniversitesi Yayınevi, 2003.
- Gemalmaz, Mehmet Semih: **Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş**, 7. Baskı, İstanbul Legal Yayıncılık, 2010.
- Gemalmaz, Mehmet Semih: **Ulusalüstü İnsan Hakları Usul Hukuku Mevzuatı: Avrupa Konseyi Belgeleri & Avrupa İnsan Hakları Mahkemesi Kuralları Şerhi**, İstanbul, Legal Yayıncılık, Nisan 2006,
- Givens, Cherie L.: **Information Privacy Fundamentals for Librarians and Information Professionals**, United Kingdom, Rowman & Littlefield, 2014.
- Görgeç, Başak: "Genel İşlem Koşullarının Kişilik Hakkı Kapsamında Değerlendirilmesi", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt 19, Sayı 1, 2013, s. 403-440.
- Gözübüyük, Şeref / Gölcüklü, Feyyaz: **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması: Avrupa İnsan Hakları Mahkemesi İncelemesi ve Yargılama Yöntemi**, 11. Ek Protokola göre hazırlanıp genişletilmiş 11. Baskı, Ankara, Turhan Kitabevi, Ocak 2016.
- Gutwirth, Serge: "Short statement about the role of consent in the European data protection directive", **Selected Works of Serge Gutwirth**, University of Vrije, Brussel, 2012.
- Güneş, Ahmet M.: **Avrupa Birliği Hukukuna Giriş**, Güncellenmiş 3. Baskı, Ankara, Ekin Basım Yayın Dağıtım, 2017.

- Günoğur, Haluk: “Avrupa Birliği’nin Hukuk Düzeni”, **Avrupa Ekonomik Danışma Merkezi**, Ankara, 2007.
- Gürsaka, Necmi: **Büyük Veri**, 3. Baskı, Bursa, Dora Yayınları, 2017
- Henderson, Harry: **Privacy in the Information Age**, “Facts of File”, Brookings Institution Press, USA, 2006.
- Hermstruwer, Yoan “Contracting around Privacy: The (Behavioral) Law and Economics of Consent and Big Data”, **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, Cilt 8, Sayı 1, 2017, s. 9-26.
- Hert, Paul De / Czerniawski, Michael: “Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context”, **International Data Privacy Law**, Cilt 6, Sayı 3, Temmuz, 2016.
- Hoeren, Thomas: “Big Data and Data Quality”, **International Journal of Law and Information Technology**, Sayı 25, Oxford University Press, United Kingdom, 2017.
- Hofstadter, Samuel H. / Horowitz, George: “The Right to Privacy, Central Book Company”, New York, 1964 (Çevrimiçi), http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html, 12 Nisan 2018.
- IBM: “**Information lifecycle governance in a big data environment**” IBM Corporation, Ocak 2015, (Çevrimiçi) https://www-01.ibm.com/software/it/events/bigdata/pdfs/IBM_ILG_in_a_Big_Data_environment.pdf, 18 Nisan 2018.
- IT Governance Privacy Team: **EU General Data Protection Regulation: An Implementation and Compliance Guide**, IT Governance Publishing, United Kingdom, 2016.
- Karagülmez, Ali: **Bilişim Suçları ve Soruşturma–Kovuşturma Evreleri**, 5. Baskı, Ankara, Seçkin Yayıncılık, 2014.
- Karataş Durmuş, Neslihan: “Ticari Sırların Ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti”, **Türkiye Adalet Akademisi Dergisi**, Yıl 8, Sayı 31, Temmuz 2017, s. 371-409.

- Karlıdağ, Serpil: “Ekonomi Politik Açıdan Kişisel Verilerin Korunması”, **Amme İdaresi Dergisi**, Cilt 46, Sayı 1, Mart 2013, s. 127-152.
- Kaya Bensgir, Türksel: **Bilgi Teknolojileri ve Örgütsel Değişim**, Ankara, 1996, (Çevrimiçi)
http://www.todaie.edu.tr/resimler/ekler/03fc57586431f03_ek.pdf, 18 Nisan 2018.
- Kaya, Arslan: “4982 Sayılı Kanun Kapsamında Bilgi Edinme Hakkının Sınırlarından Olan 'Ticari Sır' ile Fikir ve Sanat Eserleri”, **Bilgi Edinme Hakkı**, Türkiye Barolar Birliği Yayınlar no: 62, Ankara, Türkiye Barolar Birliği, Haziran 2004, s. 127-141.
- Kaya, Mehmet Bedii: “Büyük Verinin Hukuki Boyutları”, **Büyük Veri ve Açık Veri Analitiği : Yöntemler Ve Uygulamalar**, ed: Prof. Dr. Şeref Sağıroğlu, Dr. Orhan Koç, Grafiker Yayınları, Ankara, 2017.
- Kennedy, John B. : “An Interview with Nikola Tesla”, **Twenty-First Century Books**, (Çevrimiçi)
<http://www.tfcbooks.com/tesla/1926-01-30.htm>, 04 Nisan 2018.
- Keser Berber, Leyla: **Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması**, 1. Baskı, On iki levha yayıncılık, İstanbul, Ocak 2014.
- Kırıldoğan, Melih / Fidaner, Işık Barış: “Derin Veri Analizi: İnternetteki Temel Gözetim Aracı”, **XIV. Akademik Bilişim Konferansı**, Uşak, 1-3 Şubat 2012, s. 967.
- Korff, Douwe: “EC Study on Implementation of Data Protection Directive-Comparative Summary of National laws”, Cambridge, Eylül 2002, (Çevrimiçi),
<http://194.242.234.211/documents/10160/10704/Statod+i+attuazione+della+Direttiva+95-46-CE>, 28 Nisan 2018.
- Korkmaz, İbrahim : **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, 1. Baskı, Seçkin Yayıncılık, Ankara, Nisan 2017.
- Kosta, Eleni: **Consent in European Data Protection law**, 3. Baskı, Brill | Nijhoff, Boston, 2013.

- Kotov, Vadim E.: “Big Data, Big Systems, Big Challenges: A Personal Experience”, **Perspectives of Systems Informatics**, ed. Andresi Voronkov, Irina Virbitskaite, Springer, Verlag Verlin Heidelberg, 2015.
- Kuner, Christopher / Cate, Fred H. / Millard, Christopher / Svantesson, Dan Jerker B: “The challenge of ‘big data’ for data protection”, **International Data Privacy Law**, Cilt 2, Sayı 2, 1 Mayıs 2012, s. 47–49.
- Kuner, Christopher: “The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law”, **Bloomberg BNA Privacy and Security Law Report**, 2012, s. 1-15.
- Kuner, Christopher: **European Data Protection Law: Corporate Compliance and Regulation**, 2. Baskı, Oxford University Press, USA, 2007.
- Kurt, Levent: **İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Seçkin, Ankara, 2005.
- Külcü, Özgür / Henkoğlu, Turkey: “Sosyal Paylaşım Ağlarında Gizlilik: Facebook İncelemesi”, **Bilgi Dünyası**, Cilt 15, Sayı 2, Ankara, 2014.
- Küzeci, Elif: “Anayasal Bir Hak: Kişisel Verilerin Korunması”, **Bilişim Dergisi**, Sayı 128, s. 142-148, Türkiye Bilişim Derneği, Ankara, Ocak 2011, (Çevrimiçi) <http://www.bilisimdergisi.org/s128/pdf/142-149.pdf>, 24 Nisan 2018.
- Küzeci, Elif: “İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı”, **İnsan Hakları Yıllığı**, Cilt 32, 2014.
- Küzeci, Elif: “Kişisel Verilerin Korunması”, **Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku (Genel Kamu Hukuku) Anabilim Dalı Doktora Tezi**, Ankara, 2010.
- Küzeci, Elif: **Kişisel Verilerin Korunması**, Yenilenmiş ve Gözden geçirilmiş 2. Baskı, Ankara, Turhan Kitabevi Yayınları, 2018.
- Laney, Doug: “3D Data Management: Controlling Data Volume, Velocity and Variety”, **Application Delivery Strategies**,

- 6 Şubat 2001, (Çevrimiçi)
<https://blogs.gartner.com/douglaney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>, 18 Nisan 2018.
- Laney, Douglas / Bayer, Mark A.: "The Importance of 'Big Data': A Definition", **Gartner**, Amerika Birleşik Devletleri, 21 Haziran 2012.
- Lessig, Lawrence: "Privacy as Property", **Social Research**, Cilt 69, Sayı 1, The New School, 2002.
- Liew, Anthony: "Understanding Data, Information, Knowledge and Their Inter-Relationships", **Journal of Knowledge Management Practice**, Cilt 8, Sayı 2, Haziran 2007.
- Malgieri, Gianclaudio: "Trade Secrets v Personal Data: a possible solution for balancing rights", **International Data Privacy Law**, Cilt 6, Sayı 2, 2016.
- Mantelero, Alessandro: "Competitive value of data protection: the impact of data protection regulation on online behaviour", **International Data Privacy Law**, Cilt 3, Sayı 4, Kasım 2013, s. 229-238.
- Marr, Bernard: **Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results**, Wiley, United Kingdom, 2016.
- Mauro, Andrea De/ Greco, Marco / Grimaldi, Michele: "What is Big Data? A Consensual Definition and a Review of Key Research Topics", 4th International Conference on Integrated Information, **AIP Proceedings**, 2014, (Çevrimiçi)
<https://aip.scitation.org/doi/abs/10.1063/1.4907823> , 18 Nisan 2018.
- Mayer-Schönberger, Viktor / Padova, Yann: "Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation" **The Columbia Science & Technology Law Review**, Cilt 17, Bahar 2016, s. 315-335.
- McCarty, Steven S. / Hilby, Anne Titus: "Research Guide to European Data Protection Law", **Legal Research Series**, Berkley, 2013.
- McCullagh, Karen: "Protecting 'privacy' through control of 'personal' data collection: a flawed approach", **International**

- Review of Law, Computers & Technology, Cilt 23, Sayı 1-2, Mart-Temmuz 2009, s. 47– 58.
- Munir, Ebu Bakar / Yasin, Siti Hajar Mohd / Sukki, Firdaus Muhammed: “Big Data: Big Challenges to Privacy and Data Protection”, **World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering**, Cilt 9, Sayı 1, 2015, s. 355-363.
- Neef, Dale: **Digital Exhaust: What Everyone Should Know About Big Data, Digitization and Digitally Driven Innovation**, PH Professional Business, Kasım 2014.
- OECD: **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**, OECD, Fransa, 2001
- OECD: **OECD Glossary of Statistical Terms**, Paris, OECD Publishing, 2007
- Oğuzman, Kemal / Seliçi, Özer / Oktay Özdemir, Saibe: **Kişiler Hukuku (Gerçek ve Tüzel Kişiler)**, Gözden Geçirilmiş ve Yenilenmiş 16. Bası, İstanbul, Filiz Kitabevi, İstanbul, 2016.
- Öğüt, Adem: **Bilgi Çağında Yönetim**, Ankara, Nobel Yayın Dağıtım, 2001.
- Öman, Sören: ”Implementing Data Protection in Law” i **IT Law – Scandinavian Studies in Law**, Cilt 47, The Stockholm University Law Faculty, 2004, s. 389-403.
- Öncü, Gülay Arslan: “Özel Yaşama ve Aile Yaşamına Saygı Hakkı”, **İnsan Hakları Avrupa Sözleşmesi ve Anayasa, Anayasa Mahkemesine Bireysel Başvuru Kapsamında Bir İnceleme**, ed. Sibel İncoğlu, 3. Baskı, İstanbul, Beta, Haziran 2013.
- Özdemir, Hayrunnisa: **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, 1. Baskı, Ankara, Seçkin Yayıncılık, 2009.
- Pagolu, Venkata Sasank / Challa, Kamal Nayan Reddy / Panda, Ganapati / Majhi, Babita: “Sentiment Analysis of Twitter Data for Predicting Stock Market Movements”, **International conference on Signal Processing, Communication, Power and Embedded System**, 2016, (Çevrimiçi) <https://arxiv.org/pdf/1610.09225.pdf> , 18 Nisan 2018
- Perugini, Maria Roberta: “Personal Data Made Public by the ‘Data Subject’ And Use Of Information Published On Social Networks: Early

- Observations Of GDPR”, **Europrivacy**, 2016
(Çevrimiçi) 22 Mart 2018
(<http://europrivacy.info/2016/10/31/italiano-dati-personali-resi-manifestamente-pubblici-dallinteressato-e-uso-di-dati-pubblicati-su-social-network-prime-osservazioni-allart-9-co-2-lett-e-gdp/>), 18 Nisan 2018.
- Rose, John / Barton, Christine / Souza, Rob / Platt, James: “The Trust Advantage: How to Win with Big Data”, **The Boston Consulting Group**, Boston, Kasım 2013.
- Rost, Martin / Bock, Kirsten: “Privacy by Design and the New Protection Goals,” İngilizce çevirisinden yararlanılmıştır, “Privacy By Design und die Neuen Schutzziele”, **Datenschutz und Datensicherheit**, Cilt 35, Sayı 1, 2011.
- Sağiroğlu, Şeref / Sinanç Terzi, Duygu / Terzi, Ramazan / Canbay, Yavuz / Gündüz, Sedef / Arslan, Bilgehan / Ayaydın, Anıl / Gökalp, Ahmet Burak: **Büyük Veri Analitiği, Güvenliği Ve Mahremiyeti**, Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Büyük Veri Analitiği Ve Güvenliği (BIDISEC) Araştırma Gurubu, Nisan 2016.
- Saymen, Ferit H.: **Türk Medeni Hukuku: Şahsın Hukuku**, Cilt 2, Yenilenmiş 2. Baskı, Hak Kitabevi, İstanbul, 1960.
- Schwartz, Paul M.: “The EU-U.S. Privacy Collision: A Turn To Institutions and Procedures”, **Harvard Law Review**, Cilt 126, Sayı 7, 2013, s. 1966-2009.
- Sencer, Muzaffer: **Belgelerle İnsan Hakları**, Beta, İstanbul, 1988.
- Siegel, Eric: **Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die**, Jeopardy Productions, Canada, 2013.
- Simitis, Spiros: “From the Market to the Polis: The EU Directive on Protection of Personal Data”, **Iowa Law Review**, Cilt 80, 1994.
- Smith, Matthew / Henne, Benjamin / Szongott, Christian / Voigt, Gabriele von: “Big data privacy issues in public social media”. **6th IEEE International Conference on Digital Ecosystems Technologies**, İtalya, Haziran 2012.

- Supriyadi, Daniar: “Personal and Non-Personal Data in the Context of Big Data”, **Tilburg Institute for Law, Technology and Society**, Tilburg University, Ocak 2017.
- Taigman, Yaniv, Yang, Ming, Ranzato, Marc’Aurelio, Wolf, Lior: “DeepFace: Closing the Gap to Human-Level Performance in Face Verification”, 2014, (Çevrimiçi) https://www.cs.toronto.edu/~ranzato/publications/taigman_cvpr14.pdf , 8 Nisan 2018.
- Tanör, Bülent, Yüzbaşıoğlu, Necmi : **1982 Anayasasına Göre Türk Anayasa Hukuku**, 8. Baskı, İstanbul, Beta, Aralık 2006.
- Tansan, Burak / Gökbulut, Aykan / Eren, Tevfik / Targotay, Çağlar / Balkır, Mehmet Bahadır / Pekarun, Mehmet Nurettin: “Türkiye’nin Küresel Rekabetçiliği İçin Bir Gerekliklik Olarak Sanayi 4.0: Gelişmekte Olan Ekonomi Perspektifi”, Editörler: Nurşen Numanoglu, Mehmet Evren Eynehan, Yayın no TÜSİAD-T/2016-03/576, TÜSİAD, İstanbul, Mart 2016.
- Taranto, Lill: “Data Protection Principles”, **European Privacy: Law and Practice for Data Protection Professionals**, Editör: Eduardo Ustaran, IAPP publication, USA, 2012.
- Taştan, Furkan Güven: **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, 2. Baskı, İstanbul, On İki Levha Yayıncılık, Kasım 2017, s. 67.
- Tekin, Nurullah: “Kişisel Verilerin Korunması İle İlgili Türkiye’deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi”, **Uyuşmazlık Mahkemesi Dergisi**, sayı 4, 2014.
- Tekinalp, Gülören / Tekinalp, Ünal: **Avrupa Birliği Hukuku**, 2. Basım, İstanbul, Beta, 2000.
- Tezcan, Durmuş: “Bilgisayar Karşısında Özel Hayatın Korunması”, **Anayasa Yargısı, Dergisi**, Cilt 8, 1991, s. 385-392.
- Tikkinen-Piri, Christina / Rohunen, Anna/ Markkula, Jouni: “EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies”, **Computer Law & Security Reviews**, Cilt 34, Sayı 1, Şubat 2018, s. 134-153.
- Uncular, Selen: **İş İlişkisinde İşçinin Kişisel Verilerinin Korunması**, Ankara, Seçkin Yayıncılık, 2014.
- Uygun, Murat: “Avrupa Birliği 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması”, **Gazi**

Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara, 2010.

- Velidedeoğlu, Hıfzı Veldet: **Türk Medeni Hukuku: Şahsın Hukuku**, İstanbul Üniversitesi Neşriyatından Sayı 357, Hukuk Fakültesi, Cilt 1, Sayı 81, 3. Baskı, İstanbul, 1963.
- Warner, Jeremy: “The Right to Oblivion: Data Retention From Canada to Europe in Three Backward Steps”, **University of Ottawa Law and Technology Journal**, Sayı 2, 2005.
- Warren, Samuel D. / Brandeis, Louis D.: “The Right to Privacy”, **Harvard Law Review**, Cilt 4, Sayı 5, Boston, 15 Aralık 1890.
- White, Alison: “Control of transborder data flow: reactions to the European Data Protection Directive”, **International Journal of Law and Information Technology**, Cilt 5, Sayı 2, Kanada, 1997.
- Yücedağ, Nafiye: “The Protection Of IP Addresses In Peer-To-Peer (P2P) Networks”, 13th International Conference on Internet, Law & Politics, **Managing Risk in the Digital Society**, Barselona, İspanya, 29 Haziran - 30 Eylül 2017.
- Yücedağ, Nafiye: “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt 75, Sayı 2, 2017.
- Zarsky, Tal Z.: “Incompatible: The GDPR in the Age of Big Data”, **Seton Hall Law Review**, Cilt 47, Sayı 4, 2017, s. 995-1020.
- Zevkliler, Aydın / Acabey, M. Beşir / Gökyayla, K. Emre: **Medeni Hukuk: Giriş ve Başlangıç Hükümleri Kişiler hukuku Aile hukuku**, Gözden Geçirilmiş ve Genişletilmiş 6. Baskı, Seçkin Yayınevi, Ankara 1999, s. 207.

II. Belge, Görüş, Araştırma ve Raporlar

- Article 29 Working Party: “Statement on Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU (the European Commission 2014)”, WP 221, 16 Eylül 2014.

- Article 29 Working Party: “Report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union”, WP 106, 18 Ocak 2005
- Article 29 Working Party: “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, WP 251, 3 Eylül 2017.
- Article 29 Working Party: “Guidelines on Consent under Regulation, 2016/679”, WP 259, 28 Kasım 2017.
- Article 29 Working Party: “Opinion 01/2012 on the data protection reform proposals Adopted on 23”, WP 191, 29 Mart 2012.
- Article 29 Working Party: “Opinion 03/2013 on purpose limitation”, WP 203, Görüş, 2 Nisan 2013.
- Article 29 Working Party: “Opinion 05/2014 on Anonymisation Techniques, Adopted”, WP216, 10 Nisan 2014.
- Article 29 Working Party: “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”, WP 217, 9 Nisan 2014.
- Article 29 Working Party: “Opinion 15/2011 on the definition of consent”, WP187, 13 Haziran 2011.
- Article 29 Working Party: “Guidelines on transparency under Regulation 2016/679” WP 260, 29 Kasım 2017.
- Article 29 Working Party: “Opinion 6/2002 on transmission Passenger Manifest Information and other data from airlines to the United States”, WP 66, 24 Ekim 2002.
- Article 29 Working Party: “Opinion 2/2010 on online behavioural advertising”, WP 171, 22 Haziran 2010.
- Article 29 Working Party: “Opinion 8/2001 on the processing of personal data in the employment context”, WP 48, 13 Eylül 2001.
- Article 29 Working Party: “Opinion 3/2010 on the principle of accountability”, WP 173, , 13 Temmuz 2010.
- Article 29 Working Party: “Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)”, WP 258, 29 Kasım 2017.
- Article 29 Working Party “Opinion 1/2010 on the concepts of "controller" and "processor"”, WP 169, 16 Şubat 2010.

- Article 29 Working Party: “Press Release”, Brüksel, 15 Aralık 2011, (Çevrimiçi), http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2011/20111215_press_release_obo_final.pdf, 22 Mart 2018.
- Article 29 Working Party: “Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 2093/05/EN”, WP 114, 25 Kasım 2005.
- Article 29 Working Party: ”Opinion 4/2007 on the Concept of Personal Data”, WP 136, 20 Haziran 2007.
- Avrupa Veri Koruma Denetmeni: “Meeting the challenges of big data, Opinion 7/2015”, 19 Kasım 2015, (Çevrimiçi) https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf, 8 Nisan 2018.
- Avrupa Veri Koruma Denetmeni: “Opinion of the European Data Protection Supervisor on the Data protection Reform Package”, 7 Mart 2012.
- Avrupa Veri Koruma Denetmeni: “Opinion of the European Data Protection Supervisor, on the proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure”, 12 Mart 2014, (Çevrimiçi), https://edps.europa.eu/sites/edp/files/publication/14-03-12_trade_secrets_en.pdf, 8 Nisan 2018
- Council of Europe: Fact Sheet, “**Questions and Answers - Data Protection Reform**”, 21 Aralık 2015, (çevrimiçi) http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm, 18 Nisan 2018.
- Council of Europe: “New Technologies: A Challenge to Privacy Protection?”, Fransa, 1989.
- Executive Office of the President: “Big Data: Seizing Opportunities, Preserving Values”, **The White House**, Washington, Mayıs 2014.
- Garante Per La Protezione Dei Dati Personali: “Linee guida in materia di attività promozionale e contrasto allo spam”, 4 Temmuz 2013, (Çevrimiçi) (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2542348>), 22 Mart 2018.
- Information Commissioner Office: “‘Anonymisation: managing data protection risk’ code of practice” Kasım 2012, (Çevrimiçi)

- <https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf> , 18 Nisan 2018.
- Information Commissioner Office: ““Big Data and Data Protection”, 7 Nisan 2014, (Çevrimiçi) <https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220> , 18 Nisan 2018.
- Information Commissioner Office: “How can we apply legitimate interests in practice?” , 23 Mart 2018, (Çevrimiçi) <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>, 2 Nisan 2018.
- Information Commissioner Office: “Direct marketing”, 6 Mart 2018
- Information Commissioner’s Office: “Big data, artificial intelligence, machine learning and data protection”, 4 Eylül 2017, (Çevrimiçi) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>, 18 Nisan 2018
- International Institute of Communications: “Personal data management: the user’s perspective”, Londra, Eylül 2012.
- Joint Committee: “Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions”, (Çevrimiçi) https://esas-joint-committee.europa.eu/publications/discussion%20paper/jc-2016-86_discussion_paper_big_data.pdf , 18 Nisan 2018.
- Kişisel Verileri Koruma Kurumu: “6698 Sayılı Kanun’da Yer Alan Kurumsal Terimler”, (Çevrimiçi) , 2017, Ankara, <http://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20KANUN%E2%80%99DA%20YER%20ALAN%20KURUMSAL%20TERIMLER.pdf> , 22 Mart 2018.
- Kişisel Verileri Koruma Kurumu: “Kişisel Verilerin Korunması Kanunu ve Uygulaması”, (Çevrimiçi) , 2017, Ankara, <http://www.kvkk.gov.tr/yayinlar/K%C4%B0C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf> , 22 Mart 2018.

Kişisel Verileri Koruma Kurumu:	“Ulusal Ve Uluslararası Alanda Kişisel Verilerin Korunmasına Duyulan İhtiyaç”, 2017, Ankara,(Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8e39e0a1-6ec4-4179-a5d3-bbd8e78dce31.pdf , 13 Nisan 2018
Kişisel Verileri Koruma Kurumu:	“6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar”, 2017, Ankara, (Çevrimiçi) https://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20Y%C3%96NEL%C4%B0K%20SORU%20VE%20CEVAPLAR.pdf , 14 Nisan 2018
Kişisel Verileri Koruma Kurumu:	“6698 Sayılı Kanun’da Yer Alan Temel Kavramlar”, 2017, Ankara, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/45af208d-3718-49ed-b51a-9be9edde6ff2.pdf , 14 Nisan 2018.
Kişisel Verileri Koruma Kurumu:	Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi , Ankara, KVKK Yayınları, Mart 2018, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf , 14 Nisan 2018.
Kişisel Verileri Koruma Kurumu:	Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi , Ankara, KVKK yayınları, Ocak 2018, (Çevrimiçi) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf , 18 Nisan 2018.
KPMG:	“Crossing the line: Staying on the right side of consumer privacy”, KPMG, Ocak 2017, (Çevrimiçi) https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/crossingthe-line.pdf , 8 Nisan 2018.
Networked Software and Services Initiative:	“Big Data: A New World of Opportunities, White Paper”, Aralık 2012, (Çevrimiçi) http://www.nessi-europe.com/Files/Private/NESSI_WhitePaper_BigData.pdf , 14 Nisan 2018.

- Office of the Australian Information Commissioner: “Consultation draft: Guide to big data and the Australian Privacy Principles”, Mayıs 2016, (Çevrimiçi) <https://www.oaic.gov.au/engage-with-us/consultations/guide-to-bigdata-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacyprinciples>, 18 Nisan 2018.
- The Boston Consulting Group: Unlocking the Value of Personal Data: From Collection to Usage, World Economic Forum, 2013, (Çevrimiçi) http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf, 8 Nisan 2018.

III. Gazete ve Dergi Haberleri

- ““Programattik” ile dijital reklamcılık alanında yeni bir dönem başlıyor!”, 8 Nisan 2016, (Çevrimiçi) <https://www.turktelekom.com.tr/hakkimizda/medya-merkezi/basin-bultenleri/sayfalar/programattik-digital-reklamcilik.aspx>, 8 Nisan 2018.
- “Are insurance companies spying on your Facebook page?” 7 Kasım 2011, (Çevrimiçi) <http://abc7.com/archive/8422388/>, 8 Nisan 2018.
- “Big data market size revenue forecast worldwide from 2011 to 2027”, (Çevrimiçi) <https://www.statista.com/statistics/254266/global-big-data-market-forecast/>, 14 Nisan 2018.
- “Cambridge Analytica used data from Facebook and Politico to help Trump”, (Çevrimiçi) <https://www.theguardian.com/technology/2017/oct/26/cambridge-analytica-used-data-from-facebook-and-politico-to-help-trump>, 4 Nisan 2018.
- “EU lawmakers to investigate alleged misuse of Facebook users' data”, Reutersi 19 Mart 2018 (Çevrimiçi), <https://www.reuters.com/article/us-facebook-cambridge-analytica-eu/eu-lawmakers-to-investigate-alleged-misuse-of-facebook-users-data-idUSKBN1GV1A3>, 22 Mart 2018.

“How Obama Used Big Data to Rally Voters”, (Çevrimiçi) <https://www.technologyreview.com/s/508836/how-obama-used-big-data-to-rally-voters-part-1/>, 8 Nisan 2018.

“Telefónica partners with advertising firm in UK big data Project”, 8 Haziran 2015, (Çevrimiçi) <https://www.eurocomms.com/industry-news/10746-telefonica-partners-with-advertising-firm-in-uk-big-data-project>, 8 Nisan 2018.

Armour, Stephanie: “Regulators Have Concerns About Lenders' Use of Facebook, Other Sites”, 08 Ocak 2014, (Çevrimiçi) <https://www.wsj.com/articles/borrowers-hit-socialmedia-hurdles-1389224469?tesla=y>, 08 Nisan 2018.

Kirk Borne, “Big Data, Small World: Kirk Borne at TEDxGeorgeMasonU”, 6 Nisan 2013, (Çevrimiçi) <https://www.youtube.com/watch?v=Zr02fMBfuRA>, 18 Nisan 2018.

Pure Storage, Big data’s big failure. “The struggles businesses face in accessing the information they need. Pure Storage” Aralık 2015, (Çevrimiçi) http://info.purestorage.com/rs/225-USM292/images/Big%20Data%27s%20Big%20Failure_UK%281%29.pdf?aliId=64921319, 8 Nisan 2018.

Rijmenam, Mark van: “A Short History Of Big Data”, 07 Ocak 2016, (Çevrimiçi) <https://datafloq.com/read/big-data-history/239>, 8 Nisan 2018.

Harari, Yuval Noah, “Will the Future Be Human?”, (çevirimiçi), <https://www.weforum.org/events/world-economic-forum-annual-meeting-2018/sessions/will-the-future-be-human>, 22 Mart 2018.

Warner, Andrew, George Dyson seminar media, “The Long Now Foundation” 28 Mart 2013, (Çevrimiçi) <http://blog.longnow.org/02013/03/28/george-dyson-seminar-media/>, 08 Nisan 2018.

IV. Yararlanılan Başlıca İnternet Siteleri

Avrupa Komisyonu, (Çevrimiçi) <http://www.coe.int/>, 12 Nisan 2018.

“Federal Data Protection Act, Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung”, bölüm 3. İngilizce çevirisi için bkz., (Çevrimiçi) <http://germanlawarchive.iuscomp.org/?p=712#3>, 4 Nisan 2018.

Article 29 Working Party, (Çevrimiçi) http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm, 12 Nisan 2018.

Kazancı Yargıtay Kararı Arama Motoru, (Çevrimiçi) <http://www.kazanci.com/kho2/ibb/ara.htm>, 12 Nisan 2018.

Kişisel Verileri Korunma Kurumu, (Çevrimiçi) <https://www.kvkk.gov.tr/>, 12 Nisan 2018.

OECD, (Çevrimiçi) <http://www.oecd.org>, 12 Nisan 2018.

Mevzuat, (Çevrimiçi) mevzuat.gov.tr, 12 Nisan 2018.