

T.C.
DOKUZ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
AVRUPA BİRLİĞİ HUKUKU PROGRAMI
YÜKSEK LİSANS TEZİ

AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN
KORUNMASI

Senem OVALIOĞLU

Danışman

Doç. Dr. Şafak EVRAN TOPUZKANAMIŞ

İZMİR- 2021

TEZ ONAY SAYFASI



YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum “Avrupa Birliği Hukuku’nda Kişisel Verilerin Korunması” adlı çalışmanın, tarafımdan, akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

26/07/2021

Senem OVALIOĞLU

ÖZET
Yüksek Lisans Tezi
Avrupa Birliği Hukuku’nda Kişisel Verilerin Korunması
Senem OVALIOĞLU

Dokuz Eylül Üniversitesi
Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı
Avrupa Birliği Hukuku Programı

Küreselleşmenin her geçen gün arttığı teknoloji çağında yaşanan gelişmeler ışığında, toplumsal kalkınma da hızla artmış ve buna bağlı olarak yeni imkanlar gün yüzüne çıkmıştır. Teknoloji ile birlikte bilgi sistemlerinde yaşanan ilerlemelerle birlikte pek çok kolaylık da hayatımızda yerini almıştır. İnternet üzerinden bankacılık işlemleri, alışveriş, bilgi ve anlık durum paylaşımı, fotoğraf aktarımı başta olmak üzere bilgi sistemleri kullanılarak yapılan pek çok işlem günlük yaşamımızda önemli bir rol oynar hale gelmiştir.

Bilgi sistemlerinin bu denli önemli hale gelmesiyle birlikte kişisel verilerin korunması da önemli bir sorun haline gelmiştir. Zira veri sahiplerinin kişisel verilerinin işlenmesini kontrol altında tutması imkansız hale gelmiş ve bu durum bilgi güvenliği üzerinde açık alanlar kalmasına yol açmıştır. Bu husus, kişisel verilerin hukuka uygun işlenmesini sağlamak ve kötüye kullanılmasını önlemeye yönelik normatif düzeyde düzenlemeler yapılmasını gerektirmiştir. Kişisel verilerin korunmasının, insan onuru ve mahremiyet gereksinimi altında değerlendirmeye alınması ile birlikte temel haklar ve özgürlükler bağlamında verilerin güvenliği ve korunması da bir temel gereksinim haline gelmiştir.

Çalışmamızda da kişisel veri kavramının geçmişten günümüze şekillenmesi, tarihsel süreç içerisinde Avrupa Birliği’nde kişisel verilerin korunması bağlamında yapılan düzenlemeler ve güncel kişisel verileri koruma mevzuatı olan Avrupa Birliği Genel Veri Koruma Tüzüğü detaylarıyla ele alınmıştır.

Anahtar Kelimeler: Kişisel Veri, Kişisel Verilerin Korunması, Mahremiyet, GDPR, Hassas Veriler.



ABSTRACT
Master's Thesis
Protection of Personal Data in European Union Law
Senem OVALIOĞLU

Dokuz Eylül University
Graduate School of Social Sciences
Department of Public Law
European Union Law Program

In the light of developments in the age of technology, where globalization is increasing day by day, social development has also increased rapidly and new opportunities have emerged accordingly. Along with advances in information systems with technology, many convenience have taken their place in our lives. Many transations made using the information systems, especially online banking, shopping, snapshots, and photo transfer, have become an important role in our daily life.

With the Information systems becoming such an important, protection of personal data has also beome an important issue. Because it has become impossible for data owners to control processing of their personal data and this situation has left open areas on information security. This issue necessiated legislate normative regulations to ensure the legal processing of personal data and prevent its misuse. With the protection of personal data being eveluated under need of human dignity and privacy, the security and protection of data in context of fundamental rights and freedoms has also become basic needs.

In our study, the shaping of the concept of personal data from the past to present, the regulations made in the context of the protection of personal data in the European Unionin the historical process and the European Union General Data Protection Regulation, which is the current personal data protection legislation, are discussed in detail.

Keywords: Personal Data, Protection of Personal Data, Privacy, GDPR, Sensitive Data

AVRUPA BİRLİĞİ HUKUKU'NDA KİŞİSEL VERİLERİN KORUNMASI

İÇİNDEKİLER

TEZ ONAY SAYFASI	ii
YEMİN METNİ	iii
ÖZET	iv
ABSTRACT	vi
İÇİNDEKİLER	vii
KISALTMALAR	xi

GİRİŞ	1
-------	---

BİRİNCİ BÖLÜM

AVRUPA BİRLİĞİ HUKUKUNUN TEORİK ZEMİNİNDE KİŞİSEL VERİLERİN KORUNMASI

I. KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ	7
A. Avrupa Birliği'nde Kişisel Verilerin Tarihsel Gelişimi	8
B. Kişisel Verilerin Tarihsel Gelişimine Etki Eden Olgular	10
II. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN KAVRAMLARI VE TEMEL İLKELERİ	13
A. Kişisel Veriye İlişkin Kavramlar	13
1. Gerçek Kişi	13
2. Kimliği Belirli veya Belirlenebilir Olma	16
3. Kişiye Ait Veri	17
4. Her Türlü Bilgi	18
5. Hassas Veriler	18
B. Kişisel Verinin İşlenişine İlişkin Kavramlar	20
1. Veri İşleme Faaliyeti	21
2. Veri Sorumlusu	21
3. Veri İşleyen	23

4. Alıcı ve Üçüncü Kişi	24
C. Kişisel Verilerin Korunmasına Hakim Olan Temel İlkeler	25
1. Hukuka Uygunluk, Adalet ve Şeffaflık	25
2. Amaç İle Sınırlılık	26
3. En Az Seviyede Bilgi	28
4. Doğruluk	29
5. Sınırlı Süre İle Saklama	29
6. Bütünlük ve Gizlilik	30
7. Hesap Verebilirlik	31
III. KİŞİSEL VERİLERİN HUKUKİ NİTELİĞİ	32
A. Kişilik Hakkı Görüşü	32
B. Fikri Hak Görüşü	34
C. Mülkiyet Hakkı Görüşü	35
IV. KİŞİSEL VERİLERİN İŞLENMESİNDE HUKUKA UYGUNLUK HALLERİ	36
A. Genel Olarak	36
1. Veri Sahibinin Rızası	36
2. Sözleşmenin Gereğinin Yerine Getirilmesi	38
3. Hukuki Yükümlülüğün Yerine Getirilmesi	39
4. Hayati Menfaatin Korunması	40
5. Kamu Görevinin Yerine Getirilmesi	41
6. Meşru Menfaatlerin Korunması	42
B. Hassas Verilerin İşlenmesi	43
V. KİŞİSEL VERİLERİN KORUNMASINDA TEMEL HAKLAR VE ÖZGÜRLÜKLER BOYUTU	44
A. Özel Hayatın Gizliliği Hakkı Boyutu	44
B. Düşünce ve İfade Özgürlüğü Boyutu	46
C. Unutulma Hakkı Boyutu	47
D. Bilgi Edinme Hakkı Boyutu	49

İKİNCİ BÖLÜM
AVRUPA BİRLİĞİ HUKUKUNDA DÜZENLEMELER VE KURUMLAR
ÇERÇEVESİNDE KİŞİSEL VERİLERİN KORUNMASI

I. KURUMLAR BAZINDA KİŞİSEL VERİLERİN KORUNMASI	52
A. OECD İlkeleri	52
B. 108 Sayılı Avrupa Konseyi Sözleşmesi	54
C. 95/46/EC Sayılı Yönerge	57
D. Temel Haklar Şartı	60
E. 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü	62
II. KİŞİSEL VERİLERİN İŞLENMESİNDE TARAFLARIN HAKLARI VE YÜKÜMLÜLÜKLERİ	64
A. Veri Sahibinin Hakları	64
1. Bilgi Alma Hakkı	64
2. Erişim Hakkı	66
3. Düzeltme Hakkı	67
4. Silinmeyi Talep Etme Hakkı	68
5. İşlemenin Kısıtlanması Hakkı	70
6. Bildirimde Bulunulmasını Talep Hakkı	71
7. Veri Taşınabilirliği Hakkı	72
8. İtiraz Hakkı	72
B. Veri Sorumlusu ve Veri İşleyenin Yükümlülükleri	73
1. Gerekli Tedbirleri Alma Yükümlülüğü	74
2. Ortak Veri Sorumlularının İşbölümü Yapma Yükümlülüğü	75
3. Temsilci Atama Yükümlülüğü	76
4. Uygun Veri İşleyenleri Seçme Yükümlülüğü	76
5. Kayıt Tutma Yükümlülüğü	77
6. Denetim Makamıyla İşbirliği Yükümlülüğü	78
7. İşlemenin Güvenliğini Sağlama Yükümlülüğü	78
8. Bildirim Yükümlülüğü	79
9. Veri Koruma Etki Değerlendirmesi ve Ön İstişare Yükümlülüğü	81
10. Veri Koruma Görevlisi Atama Yükümlülüğü	82

III. AVRUPA BİRLİĞİ'NDE KİŞİSEL VERİLERİN İŞLENMESİNİ	
DENETLEYEN VE DÜZENLEYEN KURUMLAR	83
A. Denetim Makamları	84
1. Genel Olarak	84
2. Görev ve Yetkileri	85
B. Avrupa Veri Koruma Kurulu	88
IV. HAKLARIN VE MENFAATLERİN KORUNMA YOLLARI	90
A. İdari Başvuru Yolları	90
1. Şikayet Başvurusu	91
2. İdari Para Cezası	93
B. Hukuki Yaptırımlar	94
C. Cezai Yaptırımlar	95
V. AVRUPA BİRLİĞİ'NDE ÖNCÜ ÜLKELER BAZINDA KİŞİSEL	
VERİLERİN KORUNMASI HUKUKU: ALMANYA VE FRANSA ÖRNEĞİ	95
A. Almanya'da Kişisel Verilerin Korunması	96
B. Fransa'da Kişisel Verilerin Korunması	103
SONUÇ	109
KAYNAKÇA	114

KISALTMALAR

AB	Avrupa Birliđi
ABAD	Avrupa Birliđi Adalet Divanı
ABD	Amerika Birleşik Devletleri
bkz.	Bakınız
CNIL	Fransız Ulusal Veri Koruma Kurulu
DPD	Veri Koruma Yönergesi
GDPR	Avrupa Birliđi Genel Veri Koruma Tüzüğü
M.Ö.	Milattan Önce
OECD	Ekonomik Kalkınma ve İşbirliđi Örgütü
s.	Sayfa No
ss.	Sayfadan Sayfaya
vd.	Ve Devamı

GİRİŞ

Bilişim sistemlerinin kullanımının yaygınlaşmasıyla birlikte, özellikle internetin ve diğer iletişim araçlarının hayatımızdaki yerinin önemi her geçen gün artmaktadır. Teknolojinin sağladığı imkanlar arttıkça saniyeler içinde terabaytlarca bilgiyi Dünya'nın dört yanına tek tuş ile aktarmak mümkün hale gelmiştir. İnternet kullanıcıları kimi zaman bu aktarımı kendileri bilerek ve isteyerek yapmakta, kimi zaman ise toplumsal hayatın bir parçası olmaktan kaynaklanan işlemlerin yerine getirilebilmesi için verilerimiz, bilgimiz veya kontrolümüz dışında işlenmektedir. Modern toplumlarda yaşayan gerçek kişilerin, çoğu zaman herkes tarafından bilinmek dürtüsüyle ortaya çıkan kişisel verilerine ilişkin internet paylaşımları veya verilerin olağan hayat akışı içinde çeşitli kişi ve kurumlarca elde edilmesi, kişisel özgürlükler ve temel hakların korunması alanında bir takım sorunları da beraberinde getirmektedir. Bu sorunların ortaya çıktığı noktada ise çözüm olarak kişisel verilerin korunmasına yönelik hukuki düzenlemeler gündeme gelmektedir.

Gelişen teknoloji ile birlikte hayatımıza pek çok kolaylık girmiş ve sahip olduğumuz bilgi ve veri akışı sınırsız denebilecek bir boyuta ulaşmıştır. Ancak bu bilgi ve veri akışı bolluğunun aynı zamanda kişisel verilerimizden ve dolayısıyla bireysel özgürlüğümüzden vazgeçme anlamını da beraberinde getirdiğini kabul etmek en temelde insan haklarına aykırı bir tutum olacaktır. Günlük hayata ayak uydururken, teknoloji ile birlikte yaşamın içine dahil olan kolaylıklardan faydalanmak karşılığında kişinin kendi verilerini takas etmesi fikri de insan onuru ve bireyin kendini gerçekleştirme için tüm gerekliliklere ters düşecektir.

Gelişen teknoloji ile birlikte artan farkındalığa bağlı olarak temel haklar ve özgürlükler bilinci de oldukça yol kat etmiştir. Bu durumda, bir hizmet kullanıcısı olan veri sahibinin yalnızca bu hizmeti kullandığı hatta bizzat kendisi kullanmasa bile vatandaş olmanın gerekliliklerinden dolayı bir hizmete maruz kaldığı durumlarda; bu hizmetin karşılığı olarak verilerini sunmasını beklemek demokratik bir toplum anlayışına aykırılık teşkil eder. Bu nedenle birey ne bir hizmet ne de bir kimlik sahibi olma dolayısıyla mahremiyet alanına müdahaleye maruz bırakılabilir. Bu düşüncenin ortaya attığı bilinç de kişisel verilerin korunması hakkının doğmasından sonra, hızlı bir şekilde gelişmesini sağlamıştır.

Kişisel verilerin korunmasına ilişkin önemli adımlar Avrupa’da atılmıştır. Kişisel verilerin korunmasına ilişkin ilk yasal düzenlemelerin adımları Avrupa’da atılmış olmakla birlikte; Avrupa Birliği içerisinde özel yaşamın korunmasına gösterilen saygının da etkisiyle veri koruma başlı başına bir hukuk dalı haline gelmiştir. Avrupa’da önem verilen bu hususlar önderliğinde dünya çapında kişisel verilerin korunmasına yönelik pek çok çalışma yapılmış, pek çok yasal düzenleme oluşturulmuştur.

Çalışmamız iki ana bölümden oluşmaktadır. Bu ana bölümler, inceleme ve açıklamada bütünlüğü sağlamak adına alt başlıklara ayrılarak ortaya konmuştur. Birinci bölümde kişisel verilerin daha çok teorik yönü açıklanarak temel haklar ve özgürlükler bağlamında yeri incelenmiştir. İkinci bölüm ise daha uygulama odaklı olup kişisel verilerin korunmasının karşımıza nasıl çıktığı üzerinde durulmuştur. Öncelikle kişisel verilerin tarih içerisinde ortaya çıktığı düşünülen ilk dönemlerden günümüze kadar geçirdiği süreç, özellikle temel haklar ve özgürlükler boyutuyla ele alınmıştır. Zira artık üzerine pek çok çalışma ve yasal düzenleme yapıldığı üzere, kişisel verilerin korunması bir temel hak olarak hukuk gündeminde yerini almıştır. Biz de kişisel verilerin temel niteliğinden hareketle konumuz doğrultusunda, Avrupa’da kişisel verilerin tarihsel gelişimi ile yola çıkarak çalışmamızı hazırladık. Bu tarihsel gelişim süreci içinde kişisel verilerin bugünkü öneme kavuşmasını sağlayan temel bilinci de işleyerek kişisel verilerin özünü oluşturan olguları da açıklamaya çalıştık.

Kişisel verilerin gündeme gelmesinde etkili olan süreçleri inceledikten sonra, kişisel verilerin korunmasında önemli rol oynayan temel kavramlar gelmektedir. Bu temel kavramlar içerisinde kişisel verinin tanımından yola çıkarak yer alan alt birimleri de ayrı başlıklar halinde ele alınmıştır. Çalışmamızın konusu itibariyle asli kaynağımız olan Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)’nde yer alan tanıma göre kişisel veri, “bir gerçek kişiye ait her türlü bilgi”dir. Bu tanımda yer alan her bir unsur tek tek incelendikten sonra, kişisel verilerin içinde özellikli bir konuma sahip olan hassas verilere değinilmiştir. Hassas veriler, içerdiği bilgi kategorileri bakımından özel bir ayrıma tabi tutulmuş ve hassas verilerin korunması için daha ayrıcalıklı önlemler öngörülmüştür. Hassas verilerin özelliklerini de açıkladıktan sonra, kişisel verilerin işlenme sürecinde etkin olan unsurlara yer verilmiştir.

Öncelikle çalışmanın asıl konusunu oluşturan veri işleme faaliyeti kavramına değinilmiş, devamında veri işleme sürecine katılan gruplar açıklanmıştır.

Kişisel verilerin korunması hususuna tam anlamıyla açıklık getirebilmek için kişisel verilerin korunmasına hakim olan temel ilkeleri ele almakta fayda vardır. Kişisel verilerin düzenlendiği uluslararası belgelerde, kişisel verilerin işlenmesi için izlenmesi gereken yollara ve uyulması gereken kurallara yer verilmiştir. Uluslararası kuruluşlar tarafından kabul edilen düzenlemeler ile her bir ilke günden güne hukuk sistemine katılmış, en son GDPR tarafından tüm ilkelerin kabul edilmesi ve yeni ilkeler öngörülmesi ile süreç günümüze kadar gelmiştir. Farklı hukuk sistemlerinde farklı ilkelerin benimsenmesi de mümkün olmakla birlikte, günümüzde en geniş haliyle yer verilen ve Avrupa Birliği'nde kişisel verilerin korunmasında kabul edilen temel ilkeler hukuka uygunluk, adalet, şeffaflık, amaç ile sınırlılık, en az seviyede bilgi, doğruluk, sınırlı süre ile saklama, bütünlük ve gizlilik, hesap verilebilirlik olarak ayrı başlıklar halinde açıklanmıştır.

Kişisel verilerin günümüze kadar gelişinde geçirdiği değişimlerde, kuşkusuz kişisel verilere farklı hukuk sistemleri tarafından getirilen farklı yaklaşımlar öncü olmuştur. Asıl inceleme alanımız olan Avrupa Birliği Hukuku'nda belirlenen kişisel verilerin hukuki niteliğine ilişkin yaklaşımların yanı sıra, farklı hukuk sistemlerince benimsenen farklı görüşler de mevcuttur. Kişisel verilere yönelik benimsenen bu görüşlerin en etkin olanları kişisel verilerin hukuki niteliği başlığı altına ele alınmıştır. Buna göre üç farklı teori olarak ortaya konan yaklaşımlarda kişi hakkı, fikri hak ve mülkiyet hakkı başlıklarına yer verilmiştir. Bu başlıklandırma yapılırken kişisel verilerin korunmasına yönelik geliştirilen ekonomik hak- kişi hakkı ayrımı temel alınmıştır. Kişisel verilerin korunmasına bir kişi hakkı olarak yer veren Avrupa Birliği Hukuku ile ekonomik hak olarak kabul eden Anglo Amerikan Hukuku görüşleri açıklanmaya çalışılmıştır.

Kişisel verilerin işlenmesinde asıl olan işlemenin hukuka aykırılığıdır. Bu sayede yetkisiz ve kötü niyetli işlemlerin önüne geçmek adına kişisel verilerin mümkün olan en az seviyede işlenmesi hedeflenmiştir. Ancak ilerleyen teknoloji ile birlikte kişisel verilerin işlenmesi bir mecburiyet halini aldığı anda, bu işlemenin hukuka uygun bir hale gelmesini sağlamak için işlemenin sahip olması gereken temel unsurlar mevcuttur. Bu unsurlar kişisel verilerin işlenmesinde hukuka uygunluk

halleri başlığı altında ele alınmıştır. Buna göre işlenmesi temelde hukuka aykırı olan kişisel verilerin, hangi durumlarda hukuka uygun bir şekilde işlenebileceği açıklanmıştır. Genel olarak kişisel verilerin işlenmesini hukuka uygun hale getiren nedenler veri sahibinin rızası, sözleşmenin gereğinin yerine getirilmesi, hukuki yükümlülüğün yerine getirilmesi, hayati menfaatin korunması, kamu görevinin yerine getirilmesi, meşru menfaatlerin korunması başlıkları altında ele alınmıştır. Kişisel verilerin işlenmesini hukuka uygun hale getiren sebeplerde hassas verileri diğer verilerden ayırma yoluna gidilmiştir. Sahip olduğu önem nedeniyle, işlenmesi daha güç gerekçelere bağlanan hassas verilerin işlenmesinde hukuka uygunluk nedenleri ayrı bir başlık altında ele alınmıştır.

Kişisel verilerin yaygın kullanım alanına sahip olması nedeniyle pek çok hukuk dalının alt başlığına dahil olacak biçimde ele alınması da mümkündür. Çalışmamızda kişisel verilerin korunması bir temel hak olarak kabul edilmiş olup temel haklar ve özgürlükler boyutuyla ayrı bir başlık altında incelenmiştir. Kişisel verilerin disiplinler arası yönü olması nedeniyle bir hak olarak da birden çok başlık altına dahil olması gündeme gelmektedir. Bu yönüyle kişisel veriler, en sıkı ilişkili olduğu haklar olarak öne çıkan özel hayatın gizliliği hakkı, düşünce ve ifade özgürlüğü, unutulma hakkı ve bilgi edinme hakkı olarak ayrı gruplar içerisinde incelenmiştir.

İkinci bölümde kurumlar ve düzenlemeler bazında kişisel veriler konuları ele alınmıştır. Geçmişten günümüze kişisel verilerin geçirdiği süreç ve bu sürecin uluslararası belgelere yansımaları, kurumlar bazında kişisel verilerin işlenmesi konusunda incelenmiştir. Kronolojik sıra ile bakıldığında kişisel verilerin korunması hususunda ortaya çıkan ilk uluslararası belge uygulamada “OECD Rehber İlkeleri” olarak da anılan OECD Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler’dir. OECD Rehber İlkeleri’nden sonra, kişisel verilerin korunması hususu Avrupa Birliği’nde 108 Sayılı Avrupa Konseyi Sözleşmesi ile düzenlenmiştir. Teknolojinin gelişmesi ile birlikte önemi artan kişisel verilerin korunmasına yönelik kapsamlı bir düzenleme ihtiyacı doğmuştur. Bu ihtiyacı karşılamak üzere, “95/46/EC Sayılı Yönerge” olarak da anılan 95/46/EC Sayılı Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği Yönergesi yürürlüğe konmuştur. Avrupa Birliği bünyesinde, Temel Haklar

Şartı, kişisel verilerin korunmasını bir temel hak olarak kabul eden ilk düzenleme olmuştur. 95/46/EC Sayı Yönerge'nin üye ülkelerin içi hukukunda uygulanması ile ilgili sorunlar ve ilerleyen teknolojinin de etkisiyle, en son kişisel verilerin korunmasının düzenlendiği metin olarak Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation- GDPR) 2016 yılında kabul edilmiştir.

Kişisel verilerin korunmasıyla ilgili düzenlenen belli başlı uluslararası belgeler tek tek başlıklar altında incelendikten sonra, GDPR'nin kişisel verilerin korunması amacıyla taraflara yüklediği haklar ve yükümlülükler ele alınmıştır. İlk olarak veri sahibinin hakları başlıklar altında açıklanmaya çalışılmış, devamında veri sorumlusu ve veri işleyenin yükümlülüklerine değinilmiştir.

Çalışmamızda hak ve yükümlülüklerin devamında, bu hak ve yükümlülüklerle uygunluğu denetleyen ve düzenleyen kurumlar incelenmiştir. GDPR'de yer aldığı sıralama doğrultusunda önce denetim makamları, denetim makamlarının görev ve yetkileri ele alınmış, sonrasında Avrupa Veri Koruma Kurul'u açıklanmıştır. Denetleyici ve düzenleyici kurumların görevleri ve işleyişinin akabinde bu kurumlar vasıtasıyla hakların ve menfaatlerin nasıl korunabileceği de işlenmiştir. Hak ve menfaatleri koruma yolları başvuru türüne göre başlıklara ayrılmış ve idari, hukuki ve cezai yollar olmak üzere üç ana başlık altında toplanmıştır. Son başlık olan Avrupa Birliği'ne üye ülkeler bazında kişisel verilerin incelenmesinde ise, Avrupa'nın iki lokomotif ülkesi kabul edilen Almanya ve Fransa örnekleri ele alınmıştır. Avrupa Ekonomik Topluluğu'nun kurucu üyeleri arasında yer alan Almaya ve Fransa üstlendikleri bu öncü rolü Avrupa'da birlik olma yolunda giden siyasi, ekonomik ve hukuki bütünleşmede de sürdürmüştür. Avrupa Birliği tarihindeki önemli yerleri de dikkate alındığında, kişisel verilerin korunması konusunda gerek Federal Alman Anayasa Mahkemesi'nin gerek Fransa'nın kişisel verilerin korunmasını denetleme kurulu olan CNIL'in da öncü kararlarının etkisiyle örnek ülkeler olarak Almanya ve Fransa incelemesi yapılmıştır.

BİRİNCİ BÖLÜM

AVRUPA BİRLİĞİ HUKUKUNUN TEORİK ZEMİNİNDE KİŞİSEL VERİLERİN KORUNMASI

Kişisel verilerin korunmasının önemi, bilgi sistemlerinde gelişmeler yaşanması ile birlikte, elektronik ortamda veri akışının çoğalmasıyla birlikte artırmıştır. Günümüzde teknolojik olanakların gelişmesiyle birlikte bireyler üzerindeki gözetim öncesine göre çok daha fazladır. Kişisel verilerin günümüzde ticarî meta hâline getirildiği görülmektedir¹. Ticari nesne haline gelen bilgiler üzerinde mevcut veri koruma mekanizmalarında tanınan kontrol çok kapsamlı değildir. Bu tanımdan yola çıkılarak oluşturulan veri koruma mevzuatlarının temelinde yer alan şeffaflık, bilgi güncelliği, doğruluk ile veri güvenliği ve hakların kullanılması gibi ilkelerin yer aldığı görülmektedir.

Kuruluş felsefesinde; barış, özgürlük, refah, demokrasi ve hukukun üstünlüğü ilkelerinin yer aldığı Avrupa Birliği, Avrupa coğrafyasında olduğu kadar küresel düzeyde de etkili olmayı hedefleyen bir bütünleşme çabasıdır. Avrupa Birliği eşitlik, insan saygınlığı, insan onuru, temel hak ve özgürlüklerin korunması, demokratik kurumların varlığı, hukukun üstünlüğü ve şeffaflığın sağlanması gibi genel anlamda kabul görmüş ortak değerler üzerine kurgulanmıştır. Kişilerin, malların, hizmetlerin, sermayenin ve bilginin serbestçe dolaşabilmesi için iç hukuklarda çalışmalar yapan Avrupa Birliği'nde serbestçe dolaşamayan şey; Birlik vatandaşlarının kişisel verileridir².

Bu denli özel niteliklere sahip bir alanda, gelişen teknolojiye bağlı olarak yakın geçmişten günümüze dek artan bir ivmeyle düzenleme yapılması; gerek üçüncü ülkelerin gerek Avrupa Birliği'nin gündeminde önemli bir noktaya ulaşmıştır. Özellikle son yıllarda kişisel verilerin elde edilmesi, işlenmesi, transfer edilmesi işlemleri son derece büyük boyutlara ulaşmış ve kişisel verilerin korunması hakkına olan ihtiyaç artmıştır. Sosyal medyanın da hayatımıza girmesiyle yeni bir boyut kazanan bu veri akışı yalnızca bankacılık, sağlık, iş hayatı, eğitim, ticaret alanlarıyla sınırlı olmaktan çıkmıştır.

Veri koruma ihtiyacının artmasıyla birlikte, 2018 yılının Mayıs ayı itibarıyla Avrupa Birliği'nde kişisel verilerin korunmasıyla ilgili Avrupa Birliği Genel Veri

¹ Habip Oğuz, “ Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum”, **Uyuşmazlık Mahkemesi Dergisi**, Cilt:1 Sayı:3, 2013, s. 3

² Doğan Kılınç, “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 61, Sayı: 3, 2012, s.1118.

Koruma Tüzüğü (General Data Protection Regulation – GDPR) yürürlüğe girmiştir. Bu düzenleme öncesinde de Avrupa Birliği’nde kişisel verilerin korunması hakkı çerçevesinde yasal zemin oluşturan 95/46/EC sayılı AB Veri Koruma Yönergesi (Data Protection Directive- DPD) verileri toplanan kişilerin hak ve yükümlülüklerini belirlemek amacıyla kullanılmıştır. GDPR, tüm Avrupa Birliği sakinleri ve pek çok Avrupa Birliği kurumu için bağlayıcı düzenlemeler içermektedir. Bu düzenlemeleri incelemeden önce, konuyu daha iyi açıklığa kavuşturabilmek adına kişisel verilerin korunması hukukuna ilişkin tarihsel süreci ele almak yerinde olacaktır.

I. KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ

Kişisel verilerin korunmasıyla ilgili hukuki sorunlar, büyük ölçüde kişisel verilerin otomatik olarak işlenmeye başlamasıyla gündeme gelmiş olsa da kişilerin kendilerine ait verilerin gizli kalmasına yönelik düşünceleri neredeyse insanlığın başlangıcından beri vardır. Örneğin, M.Ö. 5. yüzyılda ortaya çıkan, hekimin hastalarıyla ilgili öğrenmiş olduğu bilgileri sır saklama yükümlülüğü çerçevesinde saklama ve açıklamama yükümlülüğüne ilişkin Hipokrat yemini, kişisel verilerin korunması konusundaki en eski örneklerden birisidir. İzleyen dönemlerde bunu, din adamlarının günah çıkartma sırasında öğrendiği bilgilere ilişkin sır saklama yükümlülüğü, memurların görev sırrı, banka sırrı, avukatların sır saklama yükümlülüğü gibi farklı meslek gruplarından kişilerin sır saklama yükümlülükleri izlemiştir³.

Neredeyse insanlık tarihi boyunca var olan kendine özel olanı saklı tutma duygusu; yıllar geçerek temel haklar ve özgürlükler bilincinin artmasıyla, kişisel bilgilerin saklı tutulmasını isteme hakkını doğurmuştur. Gelişen teknoloji ile kişisel verilerin elde edilmesinin son derece kolaylaşması, ülkeleri bu konuda farkındalığa ve önlem almaya itmiştir. Özellikle 1960’lı yıllarda modern anlamda bilgisayarların üretilmesiyle hızlanan bu süreç, 1970 yılında somut bir görünüme kavuşmuştur. Bu bağlamda 1970 yılında Almanya’nın Hessen Federe Devleti’nde kabul edilen kanun, kişisel verilerin korunması alanında dünya çapındaki ilk yasal düzenleme olmuştur. Bu kanun ile elektronik işlenen kişisel verilerin yetkisiz üçüncü kişilere karşı

³ Elif Küzeci, **Kişisel Verilerin Korunması**, Turhan Kitabevi, Ankara 2010, s.18.

korunması gerektiği, veri işleme faaliyetinde bulunan kişilerin verilerin içeriği hususunda sır saklama yükümlülüğü ve veri sahibinin hakkındaki yanlış verileri düzeltilmesini talep hakkı düzenlenmiştir. İsveç'te 1973, Almanya'da 1976, Danimarka, Norveç ve Fransa'da ise 1978 yıllarında kişisel verilerin korunmasına ilişkin yasal düzenlemeler oluşturulmuştur. Avusturya'da 1980 yılında, İsviçre'de 1992 yılında Federal Kişisel Verilerin Korunması Kanunu yürürlüğe girmiştir. İngiltere'de de 1998 yılında Veri Koruma Kanunu yürürlüğe girmiştir.⁴ Bu düzenlemelerin akabinde ise çalışmamızın ilerleyen kısımlarında ayrıntılarıyla değinilecek olan kurumsal düzenlemeler gelmiştir. Bunların başlıcalarından biri Ekonomik Kalkınma ve İşbirliği Örgütü (OECD)'nin 1980 yılında kişisel alanın ve sınır aşan kişisel verilerin korunmasına ilişkin belirlediği rehber ilkelerdir. OECD'nin hemen ardından 1981 yılında Avrupa Konseyi tarafından 108 Sayılı Kişisel Nitelikli Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına İlişkin Sözleşme yayınlanmış ve kişisel verilerin işlenmesi Avrupa Topluluğu bağlamında özel bir korumaya tabi tutulmuştur. Birleşmiş Milletler de 1990 yılında 45/95 sayılı Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler adlı metni yayınlarak kişisel verilerin bilgisayar ile işlenmesinde genel bir koruma alanı oluşturmaya çalışmıştır.

A. Avrupa Birliği'nde Kişisel Verilerin Tarihsel Gelişimi

Kişisel verilerin korunmasına ilişkin Avrupa Birliği çapında yapılan ilk düzenleme Avrupa Konseyinin 1968 yılında kabul ettiği, "Modern Bilimsel ve Teknolojik Gelişmeler ve İnsan Hakları Hakkında 509 sayılı Tavsiye Kararı" dır. Bu karar ile birlikte ilerleyen teknolojinin kişilik haklarını tehdit eden boyutlara ulaşabileceği ortaya konmuştur. 509 Sayılı Karar'ın ardından "Yerel Kamu Kurumlarında Bilgisayarların Kullanılması Hakkında 557 Sayılı Tavsiye Kararı" alınmış ve bu kararlar birlikte vergilendirme gibi sınırlı amaçlar için zaruri olan

⁴ M. Serdar Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, 2. Baskı, On İki Levha Yayınları, İstanbul, 2019, ss.5-6

verilerin saklanması ibaret olacak bilgi bankalarına ihtiyaç duyulduğu belirlenmiştir⁵.

Verilerin korunması hususunda düzenlemeler içeren ilk uluslararası belge 108 Sayılı Avrupa Konseyi Sözleşmesi olup Sözleşme, Strazburg'da 28 Ocak 1981 tarihinde imzaya açılmıştır. 108 Sayılı Avrupa Konseyi Sözleşmesi 1 Ekim 1985 tarihinde yürürlüğe girmiştir. Türkiye 28 Ocak 1981'de Sözleşmeyi ilk imzalayan devletlerden olmuştur⁶. Bu sözleşme, "Modern Bilimsel ve Teknolojik Gelişmeler ve İnsan Hakları Hakkında 509 sayılı Tavsiye Kararına" bağlı olarak imzalanmıştır. Sözleşme'nin asıl amacı, Avrupa Birliği bünyesindeki ülkelerde, veri koruma sisteminde yeknesaklığı sağlamak ve üye ülke vatandaşlarının temel hak ve özgürlüklerini korumaktır. Avrupa İnsan Hakları Sözleşmesi'nde kişisel verilerin korunmasına ilişkin bir maddenin yer almaması, 108 Sayılı Sözleşme'nin imzalanmasını gerektiren önemli bir etken olmuştur⁷.

108 Sayılı Avrupa Konseyi Sözleşmesi'nden sonra veri koruması konusunda ulusal çalışmalar da hızlanmış ve bazı üye ülkeler mevcut kanunlarını Sözleşme'ye bağlı olarak yeniden yapılandırırken bazı ülkeler de yeni veri koruma kanunları hazırlamışlardır. 108 Sayılı Sözleşme'nin ardından üye ülkelerin mevzuatlarını yeniden gözden geçirme konusunda itici olan güç Avrupa Birliği'nin 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Verilerin Serbest Dolaşımı Bakımından Bireylerin Korunmasına ilişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi olmuştur⁸.

Her ne kadar kişisel verileri kapsamlı olarak ele alan bir düzenleme olsa da 95/64/EC sayılı Yönerge, baş döndürücü bir hızla ilerleyen teknolojik gelişmelerin gerisinde kaldığından günümüz koşullarına ayak uyduran normatif düzeyde, yeni bir düzenleme ihtiyacı doğmuştur. Avrupa Birliği'nde kişisel verilerin korunmasıyla ilgili normatif boyuttaki ilk düzenleme olan 95/46/EC sayılı Avrupa Birliği Veri Koruma Yönergesi; bilişim teknolojilerinin günümüzdeki kadar gelişmiş olmadığı bir dönemde kabul edilmiştir ve kabul edilme amacı olan Avrupa Birliği ülkelerinde

⁵ Murat Uygun, **Avrupa Birliği' nin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması**, (Yayımlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2010, s.11.

⁶ Ufuk Dal, "Avrupa Birliği Genel Veri Koruma Tüzüğü' nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslar arası Hukukta Meşruiyeti", **Kişisel Verileri Koruma Dergisi**, Cilt: 1, Sayı: 1, 2019, s.22.

⁷ Nur Halet Avcıoğlu, **Türk Hukukunda Kişisel Verilerin Korunması Hakkı**, (Yayımlanmamış Yüksek Lisans Tezi), KTO Karatay Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2018, s.41.

⁸ Uygun, s.31.

kişisel verilerin korunması hukukunda yeknesaklığı sağlamayı da yerine getirememiştir. Bu durum, Avrupa Birliği'nde kişisel verileri korumaya yönelik kurallar bütününün yeniden düzenlenmesi gereğini ortaya çıkarmıştır ve bu ihtiyaçtan hareketle Mayıs 2016'da Avrupa Birliği Genel Veri Koruma Tüzüğü kabul edilmiştir⁹.

B. Kişisel Verilerin Tarihsel Gelişimine Etki Eden Olgular

Avrupa Birliği'nde gerek topluluk bazında, gerek tek başına ülkeler bazında kişisel verilerin korunmasının bu denli önem kazanması 70'li yıllarda başlamış, 90'lı yılların sonuna kadar normatifleşme süreci devam etmiştir. Kişisel verilerin korunmasının bu denli önem arz etmesinin sebebi ise ülkelerin münhasır alanda önem verdiği mahremiyet kavramından yola çıkmıştır. Avrupa Birliği'nin oluşumunun temelinde bir serbest dolaşım ve serbest ticaret amacının yatması, bu serbest dolaşımın kişisel verileri de kapsar nitelikte olması ise ülkeleri harekete geçirmiştir. Zira üye ülkelerden özellikle Almanya ve Fransa gibi Birlik içinde sözü geçen ve “insan onuru” ile “kendi kaderini tayin etme” hakkına anayasal boyutta önem veren ülkeler, Avrupa Birliği bazında bir veri koruma düzenlemesinin oluşmasında itici güç olmuştur. Bu konuda Federal Alman Anayasa Mahkemesi 15 Aralık 1983 tarihli ve 1 BVR 209/83 sayılı nüfus sayımlarına ilişkin kararında kişisel verilerin, temel haklar kapsamında yer alan kişilik hakkı ile sınırsız olarak işlenmeye karşı korunacağını ortaya koymuştur¹⁰. Federal Mahkeme kararda, 1983 yılında hazırlanan Nüfus Sayımı Yasası'ndan yola çıkarak modern veri işleme kapsamında genel kişilik hakkının bireyin kişisel verilerin sınırsız olarak toplanması, depolanması, kullanılması ve paylaşılmasına karşı korunmasını kapsadığını kabul etmiştir. Bu hakkın ilke olarak kişisel verilerinin ifşası ve kullanımına kendilerinin karar vermesi için bireye tanınan yetkiyi garanti ettiğini ve kişiselleştirilmiş bilgi olarak toplanıp işlenen ve anonim hale getirilmeyen kişisel veriler ile istatistiksel amaçlı veriler arasında bir ayrım yapılması gerektiğini belirtmiştir. Verilerin

⁹ Murat Volkan Dülger, “Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”, **Yaşar Hukuk Dergisi**, Cilt: 1, Sayı: 2, 2019, (GDPR Bağlamında Kişisel Veriler) s.71.

¹⁰https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html (03.01.2021)

istatistiksel amaçlarla toplandığı durumlarda, kesin ve özel bir amaç sınırlamasına tabi tutulamayacağı ancak bununla birlikte, bunu telafi etmek için bu tür bilgilerin toplanması ve işlenmesi, ilgili bilgi sistemi içindeki sınırlamalara tabi olması hususu vurgulanmıştır. Bu yönüyle nüfus sayımlarını istatistiksel faaliyet olarak değerlendiren Mahkeme, nüfus sayımları sırasında toplanan verilerin başlangıçtan itibaren amaca yönelik kısıtlamalarla sınırlı olmaması nedeniyle, nüfus sayımının bireyin kişilik haklarını ihlal edecek şekilde kayıt ve kataloglama riskini beraberinde getirme ihtimali olduğunu kabul etmiştir. Bireyin kendisine ait veriler üzerindeki haklarından yola çıkarak “bilgisel kendi kaderini tayin hakkı” olduğunu ifade eden Mahkeme, bu hakkın korunmasını sağlamak için özel önlemler alınması gerektiğine, ancak Nüfus Sayımı Yasası’nda bu hususlara riayet edilmediğinden genel kişilik hakkı ihlali söz konusu olduğuna karar vermiştir.

6698 Sayılı Kişisel Verilerin Korunması Kanunu’nun 1. maddesinde de açık bir şekilde Kanun’un amacının başta özel hayatın gizliliğini korumak olduğu vurgulanmıştır. Bu bağlamda kişisel verilerin korunmasında asıl amacın verinin kendisi değil, verinin bir parçasını oluşturduğu özel hayatın gizliliği başta olmak üzere diğer temel hakların korunmasıdır¹¹. Anayasa’da özel bir düzenleme ile koruma altına alınan kişisel verilerin korunması hakkı, Kanun’da özel yaşamın gizliliği hakkı içerisinde değerlendirilerek korunması güçlendirilmiştir.

Özel yaşam bilinciyle birlikte hayatımıza giren önemli bir kavram da mahremiyet olmuştur. “Mahremiyet kavramı ilk kez 1890 yılında Amerikalı yargıç Brandeis tarafından yalnız bırakılma hakkı; hakların en kapsamlısı ve özgür insanlar tarafından en çok değer verilen hak olarak tanımlanmıştır”¹². Günümüzde ise genel olarak mahremiyet “bireylerin kendi kendilerine kalabildikleri, diledikleri gibi düşünüp yaşayabildikleri, başkalarıyla kuracakları ilişkiye diledikleri gibi karar verebildikleri bir alan ve bu alanda sahip olunan hak”¹³ olarak tanımlanmaktadır. Günümüzde ise bilgi ve teknolojilerinde meydana gelen gelişmeler neticesinde pek

¹¹ Çekin, s.21

¹² M. Cumhur İzgi, “Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri”, **Türkiye Biyoetik Dergisi**, Cilt:1, Sayı:1, 2014, s. 26.

¹³ Mehmet Yüksel, “Mahremiyet Hakkı ve Sosyo- Tarihsel Gelişimi”, **Ankara Üniversitesi Siyasal Bilimler Fakültesi Dergisi**, Cilt:58, Sayı:1, 2003 (Mahremiyet Hakkı), s.182. Mahremiyet kavramının farklı düşünürler tarafından ortaya konan kavramları için bakınız: İlhan Korkmaz, “Facebook ve Mahremiyet: Görmek ve Gözetle(n)mek” **Yalova Sosyal Bilimler Dergisi**, Cilt:3, Sayı:5, 2013, ss.116-117.

çok alanda hızla değişimler yaşanmış, bu değişimler de bireylerin özel yaşamları ve mahremiyetlerinin korunması açısından risk teşkil etmeye başlamıştır. Bu nedenle bireyler özel iletişim araçlarıyla kurdukları iletişimin gizliliğinden emin olamaz hale gelmişlerdir¹⁴. Bireylerin hissettiği bu güvensizlik duygusu, mahremiyet kavramının Dünya çapındaki bilinirliğinin artmasını sağlamıştır. Hatta bazı Avrupa ülkeleri de İngiliz kökenli olan bu kavramı kendi bireysel koruma ve veri işleme hakkındaki metinlerinde kullanmıştır. Diğer bazı ülkeler ise her şeye rağmen, farklı bir terminolojide kalma yönünde müzakere etmişlerdir (Fransa *libertés*, İsveç *integrité*). Bu birliktelikten yola çıkan Fransa ve İsveç, Almanya'yı da yanlarına dahil ederek kişilik haklarının yasal korunmasını pekiştirmek amacıyla özel yasal düzenlemeler yapan ve kişisel verilerin işlenmesini düzenleyen ilk Avrupa ülkeleri arasında olmuştur.¹⁵ Tüm bu girişimler ise, mahremiyet ve özel hayat kavramının tüm Dünya'da, özellikle araştırma konumuz olan Avrupa'da ne denli yankı bulan kavramlar olduğunu ve kişisel verilerin korunması kavramının vücut bulmasına temel oluşturduğunu göstermektedir.

Hukuk devleti ilkesine dayanan bir anayasal düzende insan onuru ve özgürlükleri, bütün hukuk düzeninin en yüksek amacını oluşturmaktadır. İnsan onuru kavramının içeriğinin hukuksal açıdan somut bir şekilde ortaya konmasının zor olduğu ifade edilse de, Alman Anayasa Mahkemesi'nin oluşturduğu "obje formülü" ne göre; şayet insan kamusal organların faaliyetleri karşısında basit bir obje veya araç haline indirgeniyorsa insan onurunun ihlalinden söz edilecektir. Bu çerçevede insanın devlet içerisinde basit bir obje olarak alçaltılmasının insan onuruna aykırı olduğu ve devletin insanı kişiliği içerisinde kayıt altına alma ve yine ona bir eşya gibi muamele etme hakkını kendisinde görmesinin insan onuru ile bağdaşmadığı ifade edilmiştir. Dolayısıyla özel yaşamın gizliliğinin kaldırılarak "şeffaf insan" tipinin yaratılması yasağı ve bireyin kişisel verilerinin korunması hakkı insan onuru temeline dayandırılmaktadır¹⁶.

¹⁴ Mehmet Yüksel, "Modernleşme ve Mahremiyet", *Kültür ve İletişim Dergisi*, Cilt:6, Sayı:1, 2003 (Modernleşme ve Mahremiyet), s.76.

¹⁵ G. Gonzalez Fuster, *The Emergence of Personel Data Protection as a Fundamental Right of the EU*, Springer, Belçika, 2014, ss.37- 49

¹⁶ Oğuz Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta Yayınları, İstanbul, 2008, s.129-130 dan aktaran Uygun, s.4

II. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN KAVRAMLARI VE TEMEL İLKELERİ

Kişisel verilerin korunması hukukunun kavramlarına değinmeden önce kişisel veri kavramını açıklamak faydalı olacaktır. Kişisel veri GDPR'nin 4. maddesinde; *“tanımlanmış veya tanımlanabilir bir gerçek kişiye ait her türlü bilgi”* olarak ifade edilmiştir. Bu tanımdan da anlaşılacağı üzere GDPR, kişisel veri kavramını ‘her türlü bilgi’ diyerek geniş kapsamlı olarak yorumlamıştır. Yine bu tanımlamada dikkat çeken diğer husus da kişisel veriyi yalnızca gerçek kişilere ait olarak görmek ve tüzel kişilere kişisel verilerin korunmasını isteme hakkını tanımamaktır. Kişisel veri kavramını en son haliyle tanımlayan GDPR, kendinden önce yürürlüğe giren düzenlemelerden ayrılmadan benzer bir tarifte bulunmuştur. Şöyle ki; 1981 yılında imzalanan 108 Sayılı Avrupa Konseyi Sözleşmesi'nin 2. maddesinde kişisel veri; *“kimliği belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgiler”*, 95/46/EC Sayılı Yönerge'nin 2/1-a maddesinde ise; *“fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere; doğrudan veya dolaylı olarak tespit edilebilen, tespit edilmiş veya tespit edilebilir gerçek kişiye ilişkin herhangi bir bilgi”* olarak tanımlanmıştır. Bu tanımlardan yola çıkarak, Avrupa Birliği'nin her düzenlemede kişisel veri kavramını geniş yorumladığı kanısına varılabilecektir. Tüm bu tanımlarda ve Avrupa Birliği'nin kişisel verilere yaklaşımında görüleceği üzere, kişisel verilerin korunması hukukuna temel olan belli başlı kavramlar mevcuttur.

A. Kişisel Veriye İlişkin Kavramlar

1. Gerçek Kişi

Kişisel verilerin korunması hukukunun içinde yer alan, GDPR'de başlangıçta belirtilmiş olan ilk husus; bir gerçek kişi olmadır. Bu kavram, kişisel verilerin korunması hakkından kimlerin faydalanabileceğini açıkça ortaya koymaktadır. Gerek Avrupa Birliği'nde gerek ülkemizde kişisel verilerin korunmasına ilişkin yapılan hukuki düzenlemelerde, tüzel kişiler korumanın dışında bırakılmıştır. Bu

nedenle korumadan yararlanacak kişiyi belirlemek adına öncelikle gerçek kişinin varlığının tespitinin yapılması önem arz etmektedir.

Kişisel verilerin korunmasını talep etme hakkının gerçek kişi olarak sadece insanlara tanındığını söylemek mümkündür. Yalnızca Avrupa’da Birlik bazında yapılan düzenlemelerde değil, ülkelerin kendi iç hukukunda yaptığı düzenlemelerde de kişisel verilerin korunması hakkının gerçek kişilere tanındığı görülmektedir. Örneğin Avusturya’da “Kişisel Veriler İşlenirken Gerçek Kişilerin Korunmasına İlişkin Federal Yasa” adlı düzenlemeye bakıldığında; yasanın adında dahi düzenlemenin yalnızca gerçek kişiler için yapıldığı görülmektedir. Yine yasanın içeriğinde de kişisel verilere ilişkin korumaların gerçek kişilere yönelik olduğu hüküm altına alınmıştır¹⁷.

Doktrinde, kişisel verilerin korunmasından tüzel kişilerin faydalanıp faydalanamayacağı hususunda tartışmalar mevcuttur. *Tezcan*; “özel hayat gerçek kişilerle ilgili bir kavramdır. Tüzel kişiler için ise ancak “ticari gizliliğin korunması” söz konusu olabilir. Ticari işletmelerin şeffaflığı bir gereklilik olarak düşünülürse, sadece gerçek kişilerin özel hayatının bilgisayar karşısında korunmasıyla yetinmek daha yerinde olacaktır”¹⁸ görüşünü savunmaktadır. Benzer bir şekilde *Develioğlu* da; Kişisel verilerin korunması hakkının, bir temel hak olan özel hayatın gizliliği hakkından doğduğunu savunmaktadır. Özel hayat da gerçek kişilere özgü bir kavram olduğundan, kişisel verilerin korunmasını isteme hakkı yalnızca gerçek kişilere tanındığını kabul etmektedir¹⁹.

Tüzel kişilere ait kişisel verilerin de korunması gerektiğini savunan görüşe göre, tüzel kişilerin verilerinin korunması bu verilerin içinde gerçek kişilere ait kişisel veriler de bulunduğu müddetçe önemlidir. Örneğin, bir şirketin yönetim kurulu üyesinin verilerine şirket vasıtasıyla ulaşılabilmesi bu şekildedir²⁰. Ancak her ne kadar tüzel kişinin verilerinden yola çıkarak gerçek kişinin verilerinin elde

¹⁷ Kanun metni için bakınız: “Undesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten”
<https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597> (04.01.2021)

¹⁸ Durmuş Tezcan, “Bilgisayar Karşısında Özel Hayatın Korunması”, **Anayasa Dergisi**, Cilt: 8, 1991, s. 389.

¹⁹ H. Murat Develioğlu, **6698 Sayılı Kişisel Verilerin korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayınları, İstanbul, 2017, s.30

²⁰ Sedat Erdem Aydın, **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, Oniki Levha Yayıncılık, İstanbul, 2015, s.8.

edilebilmesi ihtimali gündeme gelse de; bu durumda gerçek kişi yine kendisine tanınan haktan yararlanarak kişisel verilerinin korunmasını talep edebilecektir. Tüzel kişi bünyesinde yer alan gerçek kişi, kendisi başlı başına bir birey olmasından kaynaklanan bu korunma hakkından yararlanacaktır. Zira mevzuattaki düzenlemeler açık ve net bir şekilde kişisel verilerin korunmasının yalnızca gerçek kişilere tanınan bir hak olduğunu hüküm altına almaktadır.

GDPR’de kişisel verilerin korunmasından yalnızca gerçek kişilerin yararlanabileceği açıkça belirtilmiş olmasıyla birlikte, üyelerin iç hukuklarında oluşturacakları düzenlemelerde tüzel kişileri de koruma kapsamına almasının önünde bir engel de bulunmamaktadır. Öyle ki; Fransa, İsveç, Hollanda, Polonya ve Estonya ilgili kanunlarında kişiyi tanımlarken “gerçek kişi”; Almanya “birey, gerçek şahıs”; Finlandiya “özel birey, gerçek kişi” terimlerini kullanmışlardır. Bunun yanı sıra; Danimarka ve Lüksemburg ile Avrupa Birliği üyesi olmayan İzlanda, Norveç ve İsviçre de veri koruma yasaları ile tüzel kişilere ait verileri koruyan ülkelerdendir²¹.

Ölen kişilerin verilerinin korunmasına ilişkin husus ise GDPR’de değil, gerekçesinde yer almaktadır. GDPR’nin 27. gerekçesinde; Tüzük’ün ölen kişilerin kişisel verileri açısından geçerli olmadığını vurgularken; Üye Devletlerin GDPR’deki düzenlemelerin yanı sıra, ölen kişilerin kişisel verilerini koruyucu düzenlemeler yapabileceğini belirtmiştir. Bulgaristan ve Estonya, bu yönde düzenlemelerin kabul edildiği üye devletler arasındadır. İsveç ve Birleşik Krallık ise sadece hayatta olan kişilerin verilerini kişisel veri olarak kabul etmiştir²².

Cenin açısından kişisel verilerin korunmasında ise; hamilelik süresince ana rahminde bulunuyor olması nedeniyle ceninin verileri, aynı zamanda annenin verileri olarak da kabul edilebileceği görüşü savunulmuştur. Zira ceninle ilgili bilgiler, aynı zamanda annenin kimliğini belirlenebilir kılacak verilerdir. Dolayısıyla ceninin kişisel verileri, cenini taşıyan anne açısından korunmak zorundadır. Bu nedenle; cenine ilişkin veriler hem cenin açısından hem de anne açısından korunur²³.

²¹ Melike Köse Aysun, **Kişisel Verilerin Kaydedilmesi Suçu**, Seçkin Yayıncılık, Antalya, 2018, s.31.

²² Onur Doğan Yörük, (AB) 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Kişisel Verilerin Korunması, (Yayımlanmamış Yüksek Lisans Tezi), İzmir Ekonomi Üniversitesi Lisansüstü Eğitim Enstitüsü, İzmir, 2019, s.11.

²³ Furkan Güven Taştan, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, 2. Baskı, On İki Levha Yayıncılık, İstanbul, Kasım 2017, s.36.

2. Kimliđi Belirli veya Belirlenebilir Olma

Veri korumasından yararlanacak kiřinin gerek kiři olduđunun tespitinin devamında bu gerek kiřinin belirli veya belirlenebilir olması hususu nem kazanmaktadır. Kiřinin kimliđinin belirli veya belirlenebilir olduđunun tespit edilmesi, veri sahibinin insanlar tarafından ayırt edilebilmesi veya ayırt edilmesinin mmkn hale gelmesi anlamına gelmektedir. Veri sahibini, toplumdaki diđer kiřilerden ayırt etmeye yarayacak bilgilerin neler olduđu her somut olayın zelliklerine gre deđerlendirilmelidir. Bir gerek kiřinin kimliđini belirlemek iin kullanılacak bazı temel ayırt edici zellikler mevcuttur. Bu anlamda somut olayın tm zellikleri incelenirken kiřinin kimliđinin belirlenebilmesi amacıyla kullanılabilecek resmi siciller, kayıtlar zellikleri gz nnde tutulmalıdır²⁴.

Kiřinin belirli veya belirlenebilir olması gerektiđi kuralı, kiřisel verilerin korunması ve mahremiyet dřncesinden kaynaklanmaktadır. Verinin kimliđi belirli veya belirlenebilecek bir veri sahibine ait olması, korumanın kapsamını belirlemek aısından nemlidir. Zira veri sahibinin kim olduđu belirlenemiyor ve belirlenemeyecek durumda ise, bu verilerin iřlenmesi kiřisel verilerin korunması kapsamında deđerlendirilmez²⁵. Bu bađlamda, bir kiřiyle iliřkilendirilemeyen veriler olarak tanımlanan anonim veriler, kiřisel veri kabul edilmemektedir. Anonim veriyle sıklıkla karıřtırılan psdonimize veriler ise kiřinin belirlenmesinde kullanılabileceđinden kiřisel veri olarak kabul edilmektedir²⁶. Psdonimizasyon GDPR'nin 4/5. maddesinde tanımlanmıřtır. Bu tanıma gre psdonimizasyon; kiřisel verilerin bir gerek kiřiyle iliřkilendirilmemesini sađlamak iin, kiřisel veriden ayrı olarak bir takım ek bilgilerinin tutulması ve verinin bu ek bilgiler olmadan bir gerek kiřiye izafe edilememesidir. Genellikle, kimlik bilgileri ile onlara denk gelen takma ad veya kodların listeleřtirilmesi veya kriptolanması ile yapılır. Psdonimleřtirilmiř veriler, ek bilgilerle birlikte kullanıldıklarında, kiřilerin dolaylı olarak

²⁴ Elif Mendos Kuřkonmaz, **Kiřisel Verilerin Trk Ceza Kanunu Kapsamında Korunması**, (Yayımlanmamıř Yksek Lisans Tezi), İstanbul niversitesi Sosyal Bilimler Enstits, İstanbul, 2013,s.10.

²⁵ Stewart Room, **Data Protection & Compliance in Context**, Swindon, United Kingdom, The British Computer Society Publishing and Information Product, 2007, s.37 den aktaran Ayře iđdem Ayzger, **Elektronik Haberleřme Sektrnde Kiřisel Verilerin Korunması**, 2. Baskı, Beta Yayınları, İstanbul, 2019, s.19

²⁶ Yrk, s.10.

belirlenebilmesini sağlar. Örneğin; öğrencilerin sağlık bilgileri ile ilgili okul tarafından tutulan bir listede öğrenci isimleri yerine bir kodlama yerleştirilmişken, o kodun hangi öğrenciye ait olduğunun tespitini sağlayan bir anahtarın varlığı halinde veri, psödonim veridir²⁷.

3. Kişiy Ait Veri

Kişisel veriy tanımlarken kullanılan bir diğer kavram da verinin belirli veya belirlenebilir bir gerçek kişiy a ait olmasıdır. Somut bir verinin tek başına, birisine izafe edilmemiş biçimde 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 tanımlanmaktadır. Anonim veriler, hem Avrupa Birliği mevzuatı hem de Kişisel Verilerin Korunması Kanunu tarafından kapsam dışı bırakılmaktadır²⁸. 2012 yılında Avrupa Birliği'ne üye devletler açısından Birleşik Krallık Bilgi Komiseri Ofisi, anonimleştirme tekniklerini açıklayan “*Anonimleştirme: Veri Koruması Risk Yönetimi Uygulama Esasları*” adlı metni yayınlamıştır. Metne göre; veri koruma mevzuatının anonimleştirilmiş veriyi korumaması, veri işleyenleri anonimleştirmeye teşvik etmekte; böylece kişilerin kimliklerini korumuş olmaktadır²⁹.

Verinin kişiy e ilişkin olması unsurunda aranan kriter, söz konusu verinin “içerik”, “amaç” veya “sonuç” yönünden kişi ile bağlantılı olmasıdır. Bilginin içerik bakımından kişiy e ilişkin olması söz konusu bilginin kişi hakkında olmasını ifade eder. Çalışan hakkında işyerinde düzenlenen dosyalar, bir hastanın tıbbi kayıtları bu duruma örnek olarak verilebilir. Bazı hallerde ise bilgi, içerik itibarıyla kişiy e ilişkin olmamasına rağmen bu bilginin kişisel veri olarak kabul edilmesi gerekebilmektedir. Örneğin, bir taşınmazın değeri genel olarak kişisel veri kapsamında değildir. Ancak bu taşınmazın değeri malikinin vergi yükümlülüğünün kapsamında belirlemek için kullanılabilir. Bu bağlamda taşınmazın değeri, kişisel veri kapsamında değerlendirilecektir³⁰.

²⁷ Develioğlu, s.36.

²⁸ Şehriban İpek Aşıkoğlu, **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, On İki Levha Yayıncılık, İstanbul, 2018 (Büyük Veri), s.10.

²⁹ Şeyma Sert, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Seçkin Yayıncılık, İstanbul, 2019, ss.28-37.

³⁰ Mendos Kuşkonmaz, s.11.

4. Her Türlü Bilgi

Avrupa Birliđi'nde kişisel veriler konusunda yürürlüğe giren tüm düzenlemelerde kişisel veriye ilişkin benzer bir tanımlama yapıldığı görülür. Bu tanımın bir ortak noktası da Avrupa Birliđi'nin kişisel veriyi; bir kişiye ait her türlü bilgi demek suretiyle oldukça geniş yorumlamış olmasıdır. Avrupa Birliđi'nin tanımına göre bir kişiye ait her türlü bilgi yani; fiziksel özellikleri, adı, soyadı, yaşı, mesleđi, sađlık durumu, adresi, doğum yeri gibi saymakla bitmeyecek kadar kişisel bilgi yani veri bulunmaktadır. Bir verinin kişisel veri olarak sayılabilmesi için veri sahibi tarafından açıklanıp açıklanmadığının da bir önemi bulunmamaktadır. Örneğin; her ne kadar bir banka işlemi için kimlik bilgisi banka personeli ile paylaşılsa da, kimlik bilgisi yine veri sahibinin kişisel verisidir. Üstelik bu verinin doğruluđu veya yanlışlığı da önemli değildir. Veriler sisteme yanlış kaydedilmiş olsa dahi, kişisel verilerin korunması kapsamına girmektedirler.

Kişisel veri olarak kabul edilen bilginin işleme yöntemi ise, bilginin niteliğini deđiştirmediğinden, kişisel veri korumasından yararlanma hakkına hâlel getirmemektedir. Yani bir bilgi ister basılı ister elektronik ortamda olsun; her türlü işleme yöntemine karşı korunmaktadır. Bu husus GDPR'nin 2/1. maddesinde açıkça; *“Bu Tüzük, kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesine ve bir dosyalama sisteminin bir parçasını oluşturan veya bir dosyalama sisteminin bir parçasını oluşturması amaçlanan kişisel verilerin otomatik yollardan başka işlenmesine uygulanır.”* demek suretiyle ortaya konmuştur.

5. Hassas Veriler

GDPR'de özel kategorili kişisel veriler olarak ifade edilen hassas veriler; kişisel verilerin daha mahrem kalma ve korunmaya muhtaç kısmına verilen isimdir. GDPR'de özel bir başlık altında ele alınan hassas verilerle ilgili bir tanım yapılmamış, hangi verilerin özel korumaya tabi olduğundan bahsedilmekle yetinilmiştir. GDPR'nin 9. maddesinde; *“İrk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiđi kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile*

biyometrik verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır.” denmektedir.

Kişilerin ırkı ve etnik kökenini, ten rengini, siyasi görüşlerini, inançlarını, sendika üyeliğini ve mahkumiyetlerini içeren verilere hassas veri adı verilir. Doktrinde hassas verileri belirtmek üzere farklı kavramlar kullanılmaktadır. Bu bağlamda, veri koruma kanunlarında genellikle "hassas veri" kavramı kullanılmakla birlikte "özel kategorili kişisel veriler", "özel kişisel veriler" ve hatta "özel korumaya layık olan veriler" kavramları da kullanılmaktadır³¹.

Hassas veri kategorisinde yer alan bilgiler, toplumsal kaygılar nedeniyle kişilerin mahremiyetlerini ifşa edebilecek türdedir. Bu nedenle hassas verilerin özel bir korumaya sahip olmaları gerektiği kabul edilmiştir. Kişiye ait bazı bilgilerin hassas olan veri olarak tanımlanması ve bu kapsamda özel korumaya tabi olarak işlem görmesi, temel hak ve özgürlükler ile bu verilerin daha sıkı bağının olmasının sonucudur. Bu tür verilere karşı olan korumaya riayet edilmeyip hassas veriler saldırıya uğradığı takdirde, veri sahibinin uğrayacağı mağduriyetin daha büyük olacağı düşünülerek böyle bir yaklaşım izlenmektedir³².

Veri koruma mevzuatına sahip olan bütün ülkelerde de bahsettiğimiz nitelikteki veriler hassas veri olarak kabul edilmiştir. Ancak bunlardan farklı olarak genetik bilgilere (Polonya, İzlanda, Estonya ve Bulgaristan), biyometrik bilgilere (Slovenya, Slovakya, Çek Cumhuriyeti), milli kökene (Çek Cumhuriyeti ve Slovenya), siyasi partilere veya hareketlere (Slovakya), dernek üyeliğine (İtalya), engel durumuna (Estonya), bağımlılıklara (Polonya), ten rengine, alkol, tıbbi ilaç ve uyuşturucu kullanımına, cinsel yaşama ve cinsel davranışlara (İzlanda), cinsel tercihlere ve cinsel yaşama, sosyal görüşlere sosyal refah ihtiyaçlarına destek ve diğer sosyal refah yardımlarına (Finlandiya), fiziksel ve zihinsel sağlık ve duruma, işlenilen ya da işlendiği iddia edilen suçlara, işlenilen ya da işlendiği iddia edilen suçlar için yürütülen kovuşturmalara, bu kovuşturulmaların sonlandırılmasına ve bu kovuşturmalar sonucunda bir mahkeme tarafından verilen mahkumiyetlere (İngiltere) ilişkin veriler de veri koruma kanunlarında hassas veri olarak kabul edilmiştir.

³¹ Cemil Kaya, “ Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: 69, Sayı: 1-2, 2011, ss.318-319

³² Ceren Yakışır, **Türk Ceza Kanunu’nda Kişisel Verilerin Basın Yayın Yoluyla Açıklanması Suçu**, On İki Levha Yayınları, İstanbul, 2019, s. 20.

Görüldüğü gibi AB ülkelerinin hassas veri türlerinde önemli farklılıklar bulunmaktadır³³.

Nitekim Fransa’da bir takım internet kullanıcılarının Google’da yapılan aramalarda hassas veri olarak nitelendirilebilecek sonuçlarının yer alması nedeniyle; Fransa Denetim Makamı (CNIL)’a başvuruları üzerine, kullanıcılara ait hassas veri niteliğindeki sonuçların Google’dan kaldırılmasına karar verilmiş; karara Google tarafından riayet edilmemesi üzerine konu Fransız Danıştayı’na taşınmıştır. Fransız Danıştayı tarafından Avrupa Birliği Adalet Divanı’na başvurulması üzerine Divan, 24 Eylül 2019 tarihinde hassas verilerin hangi durumlarda işlenebileceğini ortaya koyan emsal niteliğinde bir karar yayınlamıştır. C-136/7 sayılı bu kararda; “ *...Sonuç olarak; arama motoru yöneticisi hassas verilerin yayımlandığı internet sitelerine ulaşan bağlantıların kaldırılması yönünde bir başvuru aldığı anda, söz konusu olaya özgü tüm faktörleri değerlendirerek ve bahse konu müdahalenin ciddiyetini; veri sahibinin Temel Haklar Şartı’nın 7. ve 8. maddesine dayanan mahremiyet ve kişisel verilerin korunması temel haklarını, 95/46/EC Sayılı Direktif’in 8/4. maddesinde veya 2016/679 Sayılı Yönetmelik’in 9/2-g maddesinde anılan önemli kamu yararını da dikkate alarak incelemelidir. Bu hükümlerde belirtilen şartlara uygun olarak bir aramanın ardından görüntülenen sonuçlar listesine bu bağlantıların dahil edilip edilmediği; veri sahibinin adı temelinde bu tür bir arama ile o web bağlantısına erişmekle potansiyel olarak ilgilenen internet kullanıcılarının Temel Haklar Şartı’nın 11. maddesi ile güvence altına alınan haber alma özgürlüğünün korunması için kesinlikle şart olması gerekmektedir.*” demek suretiyle belediye yönetimlerine aday olan siyasi kimlik sahibi ilgili hakkında hassas verilerin incelenmesiyle ilgili çok yönlü bir inceleme yapmıştır³⁴.

B. Kişisel Verinin İşlenişine İlişkin Kavramlar

Kişisel veriye ilişkin kavramların incelenmesinin ardından kişisel verinin işleniş sürecinde karşımıza çıkabilecek başka kavramlar da mevcuttur. Kişisel veriler hukukunun doğumu, verilerin hukuka aykırı işlenmesi halinde “veri sorumlusu” ve

³³ Hassas veri türleri ve işlenme halleri hakkında detaylar için Kaya, s.319 vd.

³⁴Avrupa Birliği Adalet Divanı 24.09.2019 tarihli, C-136/7 sayılı kararı için: <http://curia.europa.eu/juris/document/document.jsf?docid=218106&doclang=EN> (14.01.2021)

“veri işleyen” in bundan doğan sorumluluğu esasına dayanmaktadır. “Veri sorumlusu” ve “veri işleyen” kavramı kişisel verilerin korunması hukukunun merkezini oluşturmaktadır³⁵. Bu kavramlar ile birlikte Avrupa Birliği Hukuku açısından önem arz eden diğer kavramları incelemek yerinde olacaktır.

1. Veri İşleme Faaliyeti

GDPR’nin 4. maddesinin Tanımlar başlığı altında 2. fıkrada değinilmiş olan veri işleme faaliyeti; “*otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisi*” olarak tanımlanmıştır. Bu tanımlamaya ek olarak; kişinin kendisine özel tuttuğu kayıtlarsa kişisel verilerin işlenmesi olarak nitelendirilemeyeceğini vurgulamak gerekmektedir. Örneğin, kişinin telefonuna iletişim kurma amaçlı kaydettiği telefon numaraları gibi kişisel amaçlı tutulan kayıtlar bu kapsamda değerlendirilemeyecektir.

GDPR’de yapılan tanımdan yola çıkılarak veri işlemenin herhangi bir yöntemle gerçekleştirilebileceğini söylemek de mümkündür. Günümüz teknolojisinde veri işleme konusunda bilgisayar sistemleri çok yoğun olarak kullanılsa da Avrupa Birliği’nde yalnızca bilgisayar ortamında otomatik işlenenler değil, tüm yöntemlerle işlenen veriler koruma altındadır. Örneğin; bir hastanın muayene olduğuna dair poliklinik defterine imza atması da kişisel veri işleme faaliyeti olarak kabul edilmektedir ve kişisel verilerin işlenmesi korumasından yararlanmaktadır.

2. Veri Sorumlusu

GDPR’nin 4/7. maddesinde “kontrolör” olarak yer alan veri sorumlusu; “*yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ*” olarak tanımlanmıştır. Maddenin devamında; “*söz konusu*

³⁵ Develioğlu, s.41.

işleme amaçları ve yöntemlerinin Birlik ya da üye devlet hukukuna göre belirlenmesi durumunda, kontrolör veya kontrolörün belirlenmesine özgü kriterler Birlik ya da üye devlet hukukuna göre belirlenebilir” demek suretiyle verilerin işlenmesinin yöntemlerinin ulusal kanunlar veya Avrupa Birliği düzenlemeleri ile gösterilmesinin mümkün olduğunu ortaya koymuştur.

Kişisel verilerin korunmasında veri sorumlusu asli bir öneme sahip olmakla birlikte, GDPR ile bu kavram yeni bir anlam kazanmıştır. Şöyle ki kişisel verilerin korunmasında önceleri olay bazında bir yaklaşım izlenirken, GDPR ile birlikte artık bütüncül bir yaklaşım benimsenmiştir. Veri sorumlusunun somut olayda gerçekleştirdiği veri işleme faaliyeti için yasal dayanak sunması artık yetmemekte, aksine veri sorumlusu veri işleme faaliyetinin hukuka uygunluğu için gerekli teknik ve idari tedbirleri almalıdır. Bu nedenle artık veri sorumlusunun rolü, yalnızca bir verinin işlenme süreciyle sınırlı kalmayıp bu sürecin tamamında hukuka uygunluğu sağlamak olarak genişlemiştir. Bu bağlamda veri sorumlusu, kişisel verilerin korunmasına yönelik gereksinimleri yerine getirecek şekilde organize olmalıdır. Yani artık sadece somut olaydan olaya veri işleme faaliyetinin meşruiyetiyle sınırlı bir durum söz konusu olmamakla birlikte sürekli bir yaklaşım ortaya konmaktadır. Bu nedenle GDPR, somut olay denetimi yerine hesap verilebilirlik ilkesini esas almakta, veri sorumlularına bu doğrultuda bir organizasyon sorumluluğu yüklemektedir³⁶.

95/46/EC sayılı AB Veri Koruma Direktifi’nin yürürlükte olduğu dönemlerde Almanya, Hollanda, İsveç, Lüksemburg ve Fransa gibi üye devletler veri sorumlusunun yükümlülüklerini tüzel kişi için gerektiği şekilde yerine getirebilmesini sağlamak için “veri koruma görevlisi” istihdam etme zorunluluğunu getirmişlerdir. Almanya’da otomatik sistemler ile veri işleyen şirketlerde, kırk işçiden fazlasının istihdam edildiği hallerde, şirkete veri koruma görevlisi atanması zorunluluğu getirilmiştir. İsveç’te veri koruma görevlisi bulundurma mecburiyeti yönünde bir yasal düzenleme bulunmamasına rağmen “kişisel veri temsilcisi” terimi ile gönüllü bir istihdam uygulaması getirilmiştir. Hollanda’da ise yine veri koruma görevlisi çalıştırma zorunluluğu bulunmamaktadır. Ancak, İsveç örneğine benzer bir

³⁶ Çekin, s.49. Bu bağlamda veri sorumlusu veri işlemeye yönelik kararları alan taraf ve çoğu zaman veri sahibinin kişisel verilerini teslim ettiği taraf olarak değerlendirilmektedir. Yüksel Tolun ve İslam Safa Kaya, **Uygulayıcılar İçin Türkiye’de ve Avrupa’da Kişisel Verilerin İşlenmesi KVKK-GDPR Karşılaştırması**, Adalet Yayınevi, Ankara, 2020, s.57.

şekilde; gönüllü olarak istihdam edilebilmesinin yanı sıra, veri koruma görevlisinin veri sorumlusundan emir ve talimat alması gerektiği belirtilmiştir³⁷. GDPR’de veri sorumlusu ve veri işleyenlerin, veri koruma görevlisi ataması gereken durumlar hüküm altına alınmıştır. Buna göre; özel nitelikli kişisel verilerin işlenmesinin çoğunlukta olduğu yerlerde ve asıl işin bireylerin düzenli ve geniş kapsamlı olarak izlenmesinden oluşan yerlerdeki veri sorumluları ve veri işleyenler bakımından veri koruma görevlisi atanması bir zorunluluk olarak yer almaktadır.

3. Veri İşleyen

GDPR’nin 4/8. maddesinde “işleyici” kavramıyla yer alan veri işleyen; “*veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ*” olarak tanımlanmıştır. Veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişidir. Veri sorumlusu, veri işleyenin faaliyetlerini kanuna uygun olarak yürütmesini sağlayacak önlemleri almak zorundadır³⁸.

Veri işleyene emanet edilen faaliyetler özel veya oldukça genel ve kapsamlı olabilir. Bununla birlikte veri işleyenler başkaları için veri işleyebilecekleri gibi, kendi amaçları için gerçekleştirdikleri işleme ile ilgili veri sorumlusu konumunda olacaklardır. Örneğin; veri işleyen yanında çalışan personelin satışlarının ve hesaplarının idaresinde bu durum söz konusu olacaktır. Yani bir veri işleyen, kendi çalışanlarına karşı veri sorumlusu konumunda olabilecektir. Veri işleyenlerin belirli başlı bazı veri işleme görevlerini başka alt işleyicilere devretmek istemesi de mümkündür. Bu durum, veri işleyen ve veri sorumlusu arasında uygun ve bağlayıcı bir sözleşmenin yapılması halinde yasal olarak mümkündür. Ancak bu durumda GDPR, alt işleyicinin veri koruma yükümlülüklerini yerine getirmediği noktada; asıl veri işleyenin veri sorumlusuna karşı tamamen sorumlu olarak kalmasını şart koşmaktadır³⁹.

³⁷ Aşıkoğlu (Büyük Veri), s.69.

³⁸ Aysun, s.54.

³⁹ Avrupa Birliği Temel Haklar Ajansı, **Handbook on European Data Protection Law**, Avrupa Birliği Temel Haklar Ajansı Yayınları, Luxemburg, 2018, s. 107-108.

Veri işleyenin, veri sorumlusu tarafından görevlendirilen ayrı bir kişi olabileceği gibi, herhangi bir gerçek veya tüzel kişinin farklı veri işleme faaliyetleri esnasında veri işleyen ve veri sorumlusu sıfatlarına aynı anda haiz olması da mümkündür. GDPR kapsamında, veri işleyenin kamu tüzel kişisi ya da özel hukuk kişisi olması arasında bir fark da ortaya konmamıştır. Bu bağlamda, veri işleyen bir kamu kurumu olabileceği gibi verileri tutan bir bulut bilişim firması da olabilir. Örneğin, idarenin bir bulut bilişim hizmeti sağlayıcısıyla topladığı kişisel verilerin saklanması için anlaşması durumunda, kendisi veri toplamayan, bir tek idareden gelen buyruklar doğrultusunda kişisel verileri işleyen bulut bilişim hizmeti sağlayıcısı, veri işleyen sıfatını taşıyacaktır⁴⁰.

4. Alıcı ve Üçüncü Kişi

GDPR'nin 4/9. maddesinde alıcı; *“üçüncü bir kişi olsun veya olmasın, kişisel verilerin açıklandığı bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ”* olarak tanımlanmıştır. 4/10. maddede ise üçüncü kişi; *“veri sahibi, kontrolör, işleyici ve kontrolör ya da işleyicinin doğrudan yetkisi altında, kişisel verileri işleme yetkisi bulunan kişiler haricindeki bir gerçek veya tüzel kişi, kamu kurumu, kuruluşu veya organ”* olarak tanımlanmıştır. Bu şekilde ikili bir tanımlama farkı oluşturulmasının nedeni kişisel verilerin üçüncü kişilere aktarılmasıyla ilgilidir. Yani; veri sorumlusundan ayrı bir kişi olan üçüncü kişilere kişisel verilerin aktarılması hususunda daima ortaya ayrı bir dayanak koyulması gerekmekte iken; alıcıya yapılan veri aktarımında böyle bir zorunluluk yoktur⁴¹. Örneğin; veri sorumlusunun, alıcı konumunda olan şirketin çalışanlarına veya farklı bölümlerine kişisel verileri iletirken bunun için veri sahibinden tekrar izin almasına veya bir hukuki nedene dayanmasına gerek yoktur⁴².

⁴⁰ Cemal Başar, **Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması**, On İki Levha Yayınları, İstanbul, 2020, s.40.

⁴¹ Avrupa Birliği Temel Haklar Ajansı, s. 54.

⁴² Develioğlu, s. 44.

C. Kişisel Verilerin Korunmasına Hakim Olan Temel İlkeler

Kişisel verilerin korunması hukukunu düzenleyen bazı temel ilkeler mevcuttur. Bu ilkelerin mevcut halinin kaynağı GDPR olmakla birlikte; önceki düzenlemelerde de değinilmiş, GDPR ile geliştirilerek yeknesaklaştırılmıştır. GDPR'nin uygulanacağı durumlarda, diğer hukuka uygunluk halleri mevcut olsa bile; gözetilmesi gereken bazı temel ilkeler vardır. Başka bir deyişle, kişisel verilerin işlenmesi, veri sahibinin rızasının varlığı halinde olduğu gibi; kanuna uygun olsa bile, belirli ilkelere uyulmadan işlenmesi halinde, yine hukuka aykırı bir işleme gündeme gelecektir⁴³. Bunlar GDPR'de sayıldığı haliyle; “hukuka uygunluk, adalet ve şeffaflık”, “amaç ile sınırlılık”, “en az seviyede bilgi”, “doğruluk”, “sınırlı süre ile saklama”, “bütünlük ve gizlilik”, “hesap verilebilirlik” ilkeleridir.

1. Hukuka Uygunluk, Adalet ve Şeffaflık

GDPR'nin 5/1-a maddesinde; “*Kişisel veriler; veri sahibi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenir.*” denilmek suretiyle kişisel verilerin işlenmesinin ilk kuralı ortaya konmuştur. Bu ilke ile kişisel veriler işlenirken hukuka uygun hareket etme, adil ve şeffaf davranma gerekliliği hüküm altına alınmıştır. Hukuka uygunluk, adalet ve şeffaflık her ne kadar farklı ilkeler gibi ifade edilmiş olsa da aslında birbiriyle sıkı ilişki içindedir. Dürüstlük ve şeffaflığa uygunluk, hukuka uygunluğun gereğidir. Zira hukuka uygunluğun veya şeffaflığın olmadığı noktada, dürüstlüğün de olması söz konusu değildir. Maddede bahsedilen hukuka uygunluktan anlaşılması gereken; yalnızca kişisel verilerin korunması hukukuna veya GDPR'ye uygunluk değil, genel hukuk bağlamında geçerli olan evrensel hukuk mevzuatına uygun hareket etmektir. Bu haliyle de hukuka uygunluk ilkesi diğer tüm ilkelerin temelidir ve diğer tüm ilkeleri de kapsamaktadır. Hukuka uygun işlemenin bir koşulu da kişisel verilerin korunmasının temel ilkelerine uygunluktur. Bu bağlamda bakıldığında diğer tüm ilkelerin bu ilke ile doğrudan ilişkili olduğunu

⁴³ Develioğlu, s.44.

söylemek mümkün hale gelmektedir. Nitekim hukuk kurallarının amacı ilkelerin nasıl uygulanacağını belirlemek ve ilkeleri somutlaştırmaktır⁴⁴.

Veri işleyenin amacını kesin, net ve açık bir şekilde ortaya koyması şeffaflık ilkesinin bir gereğidir. Bu sayede ilgili verisinin ne amaçla, kim tarafından, ne kadar süre ile hangi bağlamlarda işleneceğini bilerek bunun güveni içerisinde hareket eder. Bu husus da hukuki güvenlik ve temel insan haklarının önemli bir boyutudur⁴⁵. Zira bir kişi; hakkındaki bilgilerin kim tarafından, ne denli elde edildiğini ve işlendiğini bilmezse kendini güvende hissedemez ve kendisi olmanın gereklerini yerine getiremez. Böyle bir güvensizlik de demokratik bir hukuk devleti olmanın gereklerine ters düşecektir. Bu durum da veri işleyene, veri sahibine karşı bir aydınlatma yükümlülüğü yüklemektedir.

Veri sorumluları, veri sahibinin rızasına dayanarak veri işleme faaliyeti gerçekleştirdikleri noktada veri sahibinin talepleri doğrultusunda hareket etmeyi ilke edinmelidir. Tüm bu açıklamalar doğrultusunda adil olma ilkesinin, şeffaflığın da ötesinde kişisel verilerin etiğe uygun bir şekilde işlenmesi ile ilgili olduğunu söylemek mümkündür⁴⁶.

2. Amaç İle Sınırlılık

GDPR'nin 5/1-b maddesinde yer alan bu ilkedен; “ *Kişisel veriler; belirtilen, açık ve meşru amaçlara yönelik olarak toplanır ve bu amaçlara uygun olmayan bir şekilde işlenmez; kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla işleme faaliyeti, 89(1) maddesi uyarınca, baştaki amaçlara aykırı şekilde değerlendirilmez.*” ifadesiyle bahsedilmiştir. Maddede atıf yapılan 89(1) maddesi ise; kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ile istatistiki araştırma amaçlarını düzenlemektedir. Bu amaçla hareket edilmesi halinde de veri sahibinin hakları GDPR tarafından güvence altına alınmıştır. Yani; kamu yararı, bilimsel ve tarihi araştırma ve istatistiki

⁴⁴ Yörük, s.53.

⁴⁵ Kılınç, 1159.

⁴⁶ Dülger, (GDPR Bağlamında Kişisel Veriler), s.99. Şeffaflık ilkesi, işleme faaliyetinden önce veri sahibinin bilgilendirilmesini içermesinin yanı sıra işleme devam ettiği müddetçe talebi halinde, veri sahibinin bilgilendirilmesini ve veri sahibine verilerine erişme imkanı sağlanmasını amaçlar. Avrupa Birliği Temel Haklar Ajansı, s. 120.

faaliyetler söz konusu olduğunda dahi, kişisel veriler toplandığı amaca aykırı olarak işlenemeyecektir.

Örneğin, banka tarafından sunulan hizmetlerin kullanılmasında güvenlik amacıyla işletilecek sistemlerde müşterilerin parmak izine ihtiyaç duyulması söz konusu olabilir. Bu verinin işlenmesinin rızaya tabi olduğu açıktır ve banka tarafından ancak gerekli olan durumlarda alınmalı ve kullanılmalıdır. Ancak bu verinin kullanımına ihtiyaç duyulmuyorsa ve ileride gerekli olacağı düşüncesiyle saklanıyorsa bu veri işleme faaliyeti hukuka aykırıdır⁴⁷.

Görüldüğü üzere bu düzenleme sayesinde hangi neden ile elde edilmiş olursa olsun kişisel veriler elde edildikleri amaç dahil tüm işleme nedenlerine karşı korunmuştur. İşlemenin verinin toplandığı amaç için olması gerektiğini vurgulayan GDPR, yine bu toplama amacının meşru olması gerektiğini vurgulayarak ilk ilke olan “hukuka uygunluk” a verilen önemi bir kez daha ortaya koymuştur.

Veri sorumlusunun işleme faaliyetinin ilkelere uygunluğa riayet edip etmediğini iki aşamada test etmesi mümkündür. Buna göre ilk etapta işleme için amacın tespitinin yapılması gerekir. Yani veri sorumlusu önce varmak istediği hedefi tespit etmeli, sonrasında bu hedefe giderken amacını gerçekleştirmeye yetecek kadar veriyi işlemelidir. İkinci olarak amaç tespitinin ardından gereklilik tespiti gündeme gelmektedir. Veri işleme faaliyetinin bütünüyle ele alınıp işlemenin gerekliliği tespit edilmelidir. Bu tespitler sonucunda veri sorumlusu amacı için gerekli olan verileri işleyip amacına uygun olmayan verilerden uzak durmalıdır⁴⁸.

Ancak günümüz gelişmeleri dikkate alındığında bu ilkenin ne kadar isabetli olduğu konusu ise tartışmalıdır. Bir yanda; kural olarak kişisel verilerin işlenmesinin yasak olduğu, ancak kanunlarla belirlenen belirli hallerde işlemenin mümkün olabileceği, en az seviyede veri toplama ve belirli hallerde işlemeyi hüküm altına alan kanuni düzenlemeler, öte yanda da büyük verilerin işlenmesi ile beslenen toplum düzeni ve yaygınlaşmış uygulamalar mevcuttur. Özellikle de verinin toplanması esnasında her türlü amacın önceden öngörülebilmesinin imkansız

⁴⁷ Göknıl Özcan, **Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması**, On İki Levha Yayınları, İstanbul, 2020, s.90.

⁴⁸ Habip Bozkurt, **Kişisel Verilerin İşlenmesinin Hukuki Boyutu**, (Yayımlanmamış Yüksek Lisans Tezi), Kadir Has Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul, 2019, s.93.

olmasıyla birlikte her türlü işlemeye yönelik genel rıza beyanlarının da açık rıza kuralına uygun olacağını söylemek mümkün değildir⁴⁹.

3. En Az Seviyede Bilgi

GDPR'nin 5/1-c maddesinde; “ *Kişisel veriler, işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlıdır.* ” demek suretiyle kişisel verilerin işlenirken yeterli ve en az seviyede tutulması gerektiğinin altı çizilmiştir. Bu ilke doğrultusunda kişisel veriler; açık ve net bir şekilde belirlenen amaçlarla bağlantılı, bu amaçların çizdiği sınırlar dâhilinde ve ölçülülük genel kuralı çerçevesinde toplanabilir ya da işlenebilir. Örneğin sadece belli bir okuldan mezun olan kişileri bir araya getirmeyi amaçlayan bir mezunlar derneğinin; kişinin etnik kökenini, cinsel eğilimlerini, mensup olduğu siyasî, görüşlerini işlemesi durumunda amaçla bağlılık ve en az seviyede bilgi ilkesi ihlal edilmiş olacaktır⁵⁰. Amaç ile sınırlılık ilkesi ile de yakından ilgili olan bu ilke, kişisel verilerin yalnızca hizmet edeceği amaca yetecek kadar işlenmesi gerektiğini ortaya koymaktadır.

Teknolojinin gelişmesi, kişisel verilerin daha az uğraşı ile daha kolay toplanmasına katkı sağlamıştır. Bu kolaylığın kötüye kullanılmasının önüne geçmek amacıyla hüküm altına alınan en az seviyede bilgi ilkesi, teknolojik araçlarla işlenebilecek en az miktarda kişisel verinin toplanmasını gerektirmektedir. Veri minimizasyonu olarak da ifade edilen bu ilke gereği veri sorumlusu, veri işlemenin zorunlu olup olmadığını tespit etmelidir. İşlemeye tabi olan veri, işlenmeden de veri sorumlusu amacını gerçekleştirebilecekse, veriyi işlemeye dikkat etmelidir. Ancak, veri işlemeden amacın gerçekleşmesi mümkün değilse; bu durumda en az seviyede bilgi olmasına dikkat edilmelidir. Bu anlamıyla veri minimizasyonu, kişisel veriler işlenirken yeterli ve en az miktarda sınırlı olmak olarak tanımlanabilir⁵¹. Bu durum

⁴⁹ Çekin, s.11. Kişisel veriler, asıl toplanma amacı haricinde bir amaç için işlenecekse, toplandığı amaçla bağlı olan hukuka uygunluk nedenine dayanması da mümkün değildir. Örneğin verilerin toplandığı sırada veri işleme amacına yönelik olarak veri sahibinin rızası alındıysa, asıl amacın dayandığı hukuka uygunluk nedeni rızadır. Ancak rıza olmasına rağmen veri işleme sırasında ortaya çıkan yeni amaç bu rızaya dayalı olarak meşru hale gelmez. Veri sahibinden yeni amaca yönelik olarak yeniden rıza almak gerekir. Tolun vd., s.82.

⁵⁰ Oğuz, s. 24.

⁵¹ Oğulcan Özkan, **Kişisel Verilerin Korunması**, Yetkin Yayınları, Ankara, 2020, s.110.

“veri ekonomisi” olarak da adlandırılır⁵². Veri ekonomisinin sağlanması için, veri sorumluları kişisel verileri işlerken mümkün olan en az veriyi kullanmalı, aşırıktan kaçınmalıdır.

4. Doğruluk

GDPR’nin 5/1-d maddesinde; “ *Kişisel veriler, doğrudur ve gereken şekilde, güncel tutulur; işlendikleri amaçlar göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin silinmesi veya düzeltilmesinin sağlanmasıyla ilgili makul tüm adımlar atılmalıdır.*” demek suretiyle doğruluk ilkesi tanımlanmıştır. Bu ilkeye göre kişisel verileri, doğru ve gerektiğinde güncel olmalıdır. Kişisel verilerin doğru tutulması aslında veri sahibinin çıkarlarını korumaya yöneliktir. Zira doğru tutulmayan kişisel veriler; veri sahibinin temel hak ve özgürlüklerine, ekonomik çıkarlarına ve manevi bütünlüğüne zarar verir⁵³.

Kişisel verilerin yanlışlığına ilişkin durumların ortaya çıkması halinde ise GDPR’nin 16. maddesi ile veri sahiplerinin kendileri ile ilgili doğru olmayan verilerin düzeltilmesini talep hakkı hüküm altına alınmıştır.

Veri sorumlusunun işlediği verilerin doğruluğu ve güncelliği ile ilgili yürüteceği çalışmalar olayın özelliklerine göre değerlendirilecektir. Güncel olmayan veri yeni hali araştırılarak güncellenebileceği gibi, verinin yanlış olması halinde silinmesi gerekir. Bu durumda verinin işleme faaliyetinin başında doğruluğunu kontrol etmek ile işlemek için saklanan verilerin doğruluğunu koruduğunun kontrolü yönünde yapılacak çalışma farklı olacaktır. Zira doğruluk, veri işleme sürecinin her aşamasında korunması ve uyulması gereken bir ilkedir. Bu noktada, verinin doğruluğunun ve güncelliğinin korunabilmesi adına, veri sahibinin işlenen verisine her zaman ulaşmasının önemi ortaya çıkmaktadır.

5. Sınırlı Süre İle Saklama

GDPR’nin 5/1-e maddesinde; “ *Kişisel veriler, veri sahiplerinin yalnızca kişisel verilerin işleme amaçlarının gerektirdiği sürece teşhis edilmesini sağlayan*

⁵² Küzeci, s.208.

⁵³ Develioğlu s.48.

bir şekilde tutulur; 89(1) maddesi uyarınca yalnızca kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla ya da istatistiki amaçlarla işlendikleri sürece ve veri sahibinin hakları ve özgürlüklerinin güvence altına alınmasına için bu Tüzük uyarınca gereken uygun teknik ve düzenlemeye ilişkin tedbirlerin uygulanmasına tabi olarak, kişisel veriler daha uzun süreler boyunca saklanabilir.” denilerek sınırlı süre ile saklama ilkesi tanımlanmıştır.

Bu ilke, veri minimizasyonu ilkesinin zamansal bir görünüm biçimidir. Bu ilkenin ayrıca düzenlenmesi, kanun koyucunun bu ilkeye özel bir önem verdiğini göstermektedir. Kişisel verilerin işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi, işleme amacının gerçekleşmiş olmasından kaynaklanabileceği gibi, verinin işleme amacı ile ilgisini kaybetmesinden ya da amacın ortadan kalkmasından da kaynaklanabilir⁵⁴.

Bu ilkeye göre kişisel veriler, verileri işlenen kişinin kimliğini belirleyecek şekilde, işleme amacı için gerekli olan süre boyunca tutulmalıdır. Bu hususta Avrupa Birliği’ne üye ülkelerin de tarihi incelemeler, istatistikî veya bilimsel çalışmalar amaçlarıyla olması gerekenden daha uzun süre kişisel verileri saklaması gerekiyorsa; saklamanın kötüye kullanılmaması için uygun güvenceleri sağlamalıdır⁵⁵.

Fransa Denetim Makamı CNIL, verilerin sınırlı süreyle saklanması hususunda verdiği kararda; bir gayrimenkul şirketi olan SERGIC’e genel veri koruma kurallarına uymadığı ve kişisel verilerin saklama süresini işleme amacına göre belirlemediği gerekçesiyle 400.000 Avro cezai yaptırım uygulamıştır. CNIL bu kararında; verinin saklanma amacına ulaşıldığında ve başka hiçbir yasal amaç verinin saklanmasına devam edilmesini haklı göstermediği takdirde verilerin silinmesi gerektiğini vurgulamıştır⁵⁶.

6. Bütünlük ve Gizlilik

GDPR’nin 5/1-f maddesinde; *“yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı koruma da dahil olmak üzere teknik veya düzenlemeye ilişkin uygun tedbirlerin kullanılması suretiyle kişisel verilerin güvenliğini sağlayan bir şekilde işlenir.”* demek suretiyle bütünlük ve gizlilik ilkesi

⁵⁴ P. Schantz, Beck'scher Online-Kommentar Datenschutzrecht. Heinrich Amadeus Wolff ve Stefan Brink (ed.). München, 2019, 5. paragraftan aktaran Nafîye Yücedağ, “Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler”, **Kişisel Verileri Koruma Dergisi**, Cilt:1, Sayı:1, s.60.

⁵⁵ Uygun, ss.55-56.

⁵⁶ <https://www.cnil.fr/en/node/114081> (23.01.2021)

tanımlanmıştır. Bütünlük ve gizlilik olarak belirtilen bu ilkede; bütünlük kavramını yetkisiz kişilerce işlemeye karşı koruma, gizlilik kavramını ise; verinin yetkisiz kişilerce açığa çıkarılmasına karşı koruma olarak yorumlamak mümkündür. GDPR'nin, özellikle veri sorumlusu ve veri işleyenlere ilişkin düzenlemelerin yer aldığı 4. Bölümü'nde; veri sorumluları ve veri işleyenlerin yükümlülükleri, almaları gereken tedbirler detaylı olarak düzenlenmiştir. Bu düzenlemelere göre; veri sorumlularının ve veri işleyenlerin kişisel verilerin korunmasına yönelik kurumsal politikalar geliştirmesi, bu kapsamda teknik tedbirler alması gerekmektedir⁵⁷. Bu ilke kapsamında yapılması gerekenlere örnek olarak; kişisel verilerin psödemize edilmesi, şifrelenmesi ve mevcut önlemlerin yeterli olup olmadığının düzenli olarak kontrol edilmesi verilebilir⁵⁸.

Veri işleminde yaşanan bir ihlal, başlı başına bu ilkenin de ihlal edildiğini gösterir. Bu bağlamda ihlallerin önüne geçmek için alınması gerek teknik önlemlere ek olarak, veri ile ilgili işi olmayan ve erişmesi zorunlu olmayan personelin veri erişimine kısıtlama konması gibi idari tedbirler de alınması gerekmektedir⁵⁹.

7. Hesap Verebilirlik

GDPR'nin 5/2. maddesinde; *“Kontrolör 1. paragrafta uygun davranmaktan sorumludur ve buna uygun davrandığını gösterebilmelidir.”* demek suretiyle hesap verebilirlik ilkesini tanımlamıştır. Bu amacı gerçekleştirmek için veri sorumlusu gereken tedbirleri almalıdır. Bu kapsamda izlenecek yol, verinin niteliğine bağlı olarak değişiklik gösterecektir. Bu ilkeye uygun hareket ettiğini göstermek adına veri sorumluları ve veri işleyenler, işleme faaliyetlerini kayıt altına alabilir ve kendilerinden talep edildiğinde tuttuğu kayıtları denetim makamına sunabilir. Özellikle durumlar için kişisel verilerin korunmasıyla ilgili görev yapacak bir veri koruma görevlisi atanabilir. Veri işlemeye ilişkin herhangi bir faaliyetin veri sahibinin hakları yönünden yüksek risk içermesinin söz konusu olduğu durumlarda, işleme faaliyetinden önce veri koruma etki değerlendirmesi yapılabilir⁶⁰.

⁵⁷ Develioğlu, s.50.

⁵⁸ Yörük, s.60.

⁵⁹ Tolun vd., s.84.

⁶⁰ Dülger (GDPR Bağlamında Kişisel Veriler), s.107.

GDPR, kontrolör demek suretiyle hesap verme açısından veri sorumlusunu sorumlu kılmışsa da belirli yükümlülöklere uymak zorunda olan veri işleyenin de, veri işlerken yukarıda sayılan ilkelere uygun davrandığı hususunda hesap verebilir olması gerekir⁶¹.

III. KİŞİSEL VERİLERİN HUKUKİ NİTELİĞİ

Kişisel verilerin hukuki niteliğinin ne olduğu konusunda doktrinde birlik olmamakla birlikte mülkiyet hakkı, fikri hak ve kişilik hakkı olduğu yönünde üç farklı görüş savunulmaktadır. Bu görüşlerin incelenmesi ve değerlendirilmesi, kişisel verinin yararlanacağı korumayı belirlemek açısından önem arz etmektedir. Kişisel verilerin korunmasına Avrupa yaklaşımı “sosyal değer” merkezli olup “bilgi toplumu” ndan söz edilir. Kişisel verilerin niteliğine ilişkin üç farklı görüşün olduğu bir ayırım yapılmakta ise de dünya çapında hakim olan temel yaklaşımlara göre bu üç görüşün de iki ana grupta toplanması mümkündür. Kişisel verileri sahibinden soyutlayıp bağımsız bir ürün olarak ortaya koyan yaklaşım olan “ekonomik hak” görüşü ve kişi ile veriyi bir bütün olarak ele alan “insan hakkı” görüşü olarak ikili bir ayırım da mümkündür⁶². Anglo-Amerikan hukuk sisteminde kişisel verilerin korunması ekonomik hak olarak değerlendirilirken, Avrupa hukuk sisteminde ise kişi hakkı olarak görülür. Kişisel verinin hukukî niteliğine ilişkin yapılan bu ayırım, bir diğer yönüyle Anglo-Amerikan hukuk sistemiyle Avrupa hukuk sistemi arasındaki farkı da yansıtmaktadır⁶³. Bu kapsamda; çalışmamızın konusu itibariyle biz de Avrupa’da da işlenen görüşler olarak sırasıyla; kişilik hakkı, fikri hak ve mülkiyet hakkına ilişkin yaklaşımları inceleyeceğiz.

A. Kişilik Hakkı Görüşü

Kişilik hakkı görüşünde kişisel verilerin korunması, münferit kişilik haklarından kişinin özel ve gizli hayat alanı kapsamında düşünülmektedir. Bu nedenle kişilik hakkı yaklaşımı itibariyle, kişisel verilerinin işlenmesi hususundaki

⁶¹ Dölger (GDPR Bağlamında Kişisel Veriler), s.106.

⁶² Küzeci, s.60

⁶³ Taştan, s. 54.

yetkiler ve kişisel verilerinin korunması, kişinin özel ve gizli hayat alanı üzerindeki hak ve yetkiler ile kişinin özel ve mahrem alanına yapılan müdahalelerin korunması hükümleri çerçevesinde belirlenir⁶⁴.

Kişisel verilerin hukuki niteliği konusunda, özellikle Avrupa’da kişilik hakkı görüşü yaygın bir şekilde benimsenmektedir. Mahremiyetin bir çeşidi olan “bilgi mahremiyeti”; *bireylerin kişisel verilerinin toplanması, kullanılması ve açıklanması şartlarını denetim hakkı* şeklinde tanımlanmaktadır. Genel kişilik hakkı, bireyin kendisini dış dünyada ifade edebilme özgürlüğünü de içermektedir⁶⁵.

Kişinin sahip olduğu özel yaşam alanı kişisel veriler kapsamındadır ve bu da paylaşma konusunda kişinin kendi tercihinde kalan bir alandır. Özel yaşam alanını daha kolay incelemek açısından kişi yaşamını; “gizli hayat”, “özel hayat”, “kamusal hayat” olarak sınıflandırmak mümkündür. Bu sınıflandırmalara göre gizli hayat kişinin sadece kendi istediği kişilerle, istediği kadarını paylaştığı hayat alanıdır. Özel hayat; gizli alan kadar mahrem olmayıp kişinin yine kendi yakın çevresiyle paylaştığı alandır. Kamusal hayat ise; kişinin kendisi açıklasa da açıklamasa da herkes tarafından bilinen ve herkesin gözü önünde cereyan eden hayattır. Özel ve gizli hayata yapılan izinsiz müdahale kişilik hakkına ve buna bağlı kişisel verilere saldırı niteliği taşır. Kural olarak kişilik hakkına saldırıya karşı korumalar kişinin kamuya açık hayat alanını kapsamamaktadır. Bu korumalar özel ve gizli hayat alanına ilişkindir⁶⁶.

Kişisel verilerin kişilik hakkı olduğunu savunanlar; “kişisel verilerin korunması” ile “mahremiyetin ve özel hayatın korunmasını” eş gördükleri için, kişisel verilerin korunmasını salt özel hayatın korunmasına bağlamak yetersiz bir sonuca ulaşmaya yol açabileceğinden eleştiriye maruz kalmışlardır⁶⁷.

⁶⁴ Hamza Bayındır, **Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması**, On İki Levha Yayınları, İstanbul, 2020, s.27.

⁶⁵ Aydın Akgül, **Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi**, (Yayımlanmamış Doktora Tezi), Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli, 2013, (Kişisel Verilerin Korunması), s.59.

⁶⁶ Serap Helvacı, **Gerçek Kişiler**, 7. Baskı, Legal Yayıncılık, İstanbul, 2016, ss.121-125.

⁶⁷ Özkan, s.35.

B. Fikri Hak Görüşü

Kişisel verileri fikri hak olarak değerlendiren görüşe göre kişisel verilerin korunması hakkı ile fikri mülkiyet hakkının korunması amaç olarak birbirine benzemektedir. Örneğin, bir sinema eseri üreten kişinin söz eseri üzerindeki hakkı fikri mülkiyet hakkı kapsamında yer almaktadır. Bu bağlamda, kişisel verinin de bir gerçek kişi tarafından üretilmesi nedeniyle, kişisel veriler üzerindeki hakkın korunmasının da aynı esaslara göre belirlenmelidir.⁶⁸.

Fikri hak görüşü çoğunlukla Amerikalı hukukçular tarafından ileri sürülmüştür. Fikri hak görüşünde fikri mülkiyet hakkında da kişisel verilerin korunmasında da bireye ait ancak kişinin kontrolünü sağlamayı kaybedebileceği bir veri vardır. Fikri mülkiyette veri telif hakkı alınmış bir çalışmadan oluşurken, kişisel verilerin korunmasında, kişiye ait bir bilgiyi temsil etmektedir. Her iki durumda da özellikle internet ortamı, denetimin kaybında etkili olabilir. İnternet, fikri mülkiyet hakkı kapsamındaki ürün açısından tam ve bedava kopyalamaya yardımcı olurken kişisel verilerin korunması açısından, iş ve işlemlerimizin sürekli internet sunucularına iletimi ve buradan tüm dünyaya yayılması kontrolümüz dışında gerçekleşmektedir.⁶⁹.

Eser sahibinin manevi haklarından yola çıkılarak kişilerin verileri açısından da manevi hakların varlığının kabulü ile kişisel menfaatlerinin korunmasından bahsedilebilecektir⁷⁰. Tüm bu temellendirmelere rağmen, kişilik hakkı görüşünde olduğu gibi kişisel verilerin fikri hak olarak değerlendirilmesinde de eksik yönler bulunmaktadır. Şöyle ki kişisel veriler; banka bilgilerimiz, telefon numaramız, iş adresimiz gibi toplumdaki yaşayışımız neticesinde üretilen bilgiler olduğu gibi ad, soy ad, kimlik numarası, ırk, etnik köken gibi doğuştan ve kendiliğinden var olan özellikleri de kapsamaktadır. Ancak fikri mülkiyete konu olabilecek unsurlar ise bir çalışma ve düşünsel faaliyetler sonucu bir ürün ortaya koymak üzere oluşturulan eserlerdir. Yani fikri mülkiyette bir üretme amacı söz konusudur. Ancak kişisel verilerde her zaman böyle bir amaç söz konusu olmayabilir.

⁶⁸ Sinan Sami Akkurt, “Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış”, **Kişisel Verileri Koruma Dergisi**, Cilt:2, Sayı:1, 2020, s.24.

⁶⁹ Küzeci, s.71.

⁷⁰ Ann Bartow, “Our Data, Ourselves: Privacy, Propertization and Gender”, **University of San Francisco Law Review**, Cilt: 34, 2000, s. 685’ den aktaran Mendos Kuşkonmaz, s. 23.

C. Mülkiyet Hakkı Görüşü

Kişisel verileri mülkiyet hakkı olarak değerlendiren görüş, özellikle Amerikan Hukuk Sistemi'nde kabul edilmektedir. Bu görüşe göre herkes kendine ait kişisel verinin sahibidir ve kişisel bilgilerin yönetimi veri sahibine bağlıdır. Bilgi bir çeşit varlıktır ve bu varlığın idaresi kişiye aittir. Kişisel verilerin bir mülkiyet hak alanı içinde bulunduğu görüşüne sahip hukuki düzenlemelerin Avrupa'da da ele alındığını söylemek mümkündür⁷¹.

Mülkiyet hakkı görüşüne göre, verilerinin gizli kalmasına ve mahremiyetine özen gösteren veri özneleri olduğu gibi, verilerini paylaşmaktan memnun olan ve verilerini paylaşmak suretiyle çeşitli kampanyalardan ve fırsatlardan haberdar olmak isteyen veri öznelerinin olması da söz konusudur. Buna göre veri koruma sisteminde iki tür veri sahibi de dikkate alınarak bir yaklaşım geliştirilmelidir. Bu yaklaşım geliştirilirken tüm veri öznelerinin korunmasına önem verilmelidir. Mülkiyet hakkında esas olan, sahip olunan şey üzerinde her türlü tasarrufta bulunma yetkisi, kişisel verilerin mülkiyet hakkına tabi olduğu görüşünde veri sahiplerinin verilerini işleyicilere dilediği gibi açıklama ve satma yetkisine sahip olması ile karşımıza çıkarmaktadır. Bu görüşe göre veri özneleri, verilerini paylaşmak karşılığında veri işleyenlerden uygun bir bedel talep edebilir. Bu sayede bahsettiğimiz kişisel verilerini paylaşma isteği olan veri özneleri açısından da daha adaletli bir işleme sağlanması mümkün olacaktır. Bunun yanı sıra kişisel verileri satın alma karşılığında kurumlar üzerinde bir maliyet yükünün doğması söz konusu olacaktır. Bu da kişisel veri toplama ve kullanma konusunda kurumlar üzerinde bir farkındalık yaratıp veri işlemede tutumluluk yaratılmasını sağlayabilecektir⁷².

Diğer görüşlerde olduğu gibi mülkiyet hakkı görüşünün de eleştirildiği noktalar mevcuttur. Mülkiyet hakkı malike, sahip olunan şey üzerinde en geniş anlamda tasarruf yetkisi tanımaktadır. Malik, sahip olduğu malı devredebilir, değiştirebilir ve hatta yok edebilir. Ancak bu açılardan değerlendirildiğinde mülkiyet hakkı görüşü kişisel veriler ile bağdaşmamaktadır. Örneğin malikin malını sattığı durumlarda, satın alan kişi o malın yeni maliki olur ve mülkiyet hakkının sağladığı

⁷¹ Avcıoğlu, s.16.

⁷² Pamele Samuelson, "Privacy As Intellectual Property?", *Stanford Law Review*, Cilt:52, 2000, s.1130-1170.

tüm imkanlardan yeni malik faydalanabilir. Ancak kişisel verilerin temel prensibi açısından bu şekilde bir görüşün kabul edilmesi mümkün değildir. Zira bir kişinin kişisel verilerini satın alan kişinin veri sahibinin rızası aranmaksızın bu verileri üçüncü kişilere devretme hakkına sahip olabileceği düşüncesi kişisel verilerin korunmasına ilişkin düzenlemeler ile bağdaşmamaktadır. Ayrıca veri sahibinin kişisel verilerini satıp buna ilişkin tüm hakları bir başkasına devredebileceği görüşü insan onuru ve temel hakların korunmasından uzak bir yaklaşımdır⁷³.

IV. KİŞİSEL VERİLERİN İŞLENMESİNDE HUKUKA UYGUNLUK HALLERİ

Kişisel verilerin işlenmesine ilişkin hukuka uygunluk nedenleri GDPR'nin 6. maddesinde tek tek sayılmıştır. Maddeye göre işleme faaliyeti, ancak sayılan hususlardan en az birinin varlığı halinde hukuka uygun hale gelmektedir.

A. Genel Olarak

GDPR'de sayılan hukuka uygunluk sebeplerinden çıkarılması gereken husus ise; temelde uygunluk nedeni var olmadığı halde asıl olan kişisel verilerin işlenmesinin hukuka aykırı olmasıdır. Yani kişisel verileri işlemek için yasal bir neden olmadığı müddetçe işleme hukuka aykırıdır. Kişisel verilerin işlenmesini hukuka uygun hale getiren nedenler; veri sahibinin rızası, sözleşmenin gereğinin yerine getirilmesi, hukuki yükümlülüğün yerine getirilmesi, hayati menfaatlerin korunması, kamu görevinin yerine getirilmesi ve meşru çıkarların korunmasıdır.

1. Veri Sahibinin Rızası

Veri sahibinin rızasının olması şartına bağlanan hukuka uygunluk nedeninde rıza, özgür bir irade ile veri işleme faaliyetiyle ilgili yeterli bilgiye sahip olunarak yapılan her türlü irade açıklamasını kapsamaktadır. Bu beyanı ile veri sahibi,

⁷³ Hüseyin Can Aksoy, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Çakmak Yayınevi, Ankara, 2010., s. 65.

kendisiyle ilgili kişisel verilerin işlenmesine onay vermektedir⁷⁴. GDPR'nin 4/11 maddesinde rıza; *“veri sahibinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık gösterge”* olarak ifade edilmiştir. Literatürde “açık rıza” olarak da karşılık bulan bu hukuka uygunluk nedeni, GDPR de somut bir şekilde tanımlanarak karşılık bulmuştur. Yine bu düzenlemeye göre açık rıza yazılı, sözlü veya elektronik gibi tüm şekillerde verilebilir. Elektronik ortamda verilen rızalar için, uygulamada yaygın olarak kullanılan kutucuk işaretleme metodunun da yeterli olacağı ancak, kullanıcıya önceden işaretli bir kutucuğu sunarak kabul etmeme halinde kutucuktan işaretin silinmesi yönteminin ise kullanılamayacağı belirtilmiştir⁷⁵.

Veri öznelinin kişisel verileri üzerindeki tasarruf haklarının kaçınılmaz bir sonucu olarak, bu kişilerin kişisel verilerinin işlenmesine yönelik rızaları, işlemenin hukuka uygunluğunun bir gereğidir. GDPR’de yapılan tanımdan hareketle; rızanın temelini, veri öznesinin özgür iradesinin oluşturduğu söylenebilir. GDPR’de baskı altında kalmadan, hile veya aldatma yoluyla manipüle edilmeden verilen bir rıza aranmıştır. Kuşkusuz bu, ancak veri sahibi neye rıza verdiğini biliyorsa mümkündür, bu nedenle rızanın konusu ve sınırları belli olmalı, veri öznesi, veri sorumlusunca işlemenin amaçları ve yöntemlerine dair yeterince aydınlatılmış olmalıdır⁷⁶.

Veri sahibinden alınan rızanın özgür iradeyle dayanması ancak veri sahibine gerek bir seçim hakkının tanınması halinde mümkündür. Veri sahibi rıza göstermediği takdirde olumsuz sonuçlarla karşılaşacağı yönünde bir baskıya maruz kalıyorsa bu durumda özgür iradeyle verilen gerçek bir rızadan bahsetmek mümkün değildir. Bir zarar tehlikesi olmadan rıza vermeyi reddetmek ya da verilen bir rızayı geri almak mümkün değilse, bu durumda özgür bir iradede de bahsedilemez⁷⁷.

GDPR, rızanın açıkça alınıp alınmadığını göstermek açısından bir şekil şartı öngörmemiştir. Bu durumda devreye veri sorumlusunun yükümlülükleri girmektedir. Veri sorumlusunun ve ona bağlı veri işleyenlerin hesap verme yükümlülüğü

⁷⁴ Uygun, s.56.

⁷⁵ Açık rıza ve hukuki niteliğine ilişkin detaylı açıklama için bkz. Çekin, s. 73 vd.

⁷⁶ Yörük, s.61.

⁷⁷ Geçerli rıza açıklamasının detayları için bkz. Ozan Selek, “Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 21, Sayı:2, 2019, s.922 vd.

bulunmaktadır. Bu yükümlülüğün yerine getirilmesi açısından açık rızanın alınmasına ilişkin gerekli bilgilendirmelerin yerine getirildiğini gösteren bir form tutulması, açık rıza alınırken veri sahibinin herhangi bir zorlamaya tabi tutulmadan özgür iradesiyle rıza verdiğini içeren kayıtlar bulunması ve en önemlisi de açık rızanın yazılı olarak alınması yerinde olacaktır.

Veri sahibinin başta rıza vermemesi halinde, bir kısım dahi olsa işleme faaliyeti gerçekleştirildikten sonra onayının alınması başta gerçekleştirilen işleme faaliyeti hukuka uygun hale getirmeyecektir. Bununla birlikte veri sahibi, başlangıçta veri işlenmesi için verdiği rızasını dilediği zaman geri alabilir. Bu durumda rıza mevcutken gerçekleştirilen işleme faaliyeti hukuka aykırı hale gelmeyecektir ancak, rıza geri alındıktan sonra veri işleme faaliyetine devam edildiği takdirde hukuka aykırı işlemekten söz edilir. Her iki durumda da olduğu gibi rızanın açıklanması veya geri alınması, geriye yönelik etki doğurmamaktadır⁷⁸.

Veri sahibinin çocuk olması halinde rızasının ne şekilde alınacağı GDPR'nin 8.maddesinde düzenlenmiştir. Doğrudan bir çocuğa bilgi teknolojisi hizmetinin sunumunda, çocuğun en az 16 yaşında olması halinde kişisel verileri yasal olarak işlenebilir. Çocuğun 16 yaşından küçük olması halinde ise işleme, yalnızca çocuğun velisi tarafından rızanın verilmesi durumunda yasal olacaktır. Üye ülkelerin 13 yaşın altında olmamak kaydıyla, bu amaçlar için kanunla daha düşük bir yaş öngörebileceği de düzenlenmiştir.

2. Sözleşmenin Gereğinin Yerine Getirilmesi

GDPR'nin 6/1-b maddesinde; *“veri sahibinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için, işleme faaliyetinin gerekli olması”* halinde kişisel verilerin işlenmesinin hukuka uygun olacağı hüküm altına alınmıştır. Burada altı çizilmesi gereken husus sözleşmenin ifası ve kurulması madde kapsamında ayrı ayrı düzenlenmiştir. Buna göre mevcut bir sözleşmede veri sahibinin taraf olduğu durumlardaki işlemede hukuka uygunluk sebebi mevcuttur. Eğer henüz kurulmamış bir sözleşme söz konusu ise veri sahibinin bu sözleşmenin kurulması için işleme

⁷⁸ Başar, s.48.

faaliyetini talep etmesi gerekir. Örneğin bir tüketicinin kredi çekmek amacıyla bankaya başvuruda bulunması durumunda bankanın kredi talebini değerlendirmek için tüketicinin maaş bordrosunu talep etmesi sözleşme öncesi ve sözleşmenin kuruluma yönelik bir işleme olarak hukuka uygundur. Bir satış sözleşmesinde alıcı sıfatını taşıyan veri sahibinin aldığı ürünlerin teslim edilmesi için adresini paylaşması ise sözleşmenin ifası için gereken işleme faaliyeti olduğundan hukuka uygun olarak kabul edilir. Zira burada taraflar arasındaki sözleşmenin gereklerinin yerine getirilebilmesi için kişisel verilerin işlenmesi bir zorunluluktur⁷⁹.

Maddede belirtilen “işleme faaliyeti için gereklilik” kısmına dikkat etmek gerekir. Veri işlemenin hukuka uygunluğundan bahsedebilmek adına işlemenin sözleşme için gerekli olması gerekir. Örneğin internet sitesinden alışveriş yapılması durumunda kredi kartı bilgilerinin işlenmesi “işleme faaliyeti için gereklilik” kapsamında değerlendirilebilir. Ancak satın alınan mallara göre ilgili kişinin alışveriş tercihleri ve zevkleri hakkında bir profil çıkarılması hukuka uygun bir işleme olarak kabul edilemez⁸⁰.

3. Hukuki Yükümlülüğün Yerine Getirilmesi

GDPR’nin 6/1-c maddesinde; “*veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uygunluk sağlanması amacı ile işleme faaliyetinin gerekli olması*” ifadesiyle veri sorumlusunun tabi olduğu bir yasal yükümlülüğü yerine getirmek amacıyla yapılan işleme hukuka uygun kabul edileceği düzenlenmiştir. Veri sorumlusunun sözleşmeden doğan yükümlülüğünü yerine getirmesi için zorunlu olan haller bu hukuka uygunluk sebebi kapsamında dikkate alınmaz. Hukuki yükümlülüğün muhakkak bir kanuni düzenlemeden kaynaklanması şart değildir. İkincil düzenlemeler ile getirilen mevzuat da hukuki yükümlülük olarak kabul edilir. Ancak veri sorumlusunun hukuki olarak yükümlü olarak sayılması için hukuki düzenlemenin bağlayıcı olması ve veri sorumlusuna tercih imkanı bırakmaması gerekir⁸¹.

⁷⁹ Uygun, s.57.

⁸⁰ Özkan, s.135.

⁸¹ 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 (KVKK Uygulama Alanı), s.779.

Hukuka uygunluk sebebi olan hukuki yükümlülük Avrupa Birliği ve üye devletin hukukundan kaynaklanmalı ve bu mevzuatlara dayanarak yapılmalıdır. Diğer devletlerin mevzuatından kaynaklanan politikalardan doğan yükümlülüklerin hukuka uygunluk nedeni olarak değerlendirilmesi söz konusu değildir⁸². Bu kapsamda yapılan işlemlere örnek olarak sosyal güvenlik mevzuatından kaynaklanan bildirimler, vergi mevzuatı, finans kuruluşları bakımından kara para aklama ve yolsuzlukla mücadeleyle ilişkin düzenlemeler kapsamında veri sorumluları tarafından gerçekleştirilen bildirimler verilebilir⁸³.

4. Hayati Menfaatin Korunması

GDPR'nin 6/1-d maddesinde; *“veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile işleme faaliyetinin gerekli olması”* demek suretiyle veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerinin söz konusu olması durumunda kişisel verilerin hukuka uygun olarak işlenebileceği düzenlenmiştir. Bu düzenlemedeki hayati menfaat, yalnızca yaşam faaliyetlerini sürdürmekten ibaret görülmemeli, kişinin sağlığı veya beden bütünlüğü ile ilgili olan bütün menfaatleri hayati menfaat olarak kabul edilmelidir⁸⁴. Bu kapsamda işlenen verilerin hukuka uygunluğu için geçerli bir rızanın alınıp alınamayacağı hassa bir şekilde değerlendirilmeli, yaşamsal çıkarlar için kişisel verilerin işlenmesi en son ihtimalde düşünülmelidir. Ancak rızasını açıklayamayacak durumda olan veya rızasını açıklasa bile bu rızaya bir sonuç bağlanamayacak durumda olan kişiler bakımından kişisel verileri hukuka uygun işlemenin bir sebebi olarak yaklaşılmalıdır. Veri sahibinin hayati derecedeki çıkarları için bir kişisel veri işleme faaliyetinden bahsedebilmek için hayati tehlike yaratabilecek ve acil bir durumun söz konusu olması gerektiği kabul edilmektedir⁸⁵.

Doğal afetlerde, afet bölgesinde yaşayan vatandaşların ve yakınlarının ad, soyad, telefon numarası gibi bilgilerinin sosyal medyada veya kamusal alanlarda

⁸² Develioğlu, s. 63.

⁸³ Aşıkoğlu (Büyük Veri), s.80.

⁸⁴ Yücedağ, KVKK Uygulama Alanı, s.777.

⁸⁵ Taştan, s. 168.

paylaşılmasında acil ve hayati bir menfaatin bulunduğu kabul edilebileceğinden, burada hukuka uygun bir işleme söz konusudur.

5. Kamu Görevinin Yerine Getirilmesi

GDPR'nin 6/1-e maddesinde; *“kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması hususunda işleme faaliyetinin gerekli olması”* demek suretiyle bir kamu görevinin ifası sırasında veya veri sorumlusuna verilen resmi bir yetkiyle yapılan işlemenin hukuka uygun olacağı düzenlenmiştir. Veri sorumlusuna verilen resmi yetki ile birlikte veri sahibinin haklarının korunması için sahip olduğu tüm güvenceler ayrıntılı olarak düzenlenmelidir. Bu düzenleme, hukuki sorumluluğun yerine getirilmesi ile benzer olmakla birlikte aslında birbirinden iki ayrı konuyu kapsamaktadır. Burada 6/1-c maddesinden farklı olarak veri sorumlusunun bir hukuki yükümlülüğünün bulunması şart değildir. Ancak verilerin paylaşıldığı kurumun kanunlarla resmi yetkili kılınması gereklidir. Kamu görevi, hukuki bir sorumluluğu yerine getirmeyi de içerebilir, ancak bu düzenlemenin kapsamı çok daha geniştir. Veri sorumlusunun, yasal düzenlemelerle kendisine herhangi bir sorumluluk yüklenmemiş rağmen; kamu yararını gözeterek kendi inisiyatifiyle yaptığı işlemler, somut olayda “gereklilik” unsurunun bulunması halinde bu madde kapsamında değerlendirilir. Ayrıca düzenlemenin kamu görevi demesine rağmen sadece kamu sektöründeki değil, özel sektördeki veri sorumluları yönünden de geçerlidir⁸⁶.

Maddede bahsi geçen resmi yetkinin, veri sorumlusu tarafından bizzat kullanılıyor olması şart değildir. Resmi yetkiye sahip bir kamu görevlisinin taleplerini karşılamak kapsamında yapılan işleme de hukuka uygun kabul edilecektir. Örneğin; bir suç soruşturması kapsamında resmi yetkili otoriteler tarafından yapılan bilgi taleplerini karşılamak sonucu yapılan işleme bu madde kapsamında hukuka uygun bir işleme olarak kabul görür. Yine bir veri sorumlusunun veri işleme faaliyeti

⁸⁶ Yörük, s. 67.

sırasında öğrendiği suç teşkil eden olayı yetkili kamu otoriteleri ile herhangi bir talep gelmeden paylaşması da bu madde kapsamında bir işleme faaliyetidir⁸⁷.

6. Meşru Menfaatlerin Korunması

GDPR'nin 6/1-f maddesinde; *“özellikle veri sahibinin çocuk olması halinde veri sahibinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması”* olarak tanımlandığı üzere; veri işleme faaliyeti, veri sorumlusu ya da üçüncü kişi tarafından ulaşılmak istenen meşru menfaatlere ulaşılabilmesi için gerekli ise hukuka uygun olarak kabul edilir. Meşru menfaatler söz konusu olsa bile, temel hak ve özgürlüklerin sınırına dikkat edilmesi gerekmektedir. Meşru menfaatin kime ait olduğunun belirlenmesi önemli bir husustur. Meşru menfaatin sınırlarını belirlemek adına GDPR'de meşru menfaat sahibi, veri sorumlusu olarak belirlenmiştir. Daha çok ticari konularla bağlantılı olarak kullanılması nedeniyle doktrinde bu işleme faaliyeti, meşru ticari çıkarlar olarak da ifade edilmektedir⁸⁸. Veri sorumlusunun meşru menfaati, veri işleme sonucunda ortaya çıkacak olan somut fayda ve çıkarları hedef almaktadır. Buna göre bir şirket sahibi çalışanlarının temel haklarına ve mahremiyetlerine saygı göstermek kaydıyla, çalışanlarının terfi ve maaş gibi sosyal haklarını düzenlemek amacıyla kişisel verileri işleyebilir. Bununla birlikte şirket sahibi işletmesel reformlarını da gerçekleştirmiş olacaktır. Bu bağlamda, çalışanların terfi almaları ve işletmede iyileştirmelerin yapılması veri sorumlusu olan şirket sahibinin meşru menfaatinedir⁸⁹.

GDPR, işleme faaliyetinin gerekli olmasına da özellikle değinmiştir. Buna göre; verinin işlenmesi meşru menfaatin gerçekleşmesi ya da kullanılması için gerekli olmalıdır. Yani veri işleme ile meşru menfaat arasında sıkı bir ilişki bulunmalıdır. Bununla birlikte, veri sorumlusunun menfaatinin gerçekleşmesi için

⁸⁷ Develioğlu, s.65.

⁸⁸ Yücedağ, KVKK Uygulama Alanı, s.783.

⁸⁹ Özgür Eralp, "Veri Sorumlusunun Meşru Menfaatleri için Veri İşlenmesinin Zorunlu Olması", <https://www.ozgureralp.com.tr/soru-327-ilgili-kisinin-temel-hak-ve-ozgurluklerine-zarar-vermemek-kaydiyla-veri-sorumlusunun-mesru-menfaatleri-icin-veri-islenmesinin-zorunlu-olmasi-ne-anlama-gelmektedir/> (13.03.2021)

kişisel verinin işlenmesini gerektirmeyen veya kişinin hakkını daha az ihlal eden bir seçenek mevcutsa bu seçeneğin tercih edilmesi gerekmektedir. Veri sorumlusunun kendi ürünleri hakkında reklam göndermesi de meşru menfaat kabul edilmektedir. Ancak bu durumda kişi hakkındaki farklı kaynaklarda yer alan verilerin bir araya getirilerek bir profil oluşturulması ve bu profildeki kişilere özel reklam gönderilmesi meşru menfaat kapsamında hukuka uygun kabul edilemeyecektir⁹⁰.

B. Hassas Verilerin İşlenmesi

GDPR'nin 9. maddesinde kişiye ait hangi bilgilerin özel kategori içerisinde kabul edilen hassas veriler olduğu sayılmış ve bununla birlikte hassas verilerin hangi durumlarda işlenebileceği hüküm altına alınmıştır. Kişisel verilerde olduğu gibi hassas verilerde de asıl olan işlemenin yasak olmasıdır. Yani hukuka uygunluk sebepleri olmadığı sürece hassas verilerin işlenmesi hukuka aykırıdır. Hassas verilerin bu şekilde ayrı bir öneme sahip olmasının temel nedeni, özel korumaya ihtiyaç duyan bu özelliklerin bir ayrımcılık kaynağı olmaya müsait olmasıdır. Bu nedenle adı gibi hassas olan özel korunmaya muhtaç bu verilerle ilgili daha sıkı korunma tedbirleri düzenlenmiştir. Veri sahibinin ancak açıkça muvafakat etmesi halinde hassas verileri işlenebilir. Zımnı muvafakat GDPR tarafından kabul edilmemiştir.

Veri sahibinin hukuki veya fiziki nedenlerle rıza gösteremeyecek durumda olduğu hallerde, veri sahibinin veya başka bir gerçek kişinin hayati çıkarlarının korunması için hassas verilerin işlenmesi gerekli ise; bu durumda işlemenin hukuka aykırılığı ortadan kalkar. Bu hukuka uygunluk nedeni esas itibarıyla insan hayatını tehlikeye atan durumların varlığı halinde hassas verilerin işlenmesini amaçlamaktadır.

Hassas verilerin veri sahibi tarafından açık bir şekilde kamuya açıklanmış olması halinde veriler işlenebilir. Burada açıklamanın veri sahibi tarafından iradi olarak ve açıkça herkesin bilmesini isteyerek yapılmış olmasına dikkat edilmelidir.

İşlemenin, hukuki iddiaları tesisi ve korunması için gerekli olması durumunda veya mahkemelerin yargılama yetkileri çerçevesinde hareket ettiği

⁹⁰ Meşru menfaat hakkında detaylı bilgi için bkz. Çekin, ss.95-105.

durumlarda işleme hukuka uygun hale gelir. Kişisel verilerin ve özellikle hassas verilerin korunması amacıyla gözetilen amaçlarla ters düşmeyecek şekilde Avrupa Birliği veya üye devlet hukukunun kamusal yararları için yapılan ve veri koruma hakkının özüne saygı gösteren işlemler hukuka uygun kabul edilir.

Koruyucu hekimlik veya meslek hekimliği için, bireysel sağlık ve halk sağlığına yönelik hizmetlerin sunulması amacıyla Avrupa Birliği veya üye devletin hukukuna dayalı olarak hassas verilerin işlenmesi mümkündür.

Kamu yararını sağlamaya yönelik olarak Avrupa Birliği ve üye ülkelerin hukukları doğrultusunda bilimsel, tarihi veya istatistiki amaçlarla hassas verilerin işlenmesi hukuka uygundur. Üye Devletler genetik, biyometrik veya sağlıkla ilgili veriler ile alakalı olarak sınırlamalar da dahil olmak üzere ek koşullar uygulamaya devam edebilir ya da ek koşullar getirebilir⁹¹.

V. KİŞİSEL VERİLERİN KORUNMASINDA TEMEL HAKLAR VE ÖZGÜRLÜKLER BOYUTU

Günümüzde yaygınlaşan küresel ticaret kavramıyla birlikte, kişisel veriler bu ticaretin konusu haline gelmiştir. Ekonomik imkanların artması ve hızla ilerleyen teknolojik gelişmeler sayesinde kişisel veriler tek tuş ile kaydedilebilir ve işlenebilir hale gelmiştir. Ancak kişisel verilerin korunması hakkının özünde kişisel verinin ticari kapsamında ziyade insan hakları ve temel özgürlükler boyutuyla değerlendiren görüşler de mevcuttur.

A. Özel Hayatın Gizliliği Hakkı Boyutu

Hayatının resmi makamlarca sürekli kayıt altında olduğunu düşünmek bireyi kendisi olmaktan alıkoyacak ve birey, kişi olmanın gereklerini dilediği gibi yerine getiremeyecektir. Sürekli izlenen, yaşamına ilişkin bilgiler kayıt altına alınan, bireyler bütün bunların sonucunda şeffaflaşmak zorunda kalır ve bu durumdaki bir bireyin kişiliğini serbestçe yaşaması ve geliştirmesi de beklenemez⁹².

⁹¹ Hassas veriler hakkında detaylı bilgiler için bkz. Kaya, ss. 317-333.

⁹² Şimşek'ten aktaran Küzeci s. 77.

Kişisel verilerin korunması bir hak ve özgürlük anlamında ilk olarak özel hayat ve özel hayatın gizliliğinin korunması kapsamında ele alınmıştır. Ancak gelişen teknoloji ile birlikte özel hayatın gizliliği hakkında yapılan genel incelemeler kişisel verilerin korunmasını açıklamada yetersiz kalmıştır. İlerleyen süreç içerisinde kişisel verilerin korunması özel hayatın gizliliği hakkından ayrılmaya başlamıştır. Yine de kişisel verilerin korunması ve özel hayatın gizliliği hakkı arasındaki ilişkiyi yok sayarak kişisel veri ve özel hayatın gizliliğini birbirinden ayrı düşünmek mümkün değildir. Bu nedenle kişisel verilerin korunması hakkıyla ilgili incelemeler yaparken özel hayatın gizliliği de beraberinde gelmektedir⁹³. Özel hayatın gizliliği hakkı, kişisel verilerin korunmasıyla iç içe geçmiş olan ve gerek uluslararası hukukta gerekse ulusal hukukta garanti altına alınan temel bir haktır. Bu hak, İnsan Hakları Evrensel Beyannamesi'nin 12.maddesinde, Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesi'nin 17. maddesinde, Avrupa İnsan Hakları Sözleşmesi'nin 8.maddesinde ve 1982 Anayasasının 20. maddesinde temel bir hak olarak düzenlenmiş ve koruma altına alınmıştır. Bununla birlikte, özel hayatın gizliliği hakkının kapsamı ve koruma alanı son derece geniştir. Bu denli kapsamlı bir hakka karşı yönelebilecek saldırılar da çok çeşitli alanlardan gelmektedir. Bu nedenlerle özel hayatın gizliliği konusunda mutlak bir tanımın yapılması da güçtür⁹⁴. Bayraktar'a göre özel hayat bu kavramın kapsadığı alanı kişinin kendisinin belirlediği, başkalarını bu alana almaya ve alandan çıkarmaya yetkili olduğu, izni olmaksızın da kimsenin müdahale edemeyeceği, korunaklı bir alandır⁹⁵. Özek'e göre özel hayat herkes tarafından bilinmesi mümkün olmayan, ancak özel araştırmalar sonucu öğrenilebilecek kişiye ait hususlardır⁹⁶. Westin'e göre ise özel hayat bireylerin ve toplumların kendileri hakkındaki bilgilerin ne zaman, nasıl ve hangi kapsamda başkaları ile ilişki içinde bulunacağına kendilerinin karar verme hakkıdır⁹⁷. Özel hayat tanımına dair farklı yaklaşımlar geliştirilmiş olmasına rağmen, özel hayat- kişisel veri ilişkisinin olduğuna dair görüşler aynı yönde şekillenmiştir.

⁹³ Küzeci, s. 71.

⁹⁴ Mendos Kuşkonmaz, s.26.

⁹⁵ Köksal Bayraktar, "Özel Yaşamın Gizliliğine Saygı İlkesi" **Maltepe Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:1,Sayı:1, 2007, s.113.

⁹⁶ Çetin Özek, **Türk Basın Hukuku**, İstanbul Üniversitesi Hukuk Fakültesi Yayınları, İstanbul, 1978, s. 259 dan aktaran Nagihan Türkel, **Özel Hayatın Gizliliğini İhlal Suçu**, (Yayımlanmamış Yüksek Lisans Tezi), Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir, 2010, s.3.

⁹⁷ Alan Westin, **Privacy and Freedom**, ABD, 1970, s.7'den aktaran Küzeci, s. 73

Buna göre; özel hayatın gizliliği hakkı kişisel verilerin korunmasıyla sıkı bir ilişki içerisinde olmakla birlikte, kişisel verilerin korunması başlı başına bağımsız bir hak ve özgürlük olarak karşımıza çıkmaktadır. Öyle ki kişisel verilerin korunmasına ilişkin gerek ülkemizde yürürlüğe giren Kişisel Verilerin Korunması Kanunu, gerek Avrupa Birliği bünyesinde kabul edilen GDPR, kişisel verilerin başlı başına bir hak olduğunu ve özel düzenlemeler ile korunması gerektiğini ortaya koymaktadır.

B. Düşünce ve İfade Özgürlüğü Boyutu

Kişisel verilerin korunması hakkının düşünce özgürlüğü ile de sıkı bir bağlantısı bulunmaktadır. Düşünce özgürlüğünün, ulusal sınırlar içinde birey ve toplumun gelişimi açısından taşıdığı önem, hukuk tarafından sağlam güvencelere bağlanmasını zorunlu kılmaktadır. Hukukun amacı da, düzen içerisinde toplumun varlığını devam ettirmesini sağlarken, bireyin özgürlüklerini gereksiz sınırlamalardan ve müdahalelerden korumaktır⁹⁸. Düşünce, insanı diğer canlılardan ayıran en önemli etkinliktir. Düşünebilen bir canlı olarak insan, sahip olduğu düşünceler ile birlikte kendiliğinden kişisel veriler de oluşturmaktadır. Düşünceyi koruyan hukuk sistemleri, buna bağlı olarak gelişen kişisel verileri de korumayı bir hak olarak görmektedir. Düşünceyi açıklama özgürlüğünün, hem pozitif hem de negatif yönlü etkisi vardır. Yani devlet, bir kişiyi verilerini açıklamaya zorlayamayacağı gibi kişinin verilerini kime, nasıl açıklayacağı yönünde bir sınır da çizemez⁹⁹. Düşünce ve ifade özgürlüğünün korunması ile kişisel verilerin sınırlarının korunması arasında ince bir çizgi bulunmaktadır. Zira ifade özgürlüğünde sınırın biraz aşılması kişisel verilerin korunmasına zarar verebilecekken, kişisel verilerin korunmasında olması gerekenden biraz daha sert durulması da ifade özgürlüğünün alanını zedeleyecektir. Doktrinde iki hakkın birbirinin alanına müdahalede bulunabileceği basın özgürlüğü üzerinden örneklenmektedir. Şöyle ki kişisel verilerin korunmasının üstünlüğüne yönelik düzenlemeler ifade özgürlüğüne ve dolayısıyla basın özgürlüğüne müdahale

⁹⁸ Düşünce özgürlüğü hakkında detaylı açıklamalar için: Ümmühan Kaygısız, “Düşünce Özgürlüğüne Verilen Önem Açısından Hukuk Sistemlerine Kavramsal Bir Yaklaşım”, *Akademik Bakış Dergisi*, Sayı:52, 2015, ss.102-103.

⁹⁹ Şimşek, s.147’ den aktaran Ayözger, s.51.

anlamına gelebileceğinden eleştirilmiştir¹⁰⁰. Basının haber yapma amacıyla birisinin hayatına müdahalesi, aynı zamanda kişisel verilerine müdahale anlamını taşıdığı noktada kişisel verilerin korunması hakkının zedelenmesine neden olacaktır. Ancak kişisel verileri korumak amacıyla basının devreden çıkarılması durumunda da ifade ve haber alma özgürlüğü zarar görecektir. Zira ani gelişen olaylar ve anlık yakalanan haberlerde kişisel verilerin işlenmesi için rıza alınması mümkün olmayacağından kişisel verilerin işlenmesinde hukuka aykırılık ortaya çıkacaktır. Bu nedenle haklar ve özgürlükler dengesini korumak iki hakkın da etkili olarak kullanılabilmesi açısından önem taşımaktadır.

C. Unutulma Hakkı Boyutu

Günümüzde bilgiye ulaşmak, teknolojinin geldiği nokta itibariyle son derece hızlanmıştır. Dünya'nın bir ucunda paylaşılan bir fotoğraf diğer ucunda aynı anda görüntülenebilmekte ve bu paylaşım yıllarca internet hafızalarında saklı kalabilmektedir. Bu nedenle kişinin ileride görülmesini istemediği paylaşımları ortadan kaldırması ve hayatını bu paylaşımları olmadan şekillendirmesi zor bir hale gelmiştir. Bu sorunlar dolayısıyla düzenlenmesine ihtiyaç duyulan “Unutulma hakkı dijital hafızada yer alan bireylere ait rahatsız edici her türlü kişisel içeriğin, yine bireylerin talebi üzerine bir daha geri getirilemeyecek biçimde ortadan kaldırılması/silinmesi olarak tanımlanmıştır”¹⁰¹.

Unutulma hakkının dijital hafıza ile şekillenen bu tanıma bakıldığında var olması gereken unsurların kişisel ve dijital bir içerik olduğu ön plana çıkmaktadır. Konumuzla olan ortak noktası ise bu dijital ve kişisel içeriklerin aynı zamanda kişisel veri niteliği taşıyor olmasıdır. Teknolojinin ilerlemesi ile birlikte mahremiyet alanı daralırken kişisel verilerin yayıldığı alan ve yayılma hızı artmaktadır. Bu denli hızla yayılan bilgiler özel hayatın gizliği hakkı ve kişisel verilerin korunması hakkının ihlalini de beraberinde getirmektedir. Dijital hafızanın kuvvetli ve uzun ömürlü olması da ihlalin boyutunu ağırlaştırmaktadır. Bu nedenle kişiler verilerinin hayat

¹⁰⁰ Sinem Göçmen Uyarer, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, 2. Baskı, Seçkin Yayıncılık, Ankara, 2020, s.34.

¹⁰¹ Seray Nalbantoğlu, “Bir Temel Hak Olarak Unutulma Hakkı”, **Türkiye Adalet Akademisi Dergisi**, Sayı:35, 2018, s. 589.

boyu dijital bir hafızada saklı kalarak her an yeniden karşısına çıkması ihtimalinin önüne geçmek adına kullanabilecekleri bir unutulma hakkına sahiptir. Bu bağlamda GDPR'nin 17. maddesinde silme hakkı ile eş anlamlı olarak unutulma hakkı düzenlemesine yer verilmiştir. Veri sahibinin rızası doğrultusunda işlenen verilerin işleme amacının gerçekleştirilmiş olmasıyla birlikte daha fazla tutulmasının gereksiz hale gelmesi durumunda, yine veri sahibinin rızasını geri almış olması veyahut verinin işlenmesine itiraz etmiş olması halinde; veri sahibi derhal veriyi silmek durumundadır¹⁰². Unutulma hakkı kapsamındaki silme işlemi yalnızca veri sahibinin talebi üzerine yapılmaktadır. Veri sahibi dışında bir üçüncü kişinin talepte bulunması hakkın doğası gereği mümkün değildir. Bu kapsamda ölen kişi adına mirasçılarının unutulma hakkı kapsamında herhangi bir talepte bulunmasının mümkün olup olmadığı konusunda tartışmalar mevcuttur¹⁰³.

Unutulma hakkı kapsamında ABAD tarafından verilen C-131/12 sayılı González v. Google Inc, Google İspanya kararı, unutulma hakkının kapsamı ve niteliği konusunda açıklamalar getirmektedir. 2010 yılında meydana gelen olayda; Costeja González, adını arama motoruna yazdığı 1998 yılında sosyal güvenlik borçlarının ödemek için evini satılığa çıkardığına dair haber yapan La Vanguardia gazetesinin sahibi La Vanguardia Ediciones'i İspanya Veri Koruma Kurumu'na şikayet etmiştir. Costeja González'in ilk talebi Vanguardia gazetesinin haberi kaldırması veya kendisine ait kişisel verilerin görülemeyeceği bir şekilde haberin düzeltilmesi olmuştur. Diğer talebi ise Google İspanya veya Google Inc.'in kendisiyle ilgili kişisel verilerin kaldırılması veya gizlenmesini; sonuç itibarıyla arama sonuçları arasında yer almamasını ve La Vanguardia ile olan bağlantılar içerisinde görülmemesini talep etmiştir. İspanya Veri Koruma Kurumu; haberin ihaleye katılımcı sağlamak amacıyla yapıldığı gerekçesiyle La Vanguardia'ya yönelik yapılan şikayeti reddetmiştir. Bunun yanı sıra Google İspanya ve Google Inc hakkındaki şikâyeti arama motorlarında kişisel veri işlendiği gerekçesiyle veri koruma mevzuatı kapsamında kabul etmiştir. İspanya Veri Koruma Kurumu'nun şikayeti kabul kararına karşı Google İspanya ve Google Inc, İspanya mahkemelerine başvurmuştur. Mahkeme'nin görüş bildirmesi için yaptığı başvuru üzerine konu Avrupa Birliği Adalet Divanı önüne gelmiştir. Yapılan değerlendirmede Google

¹⁰² Ayözger, s. 50.

¹⁰³ Unutulma hakkı kapsamında tartışmalar ve detaylı açıklamalar için bkz. Nalbantoğlu, ss. 583-602.

İspanya ve Google Inc.'in veri sorumlusu sıfatına sahip olduğu; bu nedenle, belirli ve meşru amaçlarla verileri elde etme, kişisel verileri hukuka ve dürüstlük kuralına uygun bir şekilde işlememe yükümlülüğü altında olduğu sonucuna varılmıştır. Olayda ise Costeja González'e ait verilerin geçersiz ve amacı aşan şekilde tutulduğu, tarihi, istatistiksel veya bilimsel amaçlar bakımından gerekmediği müddetçe öngörülen süreleri aşacak şekilde saklanmaması gerektiği, arama sonuçlarında yer alan bağlantıların kamu yararı gibi özel bir durumun olmadığı hallerde silinmesi gerektiği ve bu nedenle şikayetin haklı olduğu değerlendirilmiştir¹⁰⁴. Kararda da vurgulandığı üzere verinin sahibi tarafından rızanın geri alınması, veriyi elde etme amacının gerçekleşmesi, veriyi saklamak için olayın üzerinden uzunca zaman geçmiş olması unutulma hakkı kapsamında verilerin silinmesini talep etmek için geçerli bir sebeptir.

D. Bilgi Edinme Hakkı Boyutu

Bilgi edinme hakkı, bireylerin kamu kurum ve kuruluşlarının görevlerinden dolayı sahip oldukları bilgilere erişim hakkıdır. Bu hak, ilgili mevzuat uyarınca bireylerin idareye yapacağı bilgi edinme başvurularının yanı sıra, idarenin kendi inisiyatifi ile belli bilgi ve belgeleri erişime açmasını da kapsar. 21. yüzyıl devlet yönetiminde açıklık ve şeffaflık ilkelerinin teminatı olan bilgi edinme hakkının, tüm gerçek ve tüzel kişilere eşitlik ve tarafsızlık ilkelerine uygun olarak kullandırılmasının sağlanması, günümüz modern demokratik devletlerinin temel bir görevidir¹⁰⁵.

Bilgi edinme hakkı gündeme geldiğinde devlet, bireyin bilgiye ulaşmasını engellememe; hatta bilgiye ulaşmayı kolaylaştırma, doğru bilgiye sağlıklı bir şekilde ulaşmayı sağlama yükümlülüğü altındadır.

Bilgi edinme hakkı ile korunan eylem ve işlemlerde şeffaflık sayesinde; bireyler gerek kendileriyle gerek içinde bulundukları toplumla ilgili gelişmelerden haberdar olurlar. Bilgi edinme hakkının sağladığı güvence ile vatandaşlar, yönetim sürecinde dilerse söz sahibi olup kendi lehlerine olan sonucu elde etme yönünde

¹⁰⁴ Avrupa Birliği Adalet Divanı'nın 13.05.2014 tarihli ve C-131/12 sayılı kararı için bkz : <https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en> (19.03.2021)

¹⁰⁵ Bilgi Edinme Değerlendirme Kurulu, **25 Soruda Bilgi Edinme Hakkı**, Bilgi Edinme Değerlendirme Kurulu Yayınları, Ankara, 2015, s.7.

girişimlerde bulunur ve *kendi kaderini tayin etme*¹⁰⁶ imkanına sahip olurlar. Avrupa Birliği bünyesinde de son derece önemli olan bu hak Avrupa Birliği Temel Haklar Şartı'nın 42. maddesinde “belgelere erişim hakkı” başlığı altında güvenceye alınmıştır. Buna göre; Avrupa Birliği'nin her vatandaşı Avrupa Parlamentosu, Konsey ve Komisyon belgelerine erişim hakkına sahiptir. Avrupa Birliği düzeyinde belgelere erişim hakkını ele alan özel metin ise 1049/2001 Sayılı Avrupa Parlamentosu, Konsey ve Komisyon Belgelerine Halkın Erişimine İlişkin Yönetmelik'tir. Metinde şeffaflığın önemine vurgu yapan düzenlemeler yer almaktadır. Yönetmeliğin temel amacı Avrupa Birliği Kurumları'nın belgelerine mümkün olan en geniş erişimin sağlanması olmakla birlikte; kişisel verilerin korunmasına ilişkin hükümler bu erişimden istisna tutulmuştur. Buradan yapılabilecek çıkarım ise; Avrupa Birliği 1049/2001 Sayılı Yönetmelik ile bilgi edinme hakkının sınırını kişisel verilerin korunması hakkı ile kesiştiği alan olarak çizmiştir. Bilgi edinme ve kişisel verilerin korunması hakkı birbiriyle son derece yakın ilişkilendirilebilecek iki alandır. Pek çok noktada birbirine paralel bulunan bu iki hak, bazı kaynaklarda “*bir madalyonun iki yüzü*” veya “*bilgi toplumu hukukunun iki sütunu*” olarak değerlendirilmiştir¹⁰⁷.

Bilgi edinme hakkının kullanılmasını temin amacıyla herkese tüm bilge ve verilere ulaşma olanağı tanınırsa, veri sahiplerinin verilere ulaşma, verilerinin işlenişini kontrol altında tutuma gibi hakları zarara uğrar. Zira, veri sahibinin rızası hilafına ve bilgisi dışında verileri başkalarına aktarılırsa; veri sahibi kişisel verilerinin koruma konusunda haklarını kime karşı ileri sürebileceğini bilemez. Bu durum da en başta insan haklarının korunmasının özüne aykırıdır. Verilere ulaşımın serbest kılınması, veriye her türlü amaç için ulaşılmasını da mümkün kılar. Bu durum da başta açıkladığımız kişisel verilerin işlenmesinde hakim olan ilkelere aykırı düşer. Bu nedenle, idari yönetimde gizliliğin uygulanması gereken noktalardan biri olarak, kişisel verilerin korunması alanı karşımıza çıkmaktadır. Kişisel verilere temas etme

¹⁰⁶“Kendi kaderini tayin, I. Dünya Savaşı sonrasında büyük imparatorlukların parçalanmasıyla ortaya çıkan nispeten yeni ve küçük devletlerin kurulması süreciyle uluslararası ilişkiler çerçevesinde tartışılmaya başlanan bir kavram olmuştur. Ancak kavramın tarihsel kökleri Ortaçağa ya da Batı Avrupa'daki sosyal uyanışa dayanmaktadır”. Hakkın özüne ilişkin detaylı açıklamalar için bkz. Volkan Tatar, Nuri Gökhan Toprak, “Kendi Kaderini Tayin Kavramının Hukuki ve Siyasi Yönleri Üzerine Bir İnceleme”, **Bilge Strateji Dergisi**, Cilt:7, Sayı:13, 2015, ss.55-69.

¹⁰⁷ Alexander ROßNAGEL, “Konflikte Zwischen Informationsfreiheit und Datenschutz?”, **MMR**, 2007, Heft 1, s.16. dan aktaran Küzeci, s. 104.

ihtimalinin yüksek olması nedeniyle, bilgi edinme hakkı kullanılırken veri korumasına özen gösterilmeli; bununla birlikte veri korumasını sağlamak için bilgi edinme hakkının kapsamı da daraltılmamalıdır¹⁰⁸.



¹⁰⁸ Küzeci, s. 105-107. Ayrıca; idare hukuku anlamında bilgi edinme hakkının sınırları ve yönetimde açıklık konusunda detaylı açıklamalar için bkz. Tekin Akılhoğlu, “Yönetimde Açıklık-Gizlilik ve Bilgi Alma Hakkı”, **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, Cilt:46, Sayı:3-4, 1991, ss.1-12.

İKİNCİ BÖLÜM

AVRUPA BİRLİĞİ HUKUKUNDA DÜZENLEMELER VE KURUMLAR

ÇERÇEVESİNDE KİŞİSEL VERİLERİN KORUNMASI

Kişisel verilerin korunması hukuku, uzun yıllar boyunca yaşanan gelişmeler ışığında şekillenmiş ve üzerine pek çok çalışma yapılmıştır. Bu bağlamda gerek ülkeler münferit olarak gerek de ulus üstü birlikler bazında düzenlemeler gündeme gelmiştir. Burada da evrensel olarak kişisel verilerin korunması hukukuna yön veren ulus üstü düzenlemelere değinmek gerekmektedir.

I. KURUMLAR BAZINDA KİŞİSEL VERİLERİN KORUNMASI

1970’li yıllardan günümüze değin gelişen teknolojiye bağlı olarak önem kazanan kişisel veri kavramı hakkında ulus üstü birlikler nezdinde çalışma yapma gereği doğmuştur. Tarihsel süreçte karşımıza çıkan uluslararası kurumlar hızla ilerleyen ve artık küresel boyutta önem kazanan kişisel verilerin korunması kavramına uzak kalamamıştır. Bu nedenle Dünya’da ve Avrupa’da etkili olan kurumlar bazında çeşitli yasal düzenlemeler yapılmıştır.

A. OECD İlkeleri

Kişisel verilerin korunması hukukunun uluslararası bir mesele haline gelmesiyle birlikte, kurumların da bu konudaki hassasiyeti artmıştır. Uluslararası alanda kişisel verilerin korunması hususunda ilk girişimde bulunan ulus üstü kurum; uluslararası boyutta ekonominin gelişmesi için kurulmuş olan OECD (Uluslararası Ekonomik İşbirliği ve Kalkınma Örgütü) olmuştur. İlerleyen teknoloji ile birlikte, ekonomik açıdan da hayatın önemli bir parçası haline gelen kişisel veriler konusunda OECD; verilerin depolanması, işlenmesi, paylaşılması gibi hususlarda düzenleme yapmıştır. Bu bağlamda 1980 yılında “Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler” kabul edilmiştir. 8 maddeden oluşan bu

ilkeler, veri toplamanın ne şekilde olması, veri toplamanın amaçları, veri kullanımı konularında düzenlemeler içermektedir¹⁰⁹.

OECD'nin kişisel veriler üzerinde çalışmaya başlaması daha eskilere dayanmaktadır. Avrupalı devletlerin yanı sıra Japonya ve veri işleme alanında faaliyet gösteren ABD ile Kanada ile birlikte Avustralya'yı da bünyesinde barındıran OECD, bilgisayar kullanımı ve veri işleme konularında ilk olarak 1960'lı yıllarda ilgilenmeye başlamıştır¹¹⁰. 1969 yılında oluşturulan "Veri Bankaları Paneli" isimli uzman kişilerden oluşan grup ile kişisel veriler ile ilgili yapılacak işlemler üzerinde yoğunlaşmıştır. 1978 yılında oluşturulan yeni bir çalışma grubuna bu husustaki tavsiyeleri hazırlama görevi verilmiş ve bu çalışmalar neticesinde, 1980 yılında Rehber İlkeler kabul edilmiştir¹¹¹.

2013 yılında güncellenen ilkelerin düzenlenmesinin temel amacı; uluslararası alanda, birçok veriye kısa süre içerisinde hukuka aykırı olarak erişim sağlayan veri işleme sistemlerinin geliştirilmesi nedeniyle kişisel verilerle ilgili gizliliğin korunmasının bir takım temel prensiplere bağlanması ihtiyacıdır. Sınır ötesi kişisel veri akışının yeknesaklaştırılmasının ekonomik ve toplumsal kalkınmaya katkıda bulunması ve üye ülkeler arasındaki serbest veri akışını sağlarken yaratılan haksız engellemelerin önüne geçilmesi hedeflenmiştir¹¹². Bu ilkelerin önemi; kişisel verileri bir ekonomik hak olarak kabul ettiğinden bahsettiğimiz Amerika Birleşik Devletleri ile kişisel verilere temel bir insan hakkı olarak yaklaşan Avrupa Birliği tarafından aynı anda kabul edilmiş olmasıdır. İlkeler çerçeve niteliğinde olup herhangi bir bağlayıcılıkları olmamakla birlikte, üye ülkelerin iç hukuklarına uyarlanması zorunlu kılınmıştır¹¹³. Bu ilkeler şunlardır :

1. Veri Toplanması Sınırlama İlkesi: Kişisel veriler sınırlı olarak, hukuka uygun, adil bir şekilde ve mümkün ise veri sahibinin bilgisi ve rızası ile toplanmalıdır.

¹⁰⁹ Göçmen Uyarer, s.43.

¹¹⁰ OECD ilkelerinin tarihsel gelişimi hususunda detaylı açıklamalar için: İkbâl Gür, **Kişisel Verilerin Korunması Hususunda AB İle ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Turhan Kitabevi, Ankara, 2010, s.109 vd.

¹¹¹ Uygun, s.25.

¹¹² Muhammet Sefa Mutlu, **Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması**, Adalet Yayınevi, Ankara, 2020, ss.76-77.

¹¹³ Murat Altındere, **Kişisel Verilerin Korunması Hukuku ve Uygulaması**, Adalet Yayınevi, Ankara, 2020, s.20.

2. Veri Kalitesi İlkesi: Kişisel veriler işlenecekleri amaç için gerekli olduğu kadarıyla, doğru ve güncel tutulmalıdır.

3. Amaca Özgünlük İlkesi: Kişisel verinin hangi amaç için toplandığı en geç toplandığı ana kadar belirtilmeli ve verinin kullanımı toplandığı amaç ile sınırlı olmalıdır.

4. Kullanımı Sınırlama İlkesi: Kişisel veriler veri sahibinin rızası olmadan veya kanunun tanıdığı yetki olmadan paylaşılmamalı ve erişime açılmamalıdır.

5. Güvenlik Önlemleri İlkesi: Kişisel veriler; kaybolma, çalınma, yetkisiz erişim, yok olma durumlarına karşı makul güvenlik önlemleri ile korunmalıdır.

6. Açıklık İlkesi: Kişisel verilerle ilgili gelişmeler, politikalar hakkında bir açıklık olmalıdır. Kişisel verilerin varlığı, kullanım amacı, veri sorumlusunun kimliği ve her zamanki yerleşim adresi kolayca saptanabilir olmalıdır.

7. Bireyin Katılım İlkesi: Bireyin kendisiyle ilgili veriler hakkında; veri sorumlusunun kendisi hakkındaki verilere sahip olup olmadığını öğrenme hakkı vardır. Birey kendi verilerinin anlayabileceği şekilde ve makul bir süre içinde kendisiyle paylaşılmasını isteyebilir. Bireyin kendisiyle ilgili verilere itiraz etme, sildirme, düzelttirmesi mümkündür.

8. Hesap Verilebilirlik İlkesi: Veri sorumlusu önceki 7 ilkeye uyduğunu gösterebilmelidir¹¹⁴.

OECD Rehber İlkeleri çeşitli ülkelerde farklı sektörlerde halen kullanılmaktadır. Türkiye’de Kişisel Verilerin Korunması Kanunu gerekçesinde de ilkelere atıfta bulunulması, ulusal düzenlemelerde ilkelerin etkisinin halen devam ettiğini göstermektedir¹¹⁵.

B. 108 Sayılı Avrupa Konseyi Sözleşmesi

1960’lardan itibaren gelişen teknoloji ile birlikte artan küresellik, devletleri münferit olarak etkilediği gibi çeşitli ulus üstü kurumları da kişisel veriler konusunda yaklaşımlar geliştirmeye itmiştir. Bilgi teknolojilerinde yaşanan ilerlemeler ile

¹¹⁴ Rehber ilkelerle ilgili düzenlemenin detayları ve OECD Konsey Tavsiyesi için: Bora Gemicioğlu, Zeynephan Gemicioğlu, **Kişisel Verilerin Korunması Mevzuatı Uluslararası Düzenlemeler ve İhtihatlar**, On İki Levha Yayınları, İstanbul, 2020, ss.381-406.

¹¹⁵ Küzeci, s.132.

birlikte kişisel verilerin işlenmesinde ciddi bir artış yaşanmıştır. İnternetin yaygınlaşması ile birlikte konu daha önemli hale gelmiştir. Bu süreçte Avrupa Konseyi de özel hayatın gizliliği ve kişisel verilerin korunması konusuna yönelmiştir. Bakanlar Komitesi bünyesinde kurulan Uzmanlar Komitesi, kişisel verilerin etkili bir şekilde korunması için yapılması gerekenler konusunda tavsiyelerde bulunmuştur. Bu tavsiyeler neticesinde ortaya çıkan 108 Sayılı Kişisel Verilerin Otomatik İşlemesi Karşısında Bireylerin Korunması Sözleşmesi 1981 yılında kabul edilmiştir. 108 Sayılı Sözleşme olarak da anılan bu metin, kişisel verilerin korunmasıyla ilgili olarak kabul edilen ilk bağlayıcı uluslararası sözleşmedir¹¹⁶. Sözleşme'nin 4. maddesine göre taraf devlet, Sözleşme'yi onaylamadan önce iç hukukunda bir takım yasal düzenlemeler yaparak Sözleşme ile yerine getirme yükümlülüğü altına girdiği ilkeleri koruma altına almalıdır. Ülkemizde kişisel verilerin korunma mevzuatı ile ilgili çalışmalar 2016 yılında tamamlanmış olduğundan, Türkiye Sözleşme'yi 1981 yılında imzalamış olmasına rağmen, 2016 yılında yürürlüğe girmiştir. Sözleşme'nin amacı gerekçe kısmında da belirtildiği üzere; üye ülkede yaşayan bütün gerçek kişilerin kişisel verilerin otomatik işlemeye tabi tutulması halinde özel hayatın gizliliği haklarını korumaktır. Bu yönüyle Sözleşme, devletlerin vatandaşlarını korumaya yönelik önemli bir araçtır¹¹⁷.

Gerekçe kısmında ifade edildiği üzere Sözleşme; kişisel verilerin korunması hakkını, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde yer alan özel hayatın korunması hakkından yola çıkarak düzenlemektedir. İçeriğine bakıldığında Sözleşme'nin, OECD Rehber İlkeleri'nden etkilendiği görülmektedir. Rehber İlkelerine benzer olarak Sözleşme'de de kişisel verilerin hukuka uygun olarak elde edilmesi, amacına uygun işlenmesi ve amacı doğrultusunda saklanması konularına yer verilmektedir¹¹⁸. Yine özel veri kategorileri de 108 Sayılı Sözleşme ile düzenlenmiş ırk, siyasi görüş, dini inanç, sağlık durumu, cinsel hayat ve ceza

¹¹⁶ Sözleşmenin tarihsel süreci ve uygulama alanı hakkında detaylı açıklamalar için: Songül Atak, "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", **Türkiye Barolar Birliği Dergisi**, Sayı:87, 2010, ss.91-92.

¹¹⁷ Gemicioğlu, s. 407.

¹¹⁸ Develioğlu, s.9. Ayrıca 108 Sayılı Sözleşme özel sektör, yargı, kolluk kuvvetleri, kamu kurumları tarafından toplanan ve işlenen bütün kişisel verileri kapsar. Kişisel verilerin kötüye kullanılması, yetkisiz veri toplama ve sınır dışına veri aktarımı konularını düzenler. Bu düzenlemelere ilişkin detaylı açıklamalar için: Tolun vd. s.35.

mahkumiyetleri ile ilgili verilerin otomatik işlemeye tabi tutulamayacağı hüküm altına alınmıştır.

Sözleşme ile Avrupa Konseyi'ne üye olmayan devletlerin de Bakanlar Komitesi tarafından Sözleşme'ye katılmaya davet edilebileceği düzenlenmiştir. Bu sayede kişisel verilerin özellikle sınır ötesi işleme durumlarında da kapsamlı olarak korunmasının önü açılmıştır¹¹⁹.

108 Sayılı Sözleşme'nin hazırlanmasında önemli rol oynayan Bakanlar Komitesi'nin kişisel veriler konusunda tavsiye kararları da mevcuttur. Bu kararlar bağlayıcı olmamakla birlikte, üye ülkelerin kişisel verilere yaklaşımını ve Sözleşme'nin uygulanmasını belirlemek açısından önemlidir. Komite'nin R(85) 20 Sayılı ve 25 Ekim 1985 tarihli kararında o dönemlerde hayatımıza giren ancak Sözleşme'de bu hususta bir düzenleme yer almayan doğrudan pazarlama konusuna değinilmiştir¹²⁰. Kararda doğrudan pazarlama; mal veya hizmetlerin sunulmasını veya iletilmesini mümkün kılan tüm faaliyetler olarak tanımlanmıştır. Doğrudan pazarlama için bir kişiden aldatıcı beyanlarla veri toplanmaması; bu amaçla kişisel veri dosyalarının derlenmesinde tüm uygun teknik önlemlerin alınması, verinin güvenliğini ve gizliliğini sağlamak için temel düzenlemelerin yapılması gerektiği vurgulanmıştır. Yine Komite'nin R(86) 1 Sayılı ve 23 Ocak 1986 tarihli kararında; sosyal güvenlik amacıyla kişisel verilerin korunmasında mahremiyet kavramına değinilmiştir¹²¹. Karara göre; sosyal güvenlik amacıyla kullanılan kişisel verilerin toplama, saklama, kullanım, transfer ve muhafazasında bireylerin mahremiyetine saygı garanti edilmelidir. Sosyal güvenlik amacıyla kişisel verilerin toplanması ve depolanması; ilgili sosyal güvenlik kurumlarının görevlerini yerine getirmesini sağlamak için gerekli olanlarla sınırlandırılmalıdır.

108 Sayılı Sözleşmede önemli bir eksikliği gidermek üzere 2001 yılında 181 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol imzaya açılmıştır. 181 Sayılı Ek Protokol ile veri işlemeyi

¹¹⁹ Aydın, s.41.

¹²⁰ Avrupa Konseyi Bakanlar Komitesi R(85) 20 Sayılı ve 25 Ekim 1985 tarihli kararı: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804bd336> (31.03.2021)

¹²¹ Avrupa Konseyi Bakanlar Komitesi R(86) 1 Sayılı ve 23 Ocak 1986 tarihli kararı: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804dd352> (31.03.2021)

denetleyecek bağımsız bir organ kurulmuştur. Yine 108 Sayılı Sözleşme’ye önemli bir düzenleme getirerek Avrupa Birliği’ne üye olmayan ülkelere veri transferinde, veri koruma konusunda etkili önlemler almayan üçüncü ülkelere transferi yasaklamıştır. 2018 yılında Türkiye tarafından da onaylanan Protokol, üye ülkelere 108 Sayılı Sözleşme’ye taraf olmayan bir ülke ile veri paylaşımı söz konusu olduğunda bu devletin yeterli düzeyde koruma vermesi taahhüdünü arama zorunluğu getirmiştir¹²².

C. 95/46/EC Sayılı Yönerge

Avrupa Birliği, 1990 yılında kişisel verilerin korunmasına yönelik bir taslak hazırlamıştır. 1995 yılında yürürlüğe giren taslak, 24 Ekim 1995 tarihli 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Bu Verilerin Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi olarak hayatımızda yerini almış ve kişisel verilerin korunmasıyla ilgili önemli ilkeleri kabul etmiştir¹²³. Yönerge yürürlüğe konmadan önce; zaten kişisel verilerin korunmasına son derece hassas yaklaşan Avrupa’da çoğu ülkede kişisel verilerin korunması kanunları bulunmaktaydı. Ayrıca bağlayıcı bir düzenleme olan 108 Sayılı Sözleşme de birçok Avrupa ülkesi tarafından onaylanmış ve devletlerin iç hukukunun bir parçası haline getirilmişti. Ancak; Avrupa’da kişisel verilerin korunması alanında belirli bir düzenin oturtulmuş olmasına rağmen, Avrupa Birliği bünyesinde yeni bir düzenlemeye ihtiyaç duyulmuştur. Yönerge’nin hazırlanmasında; kişisel verilerin ulusal mevzuatlarda farklı ele alınmasının, 7 Şubat 1992’de imzalanan Maastricht Antlaşması ile kurulması hedeflenen ekonomik ve parasal birlik yani ortak pazar açısından engel oluşturacağı düşüncesi başta gelmektedir. Bununla birlikte, üye ülkelerin veri koruma düzenlemeleri arasındaki farklılık ve çelişkilerin giderilmesi de Yönerge’nin ortaya çıkışındaki temel amacı oluşturur¹²⁴.

¹²² Aşıkoğlu (Büyük Veri), s. 43.

¹²³ Ayözger, s. 80.

¹²⁴ Yörük, s.40. Ayrıca; Maastricht Antlaşmasının ortaya çıkış süreci ve tarihsel gelişimi hususunda: Ekrem Yaşar Akçay, Çiğdem Argun, Elvettin Akman, “AB’nin Tarihsel Gelişimi ve Ortak Dış ve Güvenlik Politikası”, **Süleyman Demirel Üniversitesi Vizyoner Dergisi**, Cilt:3, Sayı:4, 2011, ss.117-131.

Kişisel verilerin korunması hususunda en etkili yöntem olarak kabul edilen 95/46/EC Sayılı Yönerge; yalnızca üye ülkelere yönelik olarak hazırlanmıştır. Bu nedenle Avrupa Birliği kurumları tarafından işlenen verilerin korunmasına yönelik kurallar için 45/2001 Sayılı Kişisel Verilerin Birlik Kurum ve Kuruluşları Tarafından İşlenmesine ve Bu Verilerin Serbest Dolaşımına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Tüzüğü de ayrıca kabul edilmiştir¹²⁵.

Yönerge'nin veri korumaya ilişkin hükümleri yalnızca gerçek kişiler için uygulanabilir. Ancak üye devletler, Yönerge'nin ilkeleri kapsamında tüzel kişilerin verilerinin korunması için iç hukuklarında düzenleme yapmakta serbesttirler. Yine Yönerge'nin veri koruma ilkelerine ilişkin hükümleri, kimliği belirli veya belirlenebilir bir gerçek kişi için geçerli olduğundan; anonim veriler bakımından Yönerge uygulanamayacaktır¹²⁶. Yönerge'nin kapsamı 3. madde içerisinde düzenlenmektedir. Buna göre; bir dosyalama sisteminin parçası olan kişisel verilerin otomatik araçlar dışında işlenmesi ile kısmen ya da tamamen otomatik araçlarla işlenmesi halinde 95/46/EC Sayılı Yönerge uygulanacaktır. Bunun yanı sıra; ceza hukuku alanındaki devlet faaliyetleri, devlet güvenliği, ülke savunması, kamu güvenliği ve Avrupa Birliği Antlaşması'nın V. ve VI. başlıklarıyla belirtilenler gibi Topluluk hukukunun kapsamı dışındaki faaliyetler ve gerçek kişiler tarafından tamamen kişisel veya ev içi faaliyetler esnasında işlenen kişisel veriler Yönerge'nin kapsamı dışında tutulmuştur.

Örneğin; bilgisayar veya kağıt üzerinde tutulan verilerin, veri sahiplerinin soyadı veya doğum tarihi sırasına göre sistematik bir şekilde gruplanması halinde, Yönerge çerçevesinde veri işleme faaliyeti söz konusu olacaktır. Ancak Yönerge'ye göre, bu verilerin gerçek kişiler tarafından, yalnızca kişisel kullanım amacıyla tutulması durumu Yönerge'nin uygulama alanı dışında kalmaktadır. Örneğin; herhangi bir gerçek kişinin, kendi yakınlarının iletişim bilgilerini kaydettiği bir telefon defteri Yönerge kapsamında değerlendirilmeyecektir¹²⁷.

Yönerge'nin düzenlediği şartlara göre; üye ülkelerin tamamının Yönerge'ye uyması bir zorunluluktur. Aksi halde, üye ülkenin yasal düzenlemeleri içinde kişisel verilerin korunmasına ilişkin yaptırımların olmaması halinde tam bir korunmanın da mümkün olmayacağı belirtilmiştir¹²⁸. Ayrıca Yönerge'nin amacı olarak kişisel veriler

¹²⁵ Develioğlu, s.10.

¹²⁶ Yakışır, s.48.

¹²⁷ Aksoy, s.101.

¹²⁸ Avcıoğlu, s.44.

işlenirken başta mahremiyet olmak üzere, gerçek kişilerin temel haklarının ve özgürlüklerinin korunacağı ifade edilmek suretiyle; kişisel verilerin korunması mevzuatının oluşturulurken mahremiyet hakkına verilen önem bir kez daha ortaya konmuştur. Bütünüyle bakıldığında Yönerge, 108 sayılı Sözleşme ve ulusal hukuklarda yer alan ilkeleri içermekte ve çoğunlukla bu ilkeleri detaylandırmaktadır. Yönerge’de temel olarak yer verilen ilkeler “meşruluk ve adillik”, “kişisel verilerin açık, belirli ve meşru amaçlar için toplanması”, “şeffaflık”, “orantılılık”, “güvenlik ve veri işlemenin denetime tabi olması” dır. Bunun yanı sıra Yönerge ve 108 sayılı Sözleşme arasında bir etkileşim de bulunmaktadır. Bu etkileşim, bu düzenlemeleri kişisel verilerin korunmasının gelişimine katkıda bulunmak bakımından olumlu yönde etkilemiştir¹²⁹.

Yönerge, her üye ülkenin kendi sınırları içinde Yönerge’ye uygun davrandığını kontrol amacıyla, bağımsız bir kamu mercisi oluşturmasını zorunlu kılmaktadır. Denetleme mercilerinin, veri koruma konularını araştırma, rehberlik sağlama, ulusal kanunların ihlal edildiği yargılamalara müdahil olma ve yargı erkinin dikkatini veri ihlaline çekme konularında geniş görevleri bulunmaktadır¹³⁰. Bunun yanı sıra, Yönerge’nin 29. maddesi ile “Kişisel Verilerin İşlenmesine Dair Bireylerin Korunması Hakkındaki Çalışma Grubu” ya da uygulamadaki adıyla “Madde 29 Çalışma Grubu” kurulmuştur. Bir danışma kurulu niteliği taşıyan Madde 29 Çalışma Grubu; Komisyon’un bir temsilcisi, Avrupa Birliği kurum ve kuruluşları için kurulan makamların birer temsilcisi ve her üye devlet tarafından atanan bir temsilciden oluşturulmuştur. Madde 29 Çalışma Grubuna; kişisel verilerin korunması hususunda alınan tedbirlerin uygulanmasına katkı sağlamak, Avrupa Birliği’ndeki ve üçüncü ülkelerdeki veri koruma konularında Komisyon’a görüş bildirmek, yine kişisel verilerin Avrupa Birliği’nde ve üçüncü ülkelerdeki korunma durumu hakkında yıllık rapor hazırlayıp halka duyurmak gibi görevler verilmiştir.

Günümüzde; Avrupa Birliği bünyesinde kişisel verileri koruyan 95/46/EC sayılı Yönerge yürürlükten kaldırılmış ve yerine 2016/679 sayılı Genel Veri Koruma Tüzüğü (General Data Protection Regulation- GDPR) yürürlüğe konmuştur.

¹²⁹ Dülger (GDPR Bağlamında Kişisel Veriler), s.79.

¹³⁰ Nurullah Tekin, “Kişisel Verilerin Korunması İle İlgili Türkiye’deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi”, **Uyuşmazlık Mahkemesi Dergisi**, Sayı:4, 2014, s.237.

2016/679 sayılı Tüzük, 94. maddesiyle Yönergeyi ilga etmiş ve 28 Mayıs 2018 tarihinden itibaren Yönerge'ye yapılan atıfların Genel Veri Koruma Tüzüğü'ne yapılmış sayılacağını hüküm altına almıştır. Bunun yanı sıra Madde 29 Çalışma Grubu'na yapılan atıfların da GDPR ile kurulan Avrupa Veri Koruma Kurumu'na yapılmış kabul edileceği belirtilmiştir¹³¹.

D. Temel Haklar Şartı

İkinci Dünya Savaşı'ndan sonra Avrupa'da barış ortamını sağlamak, Avrupa ülkeleri arasında birlik ve beraberliği sağlamak üzere kurulan Avrupa Ekonomik Topluluğu, sınırlar olmadan ortak pazar sistemini hayata geçirmiştir. İkinci Dünya Savaşı sonrasında savaşın yarattığı ekonomik buhrandan kurtulmayı hedefleyerek kurulan Topluluk, ortak pazarı ortak para birimi ile işlevselleştirme amacı gütmüştür. Topluluk içindeki birlik ve bütünleşme hareketlerinin ilerlemesi sonucu amaç; yalnızca sınırlar olmadan ekonomiyi sürdürmek ve ticari kalkınmak olmaktan çıkmış ve Birlik bugünkü halini alarak siyasi bir bütünleşme de olmuştur. Bu siyasi bütünleşme yolunda en önemli adımlardan biri de Avrupa Birliği Temel Haklar Şartı'dır.

“Temel Haklar Şartı, temel hakları daha anlaşılır bir şekilde formüle etme ve temel haklara daha seçkin bir yer verme imkanı sunmaktadır. Temel Haklar Şartı'nın kabulü, Avrupa Birliği'nin meşruiyetini güçlendirmekte, temel hakları Birlik vatandaşları için "görünür kılmakta" ve korumanın düzeyini yükseltmektedir”¹³². Temel Haklar Şartı'nın doktrinde adlandırılan en önemli özelliği Avrupa Birliği'nin “Anayasası” niteliğinde olmasıdır¹³³. Bu düşünceler ışığında hazırlanan Şart, 7

¹³¹ Ayrıca bu hususta bkz: Başar, s.194, 206.

¹³² Yüksel Metin, “Avrupa Birliği Temel Haklar Şartı”, **Ankara Üniversitesi Siyasal Bilimler Fakültesi Dergisi**, Cilt:57, Sayı:4, 2001, s.36. Ayrıca Temel Haklar Şartı'nın ayrıntılı değerlendirmesi için: Bahar Yeşim Deniz, “Avrupa Birliği Hukukunda Temel Haklar ve Avrupa İnsan Hakları Sözleşmesi ile Etkileşim”, **Türkiye Barolar Birliği Dergisi**, Sayı:97, 2011, ss.49-74.

¹³³ Temel Haklar Şartı'nın Avrupa Birliği'nin Anayasası olarak kabul edilebileceği yönündeki detaylı açıklamalar ve görüşler için: Işıl Karakaş, “Ulusalüstü Anayasada Temel Haklar Problematiği: Teorik ve Pratik Sorunlar”, **Anayasa Yargısı Dergisi**, Cilt:21, Sayı:1, 2005, ss.31-38.

Aralık 2000 tarihinde Fransa'nın Nice şehrinde Avrupa Parlamentosu, Konsey ve Komisyon tarafından imzalanmıştır¹³⁴.

Kişisel verilerin korunmasına yönelik düzenlemeler Temel Haklar Şartı'nın 8. maddesinde yer almaktadır. Buna göre; *“Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. Bu veriler; adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir.”* denilmektedir. Bununla birlikte doktrinde Şart'ın 7. maddesi olan özel hayata ve aile hayatına saygı düzenlemesini de kişisel verilerin korunması kapsamında gören görüşler mevcuttur¹³⁵.

Lizbon Anlaşması, Temel Haklar Şartı'nı bağlayıcı kılmış ve 8. maddede yer alan kişisel verilerin korunması hakkını anayasal düzeyde bir temel hak olarak belirlemiştir. 108 Sayılı Sözleşme ve 95/46/EC Sayılı Yönerge de ise kişisel verilerin korunması, mevcut temel hakların bir parçası olarak ele alınmıştır¹³⁶. Kişisel verilerin ayrı bir maddede düzenlenerek özel hayat kapsamından ayrılması da oldukça önemlidir. Bu sayede kişisel verilerin korunması hakkı, insan hakları ile temel hak ve özgürlükler kapsamında değerlendirilmesinin yanında; özel hayatın gizliliğinden de ayrılarak başlı başına bir hak olarak koruma altına alınmıştır. Tüm bunların yanı sıra Temel Haklar Şartı'nda herkesin kendisi hakkındaki kişisel verilere erişim ve bu verilerini düzelttirme hakkına sahip olduğunun ifade edilmesi Avrupa İnsan Hakları Mahkemesi'nin özel hayatın gizliliği hakkına dayanarak verdiği kararlarında tam olarak çözemediği bazı hukuksal sorunları çözmeye olanağı ortaya çıkmıştır¹³⁷.

¹³⁴ 2000/C 364/01 Sayılı Temel Haklar Şartı:

https://sbb.gov.tr/wpcontent/uploads/2018/11/Avrupa_Birligi_Temel_Haklar_Sarti%E2%80%8B.pdf (06.04.2021)

¹³⁵ Özel hayata ve aile hayatına saygı ve kişisel verilerin korunması düzenlemelerini birlikte değerlendiren görüş için: Fuster, s.199.

¹³⁶ Sezen Kama Işık, **Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış**, On İki Levha Yayıncılık, İstanbul, 2020, s.111.

¹³⁷ Küzeci, s.162.

E. 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü

2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nü, 95/46/EC Sayılı Yönerge'nin güncellenmiş hali olarak kabul etmek mümkündür. Zira Yönerge, kişisel verilerin korunması hukukuna büyük katkı sağlamış ve Türkiye dahil birçok ülkenin kişisel verilerin korunması hususunda hazırladıkları mevzuatlara kaynak olmuştur. Ancak hızla gelişen teknoloji ve çağın değişen gereklilikleri; kişisel veriler gibi güncel teknolojiye bağlı olarak ilerleyen bir alanda da yenilik yapılma gereğini doğurmuştur. Bu süreç içerisinde önemini koruyan Yönerge, kişisel verilere ilişkin temel ilkelerin oluşmasında öncü rol üstlenmiştir. Öyle ki, bu temel ilkeler, hâlâ hem ülkemizin hem de diğer ülkelerin kişisel veri mevzuatlarında dikkate alınmaktadır¹³⁸.

Yönerge'nin en büyük amacı; ulusal veri mevzuatlarındaki farklılıkların giderilmesi ve Avrupa Birliği içinde yeknesaklığın sağlanması olmasına rağmen, Yönerge bu amacı tam anlamıyla yerine getirememiştir. Bunun nedeni ise; Avrupa Birliği'nde yönergelerin uygulanmasının ancak üye devletlerin yönergeyi iç hukuklarına aktarması halinde mümkün olmasıdır. Bu da; her üye devletin yönerge ile ilgili temel prensip olarak aynı, ancak içerik olarak farklı düzenlemeler kabul etmesine neden olmuştur. Tüm bunlar sonucunda 95/46/EC Sayılı Yönerge, Avrupa Birliği'nde kişisel verilerin korunması alanında yeknesaklığı sağlayamamış; hatta her bir ülkenin ayrı ayrı olmak üzere 28 adet farklı kişisel verilerin korunması mevzuatı ortaya çıkmasına neden olmuştur¹³⁹. Bu farklılıkları ortadan kaldırıp Avrupa Birliği içinde kişisel verilerin korunmasını bir bütünlüğe kavuşturmak ve gelişen teknoloji ile birlikte artan veri işleme yollarına karşı korumayı arttırmak için 2012 yılında bir tüzük çalışması başlamıştır. Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu'nun birlikte hazırladığı tüzük 2016 yılında kabul edilmiş ve 25 Mayıs 2018 tarihinde yürürlüğe girmiştir¹⁴⁰.

GDPR'nin ilk maddesinde konusu ve amacı yer almaktadır. Buna göre; 2016/679 sayılı Tüzük'ün konusu, gerçek kişilerin kişisel verilerinin işlenmesi ve

¹³⁸ Özkan, s.59.

¹³⁹ Develioğlu, s.12. Ayrıca GDPR'nin ortaya çıkış süreci ve tarihsel gelişimi için: The History of the General Data Protection Regulation, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (11.04.2021)

¹⁴⁰ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, KVKK Yayınları, Ankara, 2019, s.19.

korunması hususunda kurallar olarak hüküm altına alınmıştır. Ayrıca kişisel verilerin serbest dolaşımına ilişkin kuralların da GDPR kapsamında olduğu bu maddede belirtilmiştir. GDPR'nin amacı ise; gerçek kişilerin temel hakları ve özgürlüklerini, özellikle de kişisel verilerin korunması hakkını koruma altına almaktır. Kişisel verilerin Avrupa Birliği içerisindeki serbest dolaşımının, veri koruması sebebiyle kısıtlanamayacağı da GDPR'nin hedefi kapsamında ifade edilmiştir.

GDPR'nin maddi kapsamını düzenleyen 2. maddesine göre, Tüzük kişisel verilerin tamamen veya kısmen otomatik araçlarla ya da dosyalama sisteminin bir parçası olması hedeflenen araçlarla işlenmesinde uygulanacaktır. Maddi kapsam çerçevesinde GDPR'nin uygulanamayacağı haller ise Avrupa Birliği hukuku kapsamına girmeyen bir faaliyetler, Avrupa Birliği'ne üye devletler tarafından Avrupa Birliği Antlaşması'nın 5. Başlığının 2. Bölümü kapsamına giren faaliyetler gerçekleştirilirken¹⁴¹, tamamen kişisel veya ev faaliyeti esnasında bir gerçek kişi tarafından gerçekleştirilen işlemler ve kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkin makamlar tarafından kişisel verilerin işlenmesine ilişkin faaliyetlerdir.

GDPR; Yönerge'ye göre daha geniş bir uygulama alanına sahip olmuştur. Bu bağlamda GDPR, Avrupa Birliği'ne üye ülkeler ve kuruluşların yanı sıra; Avrupa Birliği'ne üye olmayan; ancak Birlik vatandaşlarına mal ve hizmet sunan veri işleyicilerine de uygulanacaktır. Örneğin, Avrupa Birliği içerisinde erişimin mümkün olduğu ve Avrupa Birliği vatandaşlarına ürün satan Seattle/ABD merkezli Amazon.com internet sitesi de GDPR'nin uygulama alanı içerisindedir. Bunun gibi Avrupa Birliği içerisindeki veri sahiplerinin internetteki arama tercihlerini izleyen Google arama motoruna da GDPR hükümleri uygulanacaktır. Bu kuruluşlar hakkında GDPR'nin uygulanması ise ancak bir uyumsuzluk meydana geldiğinde mümkün olacaktır¹⁴².

¹⁴¹ Avrupa Birliği Antlaşması'nın 5. Başlığı; Birliğin Dış Eylemine İlişkin Genel Hükümler ve Ortak Dış ve Güvenlik Politikasına İlişkin Özel Hükümler olup bu başlığın 2. bölümünde Ortak Dış ve Güvenlik Politikasına İlişkin Özel Hükümler yer almaktadır. <https://ab.gov.tr/files/pub/antlasmalar.pdf> (15.04.2021)

¹⁴² Taştan, s.18.

II. KİŞİSEL VERİLERİN İŞLENMESİNDE TARAFLARIN HAKLARI VE YÜKÜMLÜLÜKLERİ

Avrupa Birliği'nde kişisel verilerin korunmasına verilen önem GDPR'nin ortaya çıkış sürecinde etkili olmuştur. GDPR de kişisel verilerin korunmasını etkin bir şekilde sağlamak için veri sahibine bir takım haklar tanırken, veri sorumlusuna da bazı yükümlülükler getirmiştir.

A. Veri Sahibinin Hakları

GDPR'nin 12. ve 22. maddeleri arasında veri sahibinin haklarına yer verilmiştir. GDPR kapsamında veri sahibinin haklarının yer alması, kişisel verilerin işlenmesi faaliyetlerinin sınırlarını belirlemek ve veri sorumlusunun yerine getirmesi gereken yükümlülüklerin anlaşılması açısından büyük önem taşımaktadır¹⁴³.

1. Bilgi Alma Hakkı

GDPR, kişisel verileri işlenen veri sahibine yapılan bilgilendirme hakkını verinin veri sahibinden elde edilmesi ve başka bir üçüncü kişiden elde edilmesi hali olarak iki ayrı maddede düzenlemiştir. Düzenleme iki ayrı maddede yapılmış olmasına rağmen veri sahibine tanınan haklar ortaktır. İşlemeye konu olacak verinin, veri sahibinden elde edilmesi halinde veri sahibi verinin elde edileceği anda bilgilendirilebilecekken, üçüncü bir kişiden veri elde edilmesi durumunda veri sahibinin sonradan bilgilendirilmesi söz konusu olacaktır.

Veri sorumlusu işleme faaliyeti ile ilgili her türlü bilgiyi, veri sahibine şeffaf ve anlaşılır bir biçimde, açık ve yalın bir dil kullanarak açıklamak için gereken tüm işlemleri yapar. Bilgilendirme yazılı olarak, elektronik yollarla veya mümkün olan diğer tüm yöntemlerle yapılabilir. Bilgilendirme veri sahibi tarafından talep edildiği takdirde, veri sahibinin kimliğini doğrulamak kaydıyla sözlü olarak da yapılabilir. Bir veri sahibinden kişisel verileri toplanırken aynı anda veri sorumlusunun ve temsilcisinin kimlik ve irtibat bilgileri, veri koruma görevlisinin irtibat bilgileri,

¹⁴³ Tolun vd., s.113.

kişisel verilerin planlanan işleme amaçlarının yanı sıra işleme faaliyetinin yasal dayanağı, veri sorumlusu tarafından gözetilen meşru menfaatler, kişisel veriler başka alıcılar ile paylaşılacaksa bu alıcılar veya alıcı kategorileri, veri sorumlusundan kişisel verilere erişim ve kişisel verilerin düzeltilmesi, silinmesini veya veri sahibi ile ilgili işleme faaliyetinin kısıtlanmasını talep etme, işleme faaliyetine itiraz etme, verilerin taşınabilirliği hakkının varlığı, işleme faaliyetinin rızaya dayalı olarak gerçekleştirilmesi halinde, herhangi bir zamanda rızayı geri çekme hakkının varlığı, bir denetim makamına şikayette bulunma hakkı bilgilerin de veri sahibi ile paylaşılması gerekmektedir.

Veri sahibinin işlemeye dair bilgilendirilmesi asıl ve temel kural olmakla birlikte GDPR’de sayılan bazı hallerde bilgilendirme yapılmayabilir. Buna göre; veri sahibinin zaten bilgisinin olması, kamu yararına arşivleme, bilimsel veya tarihi araştırma amaçları ve istatistiki amaçlar ile veri işleme, veri sahibine bilgi vermenin imkansız olması veya ölçüsüz bir çaba gerektirmesi, elde etme veya açıklamanın veri sorumlusunun tabi olduğu üye devlet veya Avrupa Birliği hukukunda açık bir şekilde ortaya konması, kişisel verilerin Avrupa Birliği veya üye devlet hukuku ile düzenlenen bir mesleki gizlilik yükümlülüğüne tabi olarak gizli kalmasının gerekmesi hallerinde veri sahibine bilgi verilmeyebilir.¹⁴⁴

Veri sahibinin bilgi alma hakkının, işlemenin her anında sahip olduğu önemin yanı sıra işlemenin rızaya dayandığı hallerde ayrı bir yeri vardır. Zira işleme faaliyetinin gerçekleşmesi için veri sahibinin açık rızası alınması gerekiyorsa, açık rızanın geçerli olmasının şartı veri sahibinin rıza verdiği işleme konusuna ilişkin açık bir şekilde bilgilendirilmesidir¹⁴⁵.

Bilgi alma hakkının önemini ortaya koyan kararlardan biri ABAD’ın 1 Ekim 2015 tarihli ve C-201/14 sayılı Smaranda Bara ve diğerleri ile Agenția Națională de Administrare Fiscală (Ulusal Mali İdare Ajansı) ve diğerleri kararıdır. Karara konu olayda serbest meslek erbabı olan başvuruçuların Ulusal Mali İdare Ajansı’na beyan

¹⁴⁴ “Burada belirtilmesi gereken husus, hesap verilebilirlik ilkesi uyarınca veri sorumlusunun gerekli bilgileri imkânsız olması ya da ölçüsüz çaba gerektirmesi gerekçesiyle sunmaktan kaçındığı hâllerde bir denge testi yapması gerekliliğidir. Özellikle veri işleme faaliyetinin ilgili kişi bakımından sonuç ve etkileri büyük önem arz etmektedir. Veri sorumlusu söz konusu işleme faaliyetinin ilgili kişinin temel hak ve özgürlükleri ile menfaatlerini koruyan uygun tedbirleri aldığını ortaya koyabilmeli; kendisine ait bir internet sitesi ya da medya aracılığı ile kamuya açık bir bilgilendirme sunmalıdır”. Aşkoğlu (Aydınlatma Yükümlülüğü), s. 59.

¹⁴⁵ Rızaya dayalı işleme faaliyetlerinde veri sahibinin bilgilendirilmesi hususunda ayrıntılı bilgi için: Başar, s.56.

ettikleri geliri Ajans, başvuruculara bilgi vermeden Ulusal Sağlık Sigortası Fonu'na bildirmiştir. Ulusal Sağlık Sigorta Fonu'nun kendilerine prim borcuna ilişkin bildirim göndermesi üzerine durumdan haberdar olan başvurucular konuyu yargıya taşımıştır. Bunun üzerine ABAD, veri sorumlusu veya temsilcisinin veri sahibinden hangi verileri toplandığı, veri denetleyicisinin kimliği, işlemenin amaçları ve verilerin adil bir şekilde işlenmesini garanti etmek için gerekli olan diğer tüm bilgileri vermekle yükümlü olduğuna karar vermiştir¹⁴⁶.

2. Erişim Hakkı

Bilgi edinme hakkı gibi dürüstlük ve şeffaflık ile sıkı ilişkisi olan erişim hakkı, veri sahibinin bilgi alması hakkını tamamlayarak, veri sahiplerinin kişisel verileri üzerindeki haklarını kullanabilmesi için, kişisel verilerinin nasıl ve ne şekilde işlendiğini öğrenmesine imkan tanımaktadır. Ancak bu hakkın kapsamı geniş tutulmamalı ve başkalarının hak ve özgürlüklerine müdahale niteliği taşınamalıdır¹⁴⁷. GDPR'nin 15. maddesinde düzenlenen bu hak kapsamında veri sahibi kendisi ile ilgili kişisel verilerin işlenip işlenmediğini veri sorumlusundan teyit etme, işlemeye tabi kişisel verilerinin işlenme amaçları, kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri, kişisel verilerin saklanması açısından öngörülen süre, bu sürenin belirlenmesi amacı ile kullanılan kriterler, kişisel verilerin veri sahibinden elde edilmemesi halinde bu verilerin kaynaklarına ilişkin mevcut bilgiler, söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları hakkındaki bilgilere erişme hakkına sahiptir. Zira veri sahibi, kişisel verilerinin işlenmesine ilişkin bilgilere erişemiyorsa, kişisel verilerin korunduğu kabul etmek de mümkün değildir¹⁴⁸.

Veri sorumlusu işlenen kişisel verilerin bir örneğini veri sahibine sağlar. Veri sahibi tarafından talep edilen diğer örnekler açısından, veri sorumlusu idari masraflara dayalı olarak makul bir ücret talep edebilir. Veri sorumlusunun ücret

¹⁴⁶ ABAD'ın 1 Ekim 2015 tarihli ve C-201/14 sayılı Smaranda Bara ve diğerleri ile Agenția Națională de Administrare Fiscală (Ulusal Mali İdare Ajansı) ve diğerleri kararı için: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=168943&pageIndex=0&doclang=E N&mode=lst&dir=&occ=first&part=1&cid=10950936> (24.04.2021)

¹⁴⁷ Develioğlu, s.88. Yörük, s.75.

¹⁴⁸ Şimşek, s.88'den aktaran Bozkurt s.123.

talebi hususunda ABAD'ın 12 Aralık 2013 tarihli ve C-486/12 sayılı kararında, başvuru bir trafik suçu nedeniyle hükmedilen para cezasının adresine hiç tebliğ edilmediğini göstermek için belediyeden kendisine ilişkin tutulan verilerin bir örneğini istemesi üzere, belediyenin başvurucudan ücret talep etmesi karşısında başvuru konuyu yargıya taşımıştır¹⁴⁹. Bunun üzerine ABAD, veri sorumlusunun ücret talep edebileceğine ancak bu ücretin cüzi bir miktar olmasına, veri sahibinin erişim hakkını kısıtlayacak bir boyutta olmamasına karar vermiştir.

3. Düzeltme Hakkı

GDPR'nin 16.maddesinde düzenlenen düzeltme hakkına göre, veri sahibinin kendisi ile ilgili doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin düzeltilmesini veri sorumlusundan talep etme hakkı bulunur. Bunun yanı sıra veri sahibinin eksik kişisel verileri tamamlama hakkı da vardır. Bu hak aynı zamanda kişisel verilerin doğru ve güncel olmasını kapsayan doğruluk ilkesinin ve veri öznelerinin kişisel verilerinin geleceğini belirleme haklarının da bir gereğidir¹⁵⁰. Bu nedenle haklı bir düzeltme talebini yerine getirmeyen veri sorumlusunun, bu andan itibaren veri işleme doğruluk ilkesine aykırılık teşkil edeceğinden hukuka aykırıdır.

Veri sahibinin düzeltme talebi bir şekle tabi değildir. Bu nedenle talep, düzeltme talebi adı altında gelmiş olmasa bile içerik itibarıyla kişisel verilerin düzeltilmesini konu ediniyorsa, düzeltme hakkı kapsamında ele alınmalıdır. Veri sahibinin yalnızca kendisi ile ilgili verileri düzeltirebilmesini ele alan bu hak kapsamında, bir verinin birden çok kişiyi ilgilendirdiği hallerde de, veri sahibinin bu verinin düzeltilmesini talep etmesinin mümkün olduğu düşünülmektedir¹⁵¹.

GDPR'nin 19. maddesi yapılan bir düzeltmenin üçüncü kişiler bakımından sonucunu da ortaya koymaktadır. Buna göre, veri sorumlusu kişisel verilerin düzeltilmesi işlemini, bu durum imkânsız veya aşırı bir çabayı gerektirir olmadıkça, kişisel verilerin açıklanmış olduğu tüm alıcılara bildirmekle yükümlüdür.

¹⁴⁹ ABAD'ın 12 Aralık 2013 tarihli ve C-486/12 sayılı kararı için:

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=145533&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5350641> (24.04.2021)

¹⁵⁰ Yörük, s. 77.

¹⁵¹ Bu hususta bakınız: Çekin, s.126.

4. Silinmeyi Talep Etme Hakkı

Madde başlığında “unutulma hakkı” olarak da ifade edilen bu hak GDPR’nin 17. maddesinde düzenlenmiştir. Buna göre veri sahibinin kendisi ile ilgili kişisel verilerin herhangi bir gecikmeye mahal verilmeksizin silinmesini veri sorumlusundan talep etme hakkı bulunmaktadır. Bununla birlikte; kişisel verilerin toplanma veya işleme amaçlarıyla ilişkili olarak artık gerekli olmaması, veri sahibinin rızası ile yapılan işleme faaliyetinde iznin geri çekilmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması, veri sahibinin işleme faaliyetine itirazda bulunması, işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması, kişisel verilerin yasa dışı biçimde işlenmiş olması veya veri sorumlusunun tabi olduğu üye devlet veya Avrupa Birliği hukukundaki bir yasal yükümlülüğe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması hallerinde veri sorumlusunun kişisel verileri derhal silme yükümlülüğü vardır.

Doktrinde unutulma hakkına ilişkin farklı tanımlamalar yapılmıştır. Bu tanımlara göre unutulma hakkı, dijital hafızada yer alan bireylere ait rahatsız edici içeriğin, bireylerin talebi üzerine bir daha geri gelmeyecek şekilde ortadan kaldırılması veya silinmesi¹⁵², kişilerin internet üzerindeki haklarında yer alan rahatsız edici içeriklerin veya sahibi oldukları kişisel verilerin silinmesi ve daha fazla yayılmasının önlenmesi¹⁵³, veri sahibinin sosyal medyada kendisi hakkındaki kişisel bir veriyi tamamıyla kontrol etmesi ve bu verileri dilediğinde tamamen sildirebilmesi¹⁵⁴, veri sahibinin üçüncü kişilerin bilmesini istemediği internet ortamında yer alan bilgilerinin silinmesi suretiyle dijital dünyada unutulmayı istemesi¹⁵⁵ olarak ifade edilmektedir.

Kişisel verilerin korunması hakkının veri öznesine tanıdığı haklar arasında yer alan, bireyin kişisel verilerine yönelik sildirme hakkının tek başına yaşamı mahrem kılmaya yetmemesi gündeme gelebilmektedir. Zira bireyin her türlü

¹⁵² Serdar Güleler, “Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak 'Unutulma Hakkı'”, **Türkiye Barolar Birliği Dergisi**, Sayı: 102, 2012, s. 226.

¹⁵³ Şebnem Ahi, “Kişilere Kişisel Verileri Üzerinde Kontrol Yetkisi Veren Hak” **Aylık Bilişim Kültür Dergisi**, Ocak 2014, <http://www.bilisimdergisi.org.tr/bilisim-dergisi-sayilari/s161.pdf> (27.04.2021), s. 98.

¹⁵⁴ Allyson Haynes Stuart, “Google Search Results: Buried If Not Forgotten”, **North Carolina Journal Of Law & Technology**, Cilt:15, 2014, s. 463.

¹⁵⁵ Aydın Akgül, “Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı”, **Türkiye Barolar Birliği Dergisi**, Sayı: 116, 2016, s.17.

bilgisinin, sınırsız biçimde kayıt altına alınması ve kayıtlı bilgilerin geniş bir ağla paylaşılması nedeniyle ortadan kaldırılması da oldukça zordur. Bu nedenle, bireyin üçüncü kişilerin gözetiminden kurtulma ve özgür biçimde yaşama isteği unutulma hakkına olan ihtiyacı ortaya çıkarmaktadır¹⁵⁶. Kişisel verilerin korunması hukukunda unutulma hakkının Avrupa Birliği mevzuatında yer alması GDPR'nin yürürlüğe girmesiyle olmuştur. GDPR'den önce 95/46/EC sayılı Yönerge'nin 12. maddesinde erişim hakkı başlığı altında "Özellikle verinin eksik veya yanlış yapısı yüzünden bu Yönerge'nin hükümlerine uymayan işlemede, verilerin engellenmesi veya silinmesi, uygun olarak düzeltilmesi" şeklinde verilerin silinmesine yer verilmekle yetinilmiş, unutulma hakkından bahsedilmemiştir. Kişisel verilerin korunmasını temel haklar ve özgürlükler boyutuyla incelerken unutulma hakkı boyutunda ele aldığımız "Costeja González- Google" kararı ile birlikte unutulma hakkının kişisel veri mevzuatlarında yer alması gerektiği ortaya konmuştur¹⁵⁷. Bu karar, unutulma hakkını ilk kez hukuksal bir temelde ele alan ve unutulma hakkına yer veren ilk içtihat olması yönüyle önemlidir¹⁵⁸.

Avrupa Veri Koruma Kurulu tarafından "Costeja González- Google" kararının uygulanmasına yönelik bir rehber de yayımlanmıştır. Bu rehberde ağırlıklı olarak unutulma hakkıyla ilgili inceleme yapılırken, sonucu belirlemede faydalanılacak kıstaslara yer verilmiştir. Buna göre unutulma hakkı ile ilgili değerlendirme yapan kurumların bu hakka yönelik bir karar vermeden önce arama sonuçlarının bir gerçek kişiye ait olup olmadığının tespitini yapmaları vurgulanmıştır. Bu tespitin yanı sıra veri sahibinin çocuk olup olmadığı, kamuya mal olmuş bir kişi olup olmadığı, sonuçlarda hassas verilerin bulunup bulunmadığı, sonuçlarda yer alan verilerin ilgili kişiye yönelik bir önyargıya sebebiyet verip veremeyeceği, içeriğin orijinalinin basın hakları çerçevesinde yayınlanıp yayınlanmadığı gibi kriterlerin değerlendirilmesinin önemli olduğu belirtilmiştir¹⁵⁹. GDPR'nin yürürlüğe girmesiyle birlikte unutulma hakkının kapsamı belirlenirken

¹⁵⁶Akgül, s.15.

¹⁵⁷ Unutulma hakkının ortaya çıkış süreci ve Costeja González- Google kararının detaylı incelemesi için bakınız: Emine Hizarci, **6698 Sayılı Kişisel Verilerin Korunması Kanununun AB Veri Koruma Hukuku Işığında Değerlendirilmesi**, Yetkin Yayınları, Ankara, 2020, ss. 70-74.

¹⁵⁸ Hasan Elmalıca, "Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:65, Sayı:4, 2016, s. 1613.

¹⁵⁹ Gizem Öz Demetoğlu, **Türk ve Avrupa Birliği Veri Koruma Hukuku Bağlamında Blok Zincir Teknolojisinde Unutulma Hakkı**, (Yayımlanmamış Yüksek Lisans Tezi), Marmara Üniversitesi Avrupa Birliği Enstitüsü, İstanbul, 2019, s.67.

“Costeja González- Google” kararı da unutulma hakkı kapsamında yol gösterici niteliktedir.

Buna göre bireyin, şahsına ilişkin olup hukuka ve dürüstlük kuralına uygun bir biçimde işlenmeyen, belirli, açık, ölçülü ve meşru amaçlarla toplanmayan, bu amaçlarla toplanmasına rağmen bu amaçlarla bağdaşmayacak şekilde işlenen ve kullanılan, doğru ve güncel olarak tutulmayan kişisel verilerin unutulmasını talep etme konusunda menfaati vardır. Ancak kişinin kişisel verilerinin dijital ortamlarda tutulmasına rızası olmasa bile sayılan şartları sağlamayan ve kamunun haber alma hakkı başta olmak üzere diğer temel hak ve özgürlüklerin kişisel verilerin korunması hakkı karşısında ağır bastığı durumlarda unutulmak mümkün olmayacaktır¹⁶⁰.

Toplumsal hayatta gitgide artan önemi dolayısıyla daha çok başvuruya konu olma yolunda ilerleyen unutulma hakkı kapsamında Belçika Denetim Makamı, bir Belçika vatandaşının unutulma hakkına saygı göstermediği gerekçesiyle Google Belçika’ya 14 Temmuz 2020 tarihinde 600.000 Euro para cezasına hükmetmiştir. Belçika Denetim Makamı’nın bu tarihe dek uyguladığı en yüksek miktardaki cezaya konu olan olayda başvurucu, hakkında olumsuz bilgiler içeren bağlantıların kaldırılması için Google Belçika’ya başvuru yapmış ve bu başvurusu reddedilmiştir. Belçika Denetim Makamı’na taşınan olayda başvurucunun başvurusu bazı içerikler yönünden, başvurucunun siyasi hayatta etkin olması ve bu nedenle kamu yararı için gerekli olması nedeniyle reddedilirken, geri kalan içerikler yönünden güncel olmayan, asılsız ve başvurucunun itibarına ciddi şekilde zarar verebilecek bilgiler içermesi nedeniyle kabul edilmiştir¹⁶¹.

5. İşlemenin Kısıtlanması Hakkı

GDPR’nin 18. maddesine göre veri sahibi, kişisel verilerin doğruluğuna itiraz ettiği takdirde veri sorumlusunun kişisel verilerin doğruluğunu teyit etmeye yetecek süre boyunca işleme faaliyeti kısıtlanır. Örneğin, çalışan işverene işe giriş tarihinin yanlış işlendiğini, bu nedenle bu veri üzerindeki işlemenin kısıtlanmasını ve bu kısıtlamanın sosyal güvenlik kurumuna bildirilmesini talep ederse, işveren işçinin işe

¹⁶⁰ Elmalica, s.1631.

¹⁶¹ Belçika Denetim Makamı’nın 14 Temmuz 2020 tarih ve 37/2020 sayılı kararının orijinal metni için bakınız : <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-372020.pdf> (28.04.2021)

giriş tarihini düzeltene kadar bu verinin işlenmesini kısıtlar¹⁶². GDPR'nin tanımlar kısmında işleme kısıtlaması, "saklanan kişisel verilerin gelecekte işlenmelerinin sınırlandırılması amacı ile işaretlenmesi" olarak tanımlanmıştır. Bu tanımları örneğe uyarlayacak olursak, işveren verinin doğruluğunu teyit edene kadar bu bilgiyi işaretler ve işlenmesini sınırlar.

18. maddede veri kısıtlaması için sayılan diğer sebepler işleme faaliyetinin yasa dışı olduğu hallerde veri sahibinin kişisel verilerin silinmesine itiraz ederek silinme yerine verilerin kullanımının kısıtlanmasını talep etmesi, veri sorumlusunun işleme amaçlarına yönelik olarak artık kişisel verilere ihtiyaç duymaması ancak veri sahibinin yasal iddialarda bulunulması ve bu iddiaların savunulması amacıyla söz konusu verilere ihtiyaç duyması, veri sorumlusunun yasal işleme gerekçelerinin veri sahibinin yasal gerekçelerine ağır basıp basmadığı doğrulanana kadar veri sahibinin işleme faaliyetine itiraz etmesi halleri olarak sayılmıştır. İşleme faaliyetinin kısıtlanmasını sağlayan bir veri sahibi, işleme faaliyetine ilişkin kısıtlama kaldırılmadan önce, veri sorumlusu tarafından bilgilendirilir.

6. Bildirimde Bulunulmasını Talep Hakkı

Veri sahibi GDPR'nin 19. maddesine göre, kendisine ait her türlü kişisel verinin düzeltme, silme ya da kısıtlama işleminin kişisel verilerin açıklandığı her alıcıya bildirilmesini veri sorumlusundan talep etme hakkına sahiptir. Ancak bu hakkın kullanılabilmesi için bildirim işleminin imkansız olmaması veya orantısız bir çabayı gerektirmemesi gerekmektedir. Bu bildirimin amacı, olası iyi niyet iddialarını ortadan kaldırmak olabileceği gibi, eski hale getirmeyi sağlamak da olabilir¹⁶³.

Bu hakkın kullanılmasının zorluğuna yönelik doktrinde eleştiriler de mevcuttur. Çekin'e göre, günümüz teknolojik koşulları göz önünde bulundurulduğunda kişisel veriler birçok arama motoru tarafından işlenmekte ve böylece herkesin erişimine açık hale gelmektedir. Herkesin ulaşabileceği bir verinin de tam olarak kim veya kimler tarafından işlendiğini tespit etmek de imkansızdır. Bu nedenle veri sorumlusunun, veri sahibinin bu hakkı kapsamında kimleri, nasıl bilgilendireceği cevaplanması gereken bir sorudur. Bu noktada veri

¹⁶² Develioğlu, s.94.

¹⁶³ Oğuz, s.28.

sorumlusunun yapabileceği de söz konusu veriyi işleyen herkesi teker teker bilgilendirmek değil, elindeki teknolojik imkanları kullanarak en makul çözümü sağlamaktır¹⁶⁴.

7. Veri Taşınabilirliği Hakkı

Veri taşınabilirliği hakkı, GDPR ile birlikte veri sahiplerine tanınmış olup daha önce hiçbir belgede düzenlenmemiş bir haktır¹⁶⁵. GDPR'nin 20. maddesinde yer alan bu hakka göre veri sahibinin kişisel verileri yapılandırılmış ve yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı bulunur. Bu hak kapsamında veri sahibi, veri sorumlusunun bir engeli olmaksızın verilerini aldığı formatı başka bir veri sorumlusuna iletebilir. Teknik açıdan mümkün olması halinde, veri sahibinin kişisel verilerin doğrudan bir veri sorumlusundan diğerine ilettirme hakkı da bu kapsamdadır. Doktrinde, hakkın veri sahibine verileri üzerinde tanıdığı iletim hakkının dikkatli kullanılması yönünde görüşler mevcuttur. Aksi halde bu hak sayesinde veri sahibi, verilerini olması gerekenden çok işleyici ile paylaşarak hakkın özüne ters düşecek bir şekilde zarar görebilir¹⁶⁶.

8. İtiraz Hakkı

Veri sahibinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak, profil çıkarma da dahil olmak üzere kendisi ile ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz etme hakkı bulunur. Veri sorumlusu, veri sahibinin menfaatleri, hakları ve özgürlüklerinden ağır basan işleme faaliyetlerine yönelik olarak veya yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından zorlayıcı meşru gerekçeler göstermediği sürece, kişisel veriler artık işlenemez.

Profil çıkarma GDPR'nin 4. maddesinde, bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi ile bu

¹⁶⁴ Çekin, s.134.

¹⁶⁵ Dülger (GDPR Bağlamında Kişisel Veriler), s.158.

¹⁶⁶ Barbara Engels, "Data Portability Among Online Platforms", **Internet Policy Review- Journal on Internet Regulation**, Cilt:5, 2016, s.1-17.

kişiyeye ilişkin belirli kişisel özelliklerin değeriendirilmesi için kişisel verilerin kullanımını içeren her türlü otomatik kişisel veri işleme biçimi olarak tanımlanmıştır. Bu durumda, veri sahibinin işlemeye itiraz etmesi halinde, veri sahibine ait özelliklerin analiz edilerek profil çıkarılması dahil tüm işleme faaliyetleri durur. Kişisel verilerin doğrudan pazarlama amaçları ile işlenmesi durumunda, veri sahibinin profil çıkarma da dahil olmak üzere kendisi ile ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz etme hakkı bulunur. Veri sahibinin doğrudan pazarlama amaçlarına yönelik olarak işleme faaliyetine itiraz etmesi halinde, kişisel veriler artık bu amaçlarla işlenemez.

Veri sahibinin kişisel verilerinin bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işlenmesi durumunda, işleme faaliyeti kamu yararı sebeplerinden dolayı gerçekleştirilen bir görevin yürütülmesi için gerekli olmadığı sürece, kendisi ile ilgili kişisel verilerin işlenmesine itiraz hakkı bulunur. Bu durumda, doğrudan pazarlama amacıyla kişisel verilerin işlenmesi haricinde, kamu menfaatleri ve veri sahibinin menfaatlerinden ağır basana göre itiraz hakkı işleme konulur. İtiraz hakkına sahip olduğu, veri sahibine en geç ilk iletişim anında ifade edilmelidir. Veri sahibi itiraz hakkını otomatik yollarla kullanabilir.

GDPR'ye göre bu itiraz hakkının istisnaları da mevcuttur. 22. maddeye göre, bir sözleşmenin ifası için gerekli olması veya açık rızanın varlığı halinde veri işlemeye itiraz edilemez. Ancak bu koşulların varlığında dahi veri sorumlusu en azından veri sahibinin kendi görüşünü ifade etme ve karara karşı çıkma yönündeki haklarını kullanabilmesi için uygun tedbirler uygular¹⁶⁷.

B. Veri Sorumlusu ve Veri İşleyenin Yükümlölükleri

GDPR, veri sahibinin haklarının ardından veri sorumlusu ve işleyicinin yükümlölüklerini düzenlemiştir.

¹⁶⁷ Profilleme ve itiraz hakkına yönelik detaylı açıklamalar için: Çekin, ss.134-137.

1. Gerekli Tedbirleri Alma Yükümlülüğü

GDPR'nin 24. maddesi ve devamında veri sorumlusunun genel yükümlülükleri ve alması gereken tedbirler düzenlenmiştir. Buna göre veri sorumlusu, işleme faaliyetinin mahiyeti ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiye riskleri dikkate alarak işleme faaliyetinin GDPR uyarınca gerçekleştirilmesini sağlamakla görevlidir. Bu görevini yerine getirirken veri sorumlusu uygun teknik donanımı sağlar ve düzenlemeye ilişkin tedbirler uygular. Dönemsel olarak bu tedbirleri gözden geçirir ve gerekirse günceller. Bu bağlamda işleme faaliyetine uygun olarak ve ölçülü bir şekilde gereken veri koruma politikalarını uygulamak veri sorumlusunun sorumluluğundadır. Voight ve Bussche'e göre uygun veri koruma politikasını sağlamaya yönelik yapılması gereken risk tabanlı veri koruma yönetim sisteminin sağlanmasıdır. Bu sistem, veri korumasının yerine getirilmesini ve kurum içinde güvenlikle ilgili gereksinimleri izleyen bir dahili uyum sistemidir. Veri koruma yönetim sistemi, GDPR kapsamındaki veri korumasıyla uyumlu, uygun teknik ve organizasyonel önlemlerin başarıyla uygulanmasına yardımcı olabilir. Bununla birlikte, veri sorumluları bu uygulamanın olağanüstü bir çaba gerektirip gerektirmediğini değerlendirmelidir. Veri koruma yönetim sistemi tipik olarak, veri işleme sistemlerinin yürütülmesini düzenleyen bilişim koruma sistemlerinden oluşur. Yapı olarak ise diğer yönetim ve bilişim sistemlerinden bir farkı yoktur. Bu nedenle diğer bilişim sistemleriyle temelde benzer yapılardır ancak, veri koruma yönetim sisteminin özgülendiği amaç yalnızca veri korumasına yöneliktir¹⁶⁸.

Veri sorumlusu, son teknoloji uygulama maliyeti, işleme faaliyetinin kapsamı amaçları ve işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri açısından teşkil ettiği çeşitli olasılıklar ve ciddiye riskleri dikkate alır. Gerek işleme yönteminin belirlenmesi gerek işleme faaliyeti esnasında, verilerin en alt düzeye indirilmesi başta olmak üzere tüm veri koruma ilkelerinin etkili bir şekilde uygulanması ve GDPR'nin sağladığı korumanın yerine getirilmesine yönelik güvenceleri sağlamaya yönelik çalışmalar yürütür ve tedbirler alır. Bu bağlamda veri sahibinin haklarını korumaya yönelik takma ad kullanımı gibi uygun teknik tedbirleri

¹⁶⁸ Paul Voight ve Axel Von Dem Bussche, **The EU General Data Protection Regulation (GDPR) A Practical Guide**, Springer, Almanya, 2017, s.33-34.

uygular. Veri sorumlusunun uygulayacağı bu tedbirler, her bir işleme amacı için uygun olmalıdır. Veri sorumlusunun bu yükümlülüğü toplanan kişisel veri miktarı, işlenme derecesi, saklama süresi ve erişilebilirliğe uygulanır. Bu tedbirler, olağan durumlarda, bireyin müdahalesi olmaksızın kişisel verilerin belirsiz sayıda gerçek kişinin erişimine açılmamasını sağlar.

2. Ortak Veri Sorumlularının İşbölümü Yapma Yükümlülüğü

GDPR'nin 26. maddesi ortak veri sorumlusu "*joint controllers*" kavramını hüküm altına almaktadır. Buna göre, iki ya da daha fazla sayıda veri sorumlusunun işleme amaçları ve yöntemlerini ortak bir şekilde belirlediği hallerde, ortak veri sorumlusu olurlar. Ortak sorumluluk durumunda hangi veri sorumlusunun GDPR kapsamındaki hangi yükümlülüğü yerine getireceğine dair işbölümüne birlikte karar verilir. Bununla birlikte her bir veri sorumlusu, GDPR kapsamındaki yükümlülüklerden birlikte sorumlu olmaya devam eder. Örneğin, bir gayrimenkul yönetim şirketi ev sahibi olan üniversitenin yurtlarını koruyup yönetebilir. Bu şirket üniversite adına öğrencilerle kira sözleşmesi yapar ve kira borçlarını takip eder. Kiraları toplayıp komisyonunu aldıktan sonra üniversiteye iletir. Şirket bu durumda kira ödemeleri dahil kiracılığa ilişkin tüm bilgilerin ortak veri sorumlusudur. Kiracılarla ilişki kurmak ve süreci yönetmek için öğrencilerden hangi bilgileri toplamaya ihtiyacı olduğuna şirket karar verir ancak bu bilgileri üniversite ile de paylaşır¹⁶⁹.

Ortak veri sorumlusu kavramı GDPR'de, sorumlulukların net bir şekilde paylaştırılmasını sağlamak için düzenlenmiştir. Zira veri sahipleri, verilerini işleyen çok sayıda kaynak ile karşı karşıya kaldığında, tek işlemeye göre daha az elverişli bir konuma yerleştirilemez¹⁷⁰.

Ortak veri sorumluları, tabi olduğu üye devlet veya Birlik hukuku çerçevesinde özellikle veri sahibinin haklarının kullanımı ve bilgi sağlama görevleri ile ilgili yükümlülükler uygunluğa ilişkin sorumluluklarını aralarındaki bir anlaşma

¹⁶⁹ Örnekler ve ortak veri sorumluluğu hakkında detaylı açıklamalar için bakınız: "What does it mean if you are joint controllers?" <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/> (01.05.2021)

¹⁷⁰ Voigt ve diğerleri, s.35.

vasıtasıyla şeffaf bir şekilde belirler. Bu anlaşma, veri sahipleriyle karşılıklı rolleri ve ilişkileri uygun şekilde yansıtır. Düzenlemenin kapsamı ve sorumluluklar veri sahibine de bildirilir. Anlaşmanın varlığına rağmen veri sahibi, GDPR kapsamındaki haklarını her veri sorumlusu açısından ve her veri sorumlusuna karşı kullanabilir.

3. Temsilci Atama Yükümlülüğü

Avrupa Birliği içerisinde yerleşik bulunan veri sahiplerinin, Avrupa Birliği dışında kurulu bir veri sorumlusu veya veri işleyicisi tarafından verilerinin işlenmesi mümkündür. GDPR'nin 27. maddesi bu hallerde yapılacak işlemler için veri sorumlusu veya veri işleyenin yazılı olarak Avrupa Birliği içerisinde bir temsilci belirtmesini şart koşturmuştur. Ancak, hassas veri kategorilerinin işlenmesini nadir olarak içeren işleme faaliyeti, ve gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebep olması muhtemel olmayan bir işleme faaliyetinin varlığı halinde temsilci atama şartı aranmaz. Bununla birlikte işlemeyi gerçekleştiren Birlik dışından dahi olsa bir kamu kurum veya kuruluşu ise temsilci atanmasına gerek yoktur.

Temsilcilik kişisel verileri işlenen veri sahiplerinin bulunduğu üye devletlerin birinde kurulur. Temsilci, işleme faaliyeti ile ilgili tüm hususlarda GDPR'ye uygun hareket etmek zorundadır. Bu amaçla, özellikle denetim makamları ve veri sahipleri tarafından muhatap alınmak üzere, veri sorumlusu veya işleyici tarafından yetkilendirilir. Temsilcinin atanmış olması, veri işleme faaliyetinin asıl sorumlusu olan veri sorumlusu ve veri işleyene karşı dava açılmasına engel teşkil etmez.

4. Uygun Veri İşleyenleri Seçme Yükümlülüğü

GDPR'nin 28. maddesine göre veri sorumlusu, kendi adına bir işleme faaliyetinin gerçekleştirilmesinin gerektiği hallerde, GDPR'nin gerekliliklerinin yerine getirilmesini ve veri sahibinin haklarının korunmasını sağlamak için veri işleyenleri kullanır. Veri işleyenlerin, işleme faaliyetinin mahiyetine uygun niteliklere sahip olması ve teknik tedbirler uygulama hususunda yeterli güvenceler sağlaması gerekmektedir. Bu görevi yerine getirirken veri işleyen, veri sorumlusunun önceden verdiği yazılı onayı olmaksızın başka bir veri işleyenle çalışamaz. Veri

işleyen verileri, Avrupa Birliği veya üye devlet hukukuna tabi bir sözleşme veya bir hukuki ilişkiye bağlı olarak işlemelidir. Doktrinde “kişisel veri işleme sözleşmesi”¹⁷¹ olarak ifade edilen bu sözleşme ile işleme faaliyetinin konusu, süresi, amacı, kişisel verilerin türü, veri sahiplerinin kategorileri ve veri sorumlusunun hakları ve yükümlülükleri belirlenir. Veri sorumlusu, bu düzenleme ile veri işleyenin yalnızca kendisinin verdiği belgelendirilmiş talimatlar doğrultusunda kişisel verileri işlemesi konusunda haberdar eder. Veri işleyen, veri işleme yetkisi kapsamında gizlilik taahhüdünde bulunur ve veri sorumlusu işleme süresince bu gizlilik taahhüdünün devamlılığını sağlamakla görevlidir. Sözleşme kapsamında veri işleyenin görevi, GDPR’ye riayet ederek mümkün olduğunca veri sorumlusuna yardımcı olmaktır.

Veri işleyenin, veri sorumlusu adına işleme faaliyetlerinin gerçekleştirilmesine yönelik olarak başka bir veri işleyenle çalışması da mümkündür. Bu durumda, veri sorumlusu ile veri işleyen arasında sözleşme ile ortaya konan veri koruma yükümlülükleri, veri işleyenler arasındaki yeni bir sözleşme veya hukuki tasarruf ile diğer veri işleyen açısından da uygulanır. Her ne kadar veri işleyenler arasında bir hukuki tasarruf yapılmış olsa da, diğer işleyicinin veri koruma yükümlülüklerini yerine getiremediği hallerde, ilk işleyici veri sorumlusuna karşı sorumlu olmaya devam eder. Veri işleyen veya veri sorumlusuna bağlı olarak verilere erişimi bulunan kişiler, veri sorumlusunun talimatı dışında verileri işleyemezler.

5. Kayıt Tutma Yükümlülüğü

GDPR’nin 30. maddesinde her veri sorumlusunun ve temsilcisinin, sorumluluğu altındaki işleme faaliyetlerine ilişkin bir kayıt tutacağı hüküm altına alınmıştır. Bu kayıtlar veri sorumlusunun, varsa ortak veri sorumlusunun, temsilcilerin ve veri koruma görevlisinin isimlerini ve irtibat bilgilerini içerir. Kayıtlarda işleme amaçları, kişisel veri kategorileri, kişisel verilerin açıklandığı veya açıklanacağı alıcı kategorileri, üçüncü bir ülke veya uluslararası bir kuruluşun

¹⁷¹ “Kişisel veri işleme sözleşmesi, veri işleyenin veri sorumlusunun talimatlarına uygun olarak kişisel verileri işlemeyi taahhüt ettiği; veri sorumlusunun da bu iş görme edimi karşılığında ücret ödeme borcu altına girdiği bir sözleşmedir.” Sözleşmenin tanımı ve tarafları hakkında detaylı açıklamalar için bakınız: Gamze Turan Başara, “Kişisel Veri İşleme Sözleşmesi”, **Uyuşmazlık Mahkemesi Dergisi**, Sayı:16, 2020, ss.57-90.

tanımlanması ve üçüncü ülke veya uluslararası kuruluşa yönelik kişisel veri aktarımları, farklı kategorilerdeki verilerin silinmesiyle ilgili öngörülen süre sınırları yer alır.

Veri sorumlusunun ve temsilcisinin tutması gereken kayıtların yanı sıra veri işleyen ve temsilcisinin de ayrıca kayıt tutması gereken hususlar yine aynı maddede düzenlenmiştir. Buna göre her veri işleyen ve temsilcisi, veri sorumlusu adına gerçekleştirdikleri işlemlere ilişkin kendi isim ve irtibat bilgileri ile adına hareket ettikleri veri sorumlusunun isim ve irtibat bilgilerini kaydederler. Bunun yanı sıra her veri işleme kategorisi, üçüncü bir ülke veya uluslararası bir kuruluşun tanımlanması ve üçüncü ülke veya uluslararası kuruluşa yönelik kişisel veri aktarımları hakkındaki bilgiler de veri işleyen ve temsilcisi tarafından kayıt altında tutulur. Gerek veri sorumlusu ve temsilcisinin, gerek veri işleyen ve temsilcisinin tutması gereken bu kayıtlara ilişkin kural, işleme faaliyeti veri sahiplerinin hakları bakımından bir risk yaratmadığı ve hassas verilere ilişkin bir işleme yapılmadığı takdirde, 250’den az kişi istihdam eden bir işletme veya kuruluşa uygulanmaz. Yani, işleme faaliyeti risk ve hassas veri içermiyorsa, 250 kişiden az personel bulunan yerlerde veri sorumlusu ve veri işleyenin bu kayıtları tutma mecburiyeti yoktur.

Kayıt tutmanın mecburi olduğu durumlarda kayıtlar elektronik format da dahil olmak üzere yazılı olarak tutulur. Veri sorumlusu ve veri işleyen ile temsilcileri, gerektiği takdirde bu kayıtları denetim makamı ile paylaşır.

6. Denetim Makamıyla İşbirliği Yükümlülüğü

GDPR’nin 31. maddesinde yer alan düzenlemeye göre, veri sorumlusu ve veri işleyen ile temsilcileri, işleme faaliyetlerine ilişkin görevlerinin yürütülmesi ile ilgili olarak talep edildiği takdirde, denetim makamı ile işbirliği yapar.

7. İşlemenin Güvenliğini Sağlama Yükümlülüğü

Veri sorumlusu ve veri işleyenin son teknoloji, uygulama maliyetleri ve işleme faaliyetinin mahiyeti, gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak hareket etmek zorunda olduğu

GDPR'nin 32. maddesinde düzenlenmiştir. Risk açısından uygun bir güvenlik seviyesi sağlamak amacıyla takma ad kullanımı ve şifreleme, işleme sistemleri ve hizmetlerinin gizliliği, bütünlüğünün sürekli olarak sağlanabilmesi yönünde uygun teknik tedbirleri uygulamak veri sorumlusu ve veri işleyenin yükümlülüğüdür. Bunun yanı sıra veri sorumlusu ve işleyen, fiziksel veya teknik bir olay halinde, kişisel verilerin elverişliliği ve kişisel verilere erişimin vakitlice eski haline getirilebilmesi, işleme faaliyetinin güvenliliğinin sağlanmasına yönelik olarak teknik ve düzenlemeye ilişkin tedbirlerin etkililiğinin düzenli olarak sınanması yönünde çalışmalar yürütmelidir.

Uygun güvenlik seviyesi değerlendirilirken iletilen, saklanan veya işlenen kişisel verilerin imha edilmesi, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişim başta olmak üzere özellikle işleme faaliyetinin yol açtığı riskler göz önünde bulundurulmalıdır. Bu düzenleme ile kişisel verilerin herhangi bir suretle ele geçirilmesi halinde ortaya çıkması muhtemel riskler en az indirgenmeye çalışılmıştır¹⁷². Veri sorumlusu ve veri işleyenin yetkisiyle hareket eden herhangi bir gerçek kişinin, Birlik ya da üye devlet hukuku uyarınca mecbur olmadıkça, kişisel verileri işlemesini engellemek yönünde tedbirler alınması da bu madde kapsamında hüküm altına alınmıştır.

8. Bildirim Yükümlülüğü

GDPR, bildirim yükümlülüğünü iki boyutta ele almıştır. 33. maddede yer alan yükümlülük bir kişisel veri ihlalinin denetim makamına bildirilmesini düzenlerken, 34. maddede ise veri ihlalinin veri sahibine bildirilmesi düzenlenmiştir. İlk olarak bir veri ihlalinin denetim makamına bildirilmesi hususunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olup olmasına göre karar verilmesi gerektiği belirtilmiştir. İhlal sonucu bir riskin ortaya çıkması söz konusu ise veri sorumlusu gecikmeksizin, hatta mümkünse en geç 72 saat içerisinde, kişisel veri ihlalinin yetkin denetim makamına bildirir. Veri sorumlusu en geç 72 saat içerisinde bildirim yapmazsa, bildirimle birlikte gecikme sebeplerini de açıklamak zorundadır. Veri işleyen de bir

¹⁷² Develioğlu, s.107.

kişisel veri ihlalinin haberdar olduktan sonra gecikmeksizin veri sorumlusuna bildirimde bulunur.

Veri sorumlusunun denetim makamına yapacağı bildirimde ilgili veri sahibi kategorileri ve yaklaşık sayısı ile birlikte kişisel veri ihlalinin boyutu açıklanır. Veri koruma görevlisi gibi veri işlemeye ve korumaya yönelik görev alan kişilerin isim ve irtibat bilgileri ile birlikte kişisel veri ihlalinin olası sonuçları denetim makamına yapılacak bildirimde yer alır. Yine bu bildirimle kişisel veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik tedbirler ve ihlalinin ele alınması için veri sorumlusu tarafından alınan tedbirler belirtilir. Bu bildirim içerisinde denetim makamına verilmesi gereken bilgilerin hepsinin birlikte tek seferde sağlanması mümkün değilse, gecikmenin olası zararlarının önüne geçmek adına aşamalı olarak bilgi verilebilir. Bildirimin de yapılmasıyla birlikte veri sorumlusu kişisel veri ihlallerini belgelendirir.

GDPR'nin 34. maddesinde düzenlenen ihlalin veri sahibine bildirilmesi hususunda ise, yine bildirimin yapılması için ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olup olmadığı değerlendirilir ve riskin muhtemel olması halinde ihlal veri sorumlusu tarafından gecikmeksizin veri sahibine iletir. Veri sahibine yapılan bildirimde ihlale yönelik açıklama açık ve sade bir dil kullanılarak yapılır ve ihlalin bertaraf edilmesine yönelik alınan önlemlerden de bahsedilir. Ancak, veri sorumlusunun uygun koruma tedbirleri uygulayarak kişisel verileri erişim yetkisi bulunmayan herkese karşı okunamaz hale getirmesi ve veri sahiplerinin hakları ve özgürlüklerine ilişkin yüksek riskin ortaya çıkmasının artık mümkün olmamasını sağlayan ek tedbirler alması halinde veri sahibine bildirimde bulunma yükümlülüğü ortadan kalkar. Bununla birlikte bildirimin ölçsüz bir çaba gerektirecek olması durumunda da veri sorumlusu bildirimde bulunmayabilir. Böyle bir durumda veri sahiplerine tek tek bildirimde bulunmak yerine, kamuya yönelik bir bildirim veya benzer bir tedbir uygulanır. Kamuya yönelik yapılan bildirimin, veri sahibine doğrudan yapılacak bir bildirimle aynı etkililikte olmasına dikkat edilmelidir.

Veri sorumlusunun halihazırda kişisel veri ihlalinin veri sahibine iletmemiş olması durumunda denetim makamı, ihlalin yüksek bir riske sebebiyet verme

olasılığı olduğuna karar verdiği takdirde veri sorumlusunun bu bildirimi yapmasını şart koşabilir.

9. Veri Koruma Etki Değerlendirmesi ve Ön İstisare Yükümlülüğü

GDPR'nin 35. maddesine göre, son teknoloji kullanılarak gerçekleştirilen veri işleme faaliyetlerinde, işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesi söz konusu olabilir. Bu durumda veri sorumlusu işleme faaliyetinden önce, işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapar. Veri sorumlusu bu değerlendirmeyi yaparken eğer var ise veri koruma görevlisinin tavsiyesine de başvurur.

Veri koruma etki değerlendirmesi, kişisel verilerin korunduğundan emin olunmasını sağlar ve işlemenin GDPR ile uyumlu olarak yapıldığını gösterir. Bu değerlendirme ile veri korumasının doğası, özgünlüğü, ciddiyeti değerlendirilir. Bu yönüyle veri koruma etki değerlendirmesi için önleyici veri koruma yöntemi olduğu da söylenebilir¹⁷³.

Veri koruma etki değerlendirmesi gerekliliğine tabi olan işleme faaliyeti türlerine yönelik belirlemeyi denetim makamı yapar ve oluşturduğu listeyi kamu ile de paylaşır. Aynı zamanda denetim makamı veri koruma etki değerlendirmesinin gerekli olmadığı işleme faaliyeti türlerini de belirler.

Veri koruma etki değerlendirmesi işleme faaliyetleri ve işleme amaçlarına ilişkin sistematik açıklamalar, işleme faaliyetlerinin gerekliliği ve orantılılığına yönelik değerlendirmeler, veri sahiplerinin hakları ve özgürlüklerine yönelik risklere ilişkin görüşleri içerir. Kişisel verilerin korunmasının sağlanması ve GDPR'ye uygun işleme yapıldığının gösterilmesi, veri korumasına ilişkin güvenceler ve güvenlik tedbirleri de bu değerlendirme içerisinde yer alır. Bu değerlendirmeyi yaparken veri sorumlusu, kendi ticari menfaatlerini korumak suretiyle veri sahiplerinin işleme faaliyetine ilişkin görüşlerini de alabilir. Veri sorumlusu, işlemenin devam ettiği süreç içerisinde, işleme faaliyetlerinin teşkil ettiği risk açısından bir değişiklik

¹⁷³ Voigt ve diğerleri, s.47.

meydana geldiği takdirde, veri koruma etki değerlendirmesi yönünden yeniden bir gözden geçirme ve düzenleme yapılabilir.

GDPR'nin 36. maddesine göre veri koruma etki değerlendirmesi sonucunda riskin azaltılması hususunda tedbir alınmazsa işlemenin yüksek bir riske sebebiyet vereceğinin görüldüğü hallerde, veri sorumlusu işleme faaliyetinden önce denetim makamına danışır. İşlemeden önce bir ön istişare olarak değerlendirilen bu danışma sonucunda, denetim makamı işleme faaliyetinin GDPR'yi ihlal edeceğini düşündüğü hallerde, sekiz hafta içinde veri sorumlusuna yazılı olarak tavsiyede bulunur. Veri sorumlusu ön istişare için veri sorumluları ve veri işleyenlerin sorumluluk sınırlarını, işlemenin amaçları ve yöntemlerini, veri sahibinin temel hak ve özgürlüklerini korumak için alınan tedbirleri ve güvenceleri, var ise veri koruma görevlisinin irtibat bilgilerini ve veri koruma etki değerlendirmesini denetim makamıyla paylaşır.

Üye devletler de veri işleme hususunda ulusal meclis tarafından kabul edilecek bir yasama teklifi veya yürütme faaliyeti taslağı hazırlarken denetim makamına danışır. GDPR, üye devletlerin kendi hukukları çerçevesinde kamu yararına gerçekleştirilen bir göreve yönelik olarak yapılan işlemlerde, veri sorumlusunun denetim makamına danışmasını ve ön istişarede bulunmasını şart koşabileceğini öngörmüştür.

10. Veri Koruma Görevlisi Atama Yükümlülüğü

GDPR'nin 37. maddesi veri koruma görevlisi atamamanın zorunlu olduğu halleri düzenlemiştir. Buna göre işleme faaliyeti bir kamu kuruluşu veya organı tarafından gerçekleştiriliyorsa ve veri sahiplerinin sistematik bir şekilde büyük çaplı olarak izlenmesini gerektiriyorsa veri sorumlusu, veri koruma görevlisi atamalıdır. Bununla birlikte hassas verilerin ve mahkumiyet kararlarına ilişkin kişisel verilerin işlenmesi halinde de veri koruma görevlisi atanması gerektirdiği GDPR tarafından hüküm altına alınmıştır. Veri sorumlusu, bu zorunlu hallerin dışında da bir veri koruma görevlisi belirleyebilir. Veri koruma görevlisi, veri sorumlusuna bağlı bir çalışan olabileceği gibi, hizmet sözleşmesi ile de belirlenebilir. Seçilen veri koruma görevlisinin irtibat bilgileri denetim makamı ile paylaşılır.

Veri koruma görevlisinin kişisel verilerin korunmasına ilişkin tüm konulara zamanında müdahil olması ve görevlerini yerine getirmesi veri sorumlusu tarafından sağlanır. Veri koruma görevlisinin görevini yerine getirirken hiçbir kişi ve kurumdan talimat almaması da veri sorumlusunun denetimindedir. Veri koruma görevlisi, bu göreviyle çatışmayan başka görevleri de yerine getirebilir. Veri koruma görevlisinin görevlerinin birbiriyle çatışmadığının kontrolünü veri sorumlusu yapar. Bununla birlikte, veri koruma görevlisinin görevini yerine getirirken üzerinde baskı hissetmemesi amacıyla veri sorumlusu tarafından işten çıkarılamayacağı ve cezalandırılmayacağı hüküm altına alınmıştır. Veri koruma görevlisi, doğrudan veri sorumlusu ve işleyicinin en üst yönetimine rapor verir.

Veri sahipleri kişisel verilerinin işlenmesi GDPR kapsamındaki haklarının kullanımı ile ilgili olarak veri koruma görevlisiyle irtibata geçebilir. Veri koruma görevlisi, Birlik veya üye devlet hukuku uyarınca görevlerinin yerine getirilmesi ile ilgili olarak sır saklama veya gizlilik yükümlülüğü altındadır.

Veri koruma görevlisinin görevi, veri sorumlusu ve veri işleyenlere yükümlülükleri hususunda bilgi vermek ve tavsiyede bulunmaktır. Veri sorumlusu ve işleyenin GDPR ve diğer kişisel veri mevzuatlarına uygun hareket edip etmediğini veri koruma görevlisi denetler. Yine veri koruma etki değerlendirmesine ilişkin tavsiyede bulunmak ve denetim makamıyla işbirliği yapmak veri koruma görevlisinin görevidir.

III. AVRUPA BİRLİĞİ'NDE KİŞİSEL VERİLERİN İŞLENMESİNİ DENETLEYEN VE DÜZENLEYEN KURUMLAR

Avrupa Birliği Genel Veri Koruma Tüzüğü, uygulanmasını denetlemek ve Avrupa Birliği içinde kişisel verilerin korunması uygulamasının yeknesak bir biçimde gerçekleştirilmesini sağlamak için bir takım denetleyici ve düzenleyici kurumlar öngörmüştür. Bunlar; her üye devletin oluşturacağı bir veya birden fazla denetim makamı ile kendi hukuki kişiliği bulunan Avrupa Birliği Veri Koruma Kurulu'dur¹⁷⁴.

¹⁷⁴ Develioğlu, s. 137.

A. Denetim Makamları

GDPR'nin 51. ve devamı maddelerinde hüküm altına alındığı üzere denetim makamı her üye devletin, gerçek kişilerin işleme faaliyeti ile ilgili temel hakları ve özgürlüklerini korumak ve Avrupa Birliği içerisinde kişisel verilerin serbest akışını kolaylaştırmak üzere, GDPR'nin uygulamasının izlenmesinden sorumlu olarak belirlenmiştir.

1. Genel Olarak

Her bir denetim makamının amacı, GDPR'nin Avrupa Birliği içerisinde tutarlı bir şekilde uygulanmasını sağlamaktır. Avrupa Birliği genelinde GDPR'nin istikrarlı ve yeknesak bir şekilde uygulanmasını sağlamak üzere, denetim makamlarının birbirleriyle ve Avrupa Komisyonu ile işbirliği yapmaları düzenlenmiştir. Bu uygulamayı sağlarken denetim makamlarının kimseden emir ve talimat almadan tam bağımsız olarak hareket edeceği de hüküm altına alınmıştır. Denetim makamlarının üyeleri, dış etkilerden uzak olmalı, hiç kimseden talimat almamalıdır. Üye devletler, denetim makamlarına görevlerini yerine getirmeleri için gerekli kaynakları ve altyapıyı sağlamakla, gereken donanımına sahip personeli tahsis etmekle ve bu personelin sadece denetim makamından talimat aldığını güvence altına almakla yükümlüdür. Tüm bunlarla birlikte denetim makamı üyeleri de görevleriyle bağdaşmayan işlerden uzak durmalıdır. Denetim makamları bağımsız olmakla birlikte, finansal yönden bağlı oldukları üye devletin kontrolüne tabidirler.

Denetim makamlarının üyelerinin görevinin önemi gereği ve üyelerin üstlendiği görevin hassasiyetinden dolayı üyelerin taşınması gereken nitelikler ve göreve gelmeleri ile görevden alınmaları da GDPR'de özel olarak düzenlenmiştir. Buna göre üye devletler denetim makamlarının üyelerini; parlamento, hükümet, devlet başkanı veya ülke hukukuna göre atama yetkisine sahip bir organ aracılığıyla seçecektir. Seçilen üyeler kişisel verilerin korunması alanında yetkin olmalıdır. Denetim kurumu üyelerinin görevi Avrupa Birliği ve görev yaptıkları üye devletlerin hukukuna uygun olacak şekilde; görev süresinin dolması, istifa ya da zorunlu emeklilik ile sona erer. Ancak bunun haricinde; görevin ciddi şekilde kötüye

kullanılması ya da görevleri yerine getirmek için gerekli koşulların artık sağlanmaması hallerinde üyelerin görevden alınması gündeme gelebilir.

Her üye ülkenin denetim makamı, kendi ülkesinin sınırları içerisinde yetkilerini kullanabilir. Ancak doğal olarak bu denetim yetkisinin sınırı, konuyla ilgili yargı yetkisini kullanan mahkemelerin alanına girildiğinde son bulmaktadır. Veri işlemenin sınır ötesi olarak yapıldığı durumlarda; işlemeyi gerçekleştiren veri sorumlusu veya işleyenin ana işletmesinin tabi olduğu denetim makamı, baş denetim makamı olarak hareket eder. “Tek durak noktası” olarak anılan bu yaklaşım sayesinde, Avrupa Birliği içinde birden çok işletmesi olan veya birden çok ülkede faal olan veri sorumluları ve işleyenler tek bir denetim makamı ile muhatap olacaktır¹⁷⁵.

2. Görev ve Yetkileri

Denetim makamlarının görevleri GDPR’nin 57. maddesinde tek tek sayılmıştır. Buna göre denetim makamlarının belli başlı görevleri GDPR’nin uygulanmasını izlemek ve yürütmek, halkın işleme faaliyeti ile ilgili riskler ve haklara yönelik bilinci ve anlayışını geliştirmek ve özellikle çocuklara yönelik faaliyetlere özel alaka göstermektir. Denetim makamları, işleme faaliyeti ile ilgili olarak gerçek kişilerin hakları ve özgürlüklerinin korunmasına ilişkin yasal ve idari tedbirler hususunda ulusal parlamento, hükümet ve diğer kuruluşlar ile organlara tavsiyede bulunur. GDPR kapsamındaki yükümlülükleri hususunda veri sorumluları ve işleyicileri bilinçlendirir, veri sahibine GDPR kapsamındaki haklarının kullanımı hususunda bilgi sağlar ve bu konuda diğer üye devletlerdeki denetim makamları ile işbirliği yapar.

Veri sahibi veya bir kuruluşun veri işleme faaliyetleri hususunda denetim makamına şikayette bulunma hakları vardır. Denetim makamı bu şikayetleri titizlikle ele alır ve soruşturur. Avrupa Birliği genelinde GDPR’nin uygulanması ve yürütülmesine ilişkin tutarlılık sağlanması amacıyla, diğer denetim makamlarıyla işbirliği yapmak ve diğer denetim makamlarına karşılıklı destek sağlamak da denetim makamlarının görevidir. Bu görevlerinin yanı sıra denetim makamları

¹⁷⁵ Develioğlu, s.138.

GDPR'nin uygulanmasına ilişkin soruşturmalar yürütür, bilgi ve iletişim teknolojileri ve ticari uygulamaların gelişimi başta olmak üzere kişisel veriler ile ilgili gelişmeleri izler, kişisel verilerin işlenmesiyle ilgili tavsiyelerde bulunur, GDPR'ye yönelik ihlallerin kayıtlarını tutar.

GDPR'nin ortaya çıkış sürecinde temel amaçlardan biri olan yeknesaklığı sağlamak, denetim makamlarının görevlerinin de başlıcaları arasındadır. GDPR öncesi dönemde Facebook ve Google gibi büyük şirketlerin sınır aşan veri ihlallerinde, üye ülkelerdeki denetim makamları birbirinden farklı kararlar vermiştir. Bu durum da Avrupa Birliği'nde kişisel verilerin korunması hakkının uygulanmasında sorunlara yol açmıştır. Bu sorunları gelecekte önleyebilmek için denetim makamlarının görevleri düzenlenirken yeknesaklık mekanizması öngörülmüştür¹⁷⁶.

Denetim makamlarının bu görevleri yerine getirirken kullanabilecekleri yetkileri de GDPR'nin 58. maddesinde düzenlenmiştir. Buna göre denetim makamlarının görevlerinin yerine getirilmesi için ihtiyaç duyduğu bilgilerin sağlanması hususunda veri sorumlusu ve işleyici veya veri sorumlusunun veya işleyicinin temsilcisine talimat vermek, veri koruma denetimleri için soruşturmalar yürütmek, GDPR ile ilgili bir ihlal iddiasını veri sorumlusu veya işleyiciye bildirmek, veri sorumlusu ve işleyicinin her türlü tesisine erişim sağlamak gibi önemli yetkileri de bulunmaktadır. Bunların yanı sıra denetim makamları bir veri sorumlusu veya işleyiciye amaçlanan işleme faaliyetlerinin GDPR'nin hükümlerini ihlal etmesinin muhtemel olduğu hususunda ihtarlarda bulunup işleme faaliyetlerinin GDPR'nin hükümlerini ihlal etmiş olduğu hallerde, bir veri sorumlusu veya işleyiciye kınama cezaları verebilir. Yine denetim makamları, veri sahibinin GDPR uyarınca sahip olduğu haklarının kullanımına ilişkin taleplerine uyulması ve bir kişisel veri ihlalinin veri sahibine iletilmesi hususunda veri sorumlusu veya işleyiciye talimat verebilir, bir işleme yasağı da dahil olmak üzere geçici veya kati bir sınırlama getirebilir.

GDPR, veri ihlaline uğradığı takdirde veri sahibine doğrudan denetim makamına başvurma hakkı tanımıştır. 77. maddeye göre veri sahibi, kişisel verisine

¹⁷⁶ Nilgün Başalp, "Avrupa Birliği Veri Koruması Genel Rgölasyonu'nun Temel Yenilikleri", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**", Cilt:21, Sayı:1, 2015, s.87.

yönelik işleme faaliyetinin GDPR'ye aykırı olması nedeniyle, mutlak meskeninin veya işyerinin bulunduğu yer veya ihlalin meydana geldiği Avrupa Birliği üyesi devletin denetim makamlarından birine başvurabilir. İhlallerden doğan hak kayıplarının önüne geçmek için öngörülen kurallardan biri olarak da, veri sorumlusunun bir ihlalin varlığı halinde denetim makamını ivedi olarak bilgilendirilmesi düzenlenmiştir.

Denetim makamlarının son derece önemli yetkilere sahip olması nedeniyle, herhangi bir hak ihlalinin önüne geçmek adına GDPR'nin 78. maddesinde denetim makamına karşı iç hukuk yoluna başvurma hakkı düzenlenmiştir. Buna göre her gerçek veya tüzel kişinin kendileriyle ilgili, bir denetim makamı tarafından verilen ve yasal bağlayıcılığı olan kararlara karşı iç hukuk yoluna başvurma hakkı vardır. Bununla birlikte yetkin olan denetim makamının bir şikayeti üç ay içerisinde incelemeye almadığı, şikayetin akıbeti veya sonucu hakkında veri sahibini bilgilendirmediği hallerde veri sahibinin de iç hukuk yollarına başvurma hakkı vardır. Bu sayede, veri sorumlusu, veri işleyicileri ve veri öznelere denetleme makamlarının işlem ve kararlarına karşı mahkemeler önünde hak arama imkanı tanınmıştır.

Denetim makamları faaliyetleriyle ilgili olarak bir yıllık rapor hazırlar. Bu raporlar ulusal parlamentoya, hükümete ve üye devlet hukuku çerçevesinde belirlenen diğer kuruluşlara da iletilir.

Veri sorumlusu veya veri işleyen ana işletmesinin veya tek işletmesinin denetim makamının sınır ötesi işleme faaliyetlerine yönelik olarak baş denetim makamı olarak hareket edeceği düzenlenmiştir. Baş denetim makamı ve ilgili denetim makamları uzlaşmaya varmak için gerekli tüm bilgileri birbirleriyle paylaşır. Baş denetim makamı, soruşturmaların yürütülmesi açısından veya başka bir üye devlette kurulu bulunan bir veri sorumlusu veya veri işleyene ilişkin bir tedbirin uygulanmasının izlenmesi açısından ilgili diğer denetim makamlarının karşılıklı yardım sağlamasını herhangi bir zamanda talep edebilir.

GDPR'nin 61. maddesine göre her denetim makamı başka bir denetim makamının talebine herhangi bir gecikmeye mahal verilmeksizin ve talebi aldıktan sonra en geç bir ay içerisinde yanıt vermelidir. Yardım taleplerinde talebin amacı ve sebepleri de dahil olmak üzere gerekli tüm bilgilere yer verilir. Paylaşılan bu bilgiler

yalnızca talep edilen amaç doğrultusunda kullanılabilir. Denetim makamları, diğer üye devletlerin denetim makamlarının üyelerinin veya personelinin dahil olduğu ortak çalışmalar gerçekleştirebilir. Veri sorumlusu veya veri işleyenin çeşitli üye devletlerde işletmelerinin bulunduğu hallerde, her üye devletin bir denetim makamının ortak çalışmalara katılma hakkı bulunur. Bu durumda çalışmayı yürütmeye yetkili olan denetim makamı her üye devletin denetim makamını ortak çalışmalara katılmaya davet eder.

GDPR'nin 63. maddesinde düzenlenen tutarlılık mekanizmasına göre, denetim makamları, kişisel verilerin korunmasının etkin ve istikrarlı bir şekilde sağlanabilmesi için işbirliği içinde hareket eder. İşbirliği, bir üye devletin denetim kurumuyla diğer üye devletin denetim kurumunun birlik içinde ve Komisyon ile irtibatlı hareket etmesi şeklinde olabileceği gibi, bir üye ülkede baş denetim kurumu ile diğer denetim kurumları arasında da söz konusu olabilir.

Bazı istisnai hallerde, ilgili bir denetim makamının veri sahiplerinin hakları ve özgürlüklerinin korunmasına yönelik olarak acil bir şekilde harekete geçilmesine ihtiyaç olduğu değerlendirilebilir. Bu durumda ilgili denetim makamı, tutarlılık mekanizmasından istisnaya giderek, kendi topraklarında üç ayı geçemeyecek belirli bir geçerlilik süresi boyunca hukuki sonuçlar doğurması amaçlanan geçici tedbirleri ivedilikle alabilir. İlgili denetim makamı, bu tedbirleri ve tedbirlerin alınma sebeplerini, herhangi bir gecikmeye mahal vermeksizin diğer ilgili denetim makamlarına, Kurul'a ve Komisyon'a iletir.

B. Avrupa Veri Koruma Kurulu

GDPR'nin 68. maddesine göre Avrupa Veri Koruma Kurulu adı altında tüzel kişiliğe sahip Avrupa Birliği organı kurulması düzenlenmiştir. GDPR'nin Avrupa Birliği içinde etkili bir şekilde uygulanmasını sağlamak amacıyla kurulan Avrupa Veri Koruma Kurulu'nun, üye devletler arasında da kişisel verilerin korunmasının yeknesak bir şekilde uygulanmasını sağlama hedeflerine yönelik bir yenilik olduğu söylemek mümkündür¹⁷⁷.

¹⁷⁷ Yörük, s.44.

Kurul kararlarını üyelerinin salt çoğunluğu ile alır. Başkan, üyeler arasından salt çoğunluk ile seçilir. Kurul'un toplantılarının düzenlenmesi, toplantı gündeminin hazırlanması, Kurul tarafından alınan kararların baş denetim makamına veya ilgili denetim makamlarına bildirilmesi başkanın görevleridir. Kurul görüşmeleri gizli yapılır. İdari yapı başkan, iki adet başkan yardımcısı ve sekreteryadan oluşur. Sekreterya Kurul'a günlük çalışmaları hususunda analitik, idari, lojistik destek sağlar.

Kurul'un temsilcisi başkanıdır ve Kurul her üye devletin bir denetim makamı başkanı ile Avrupa Veri Koruma Denetmeni veya temsilcilerinden meydana gelir. Kurul, görevlerini yerine getirirken veya yetkilerini kullanırken, hiç kimseden talimat talebinde bulunmaz ve talimat almaz. GDPR'nin 70. maddesinde Avrupa Veri Koruma Kurulu'nun görevleri sayılmıştır. Kurul'un görevleri GDPR'nin doğru bir şekilde uygulanmasını sağlamak, Birlik içerisinde kişisel verilerin korunmasıyla ilgili her türlü hususta Komisyona tavsiyede bulunmak, kişisel verilerin kopyalarının halka açık iletişim hizmetlerinden silinmesiyle ilgili usullere yönelik kılavuzlar yayınlamak, denetim makamlarının tutarlılık mekanizması uyarınca sunulan konulara yönelik olarak çıkardığı taslak kararlara ilişkin görüşler bildirmek ve bu hususta denetim makamları ve mahkemeler tarafından alınan kararlara ilişkin halkın erişebileceği bir elektronik sicil tutmaktır.

Kurul dilerse kendi kararıyla veya üyelerinden birinin talebi üzerine GDPR'nin uygulanmasına ilişkin her türlü konuyu inceler ve GDPR'nin tutarlı bir şekilde uygulanmasını teşvik etmek üzere tavsiyeler ve yayınlar. Kişisel veri ihlallerinin tespit edilmesi ve veri sorumlusu ile veri işleyenin kişisel veri ihlali hususunda bildirimde bulunmasının gerekli olduğu özel durumlar açısından olabilecek en iyi uygulamaları yayınlar. Kişisel veri ihlalinin, gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir risk teşkil etmesinin muhtemel olduğu halleri açıklamak da Kurul'un görevidir. Kişisel veri aktarımlarına yönelik kriterler ve gereklilikleri Kurul belirler. Yayınladığı tüm kılavuz, tavsiye ve en iyi uygulamalara yönelik kararların uygulanıp uygulanmadığı yine Kurul tarafından denetlenir. Kurul, GDPR'ye karşı yapılan ihlallerin gerçek kişiler tarafından bildirilmesine yönelik ortak usulleri oluşturur, davranış kurallarının hazırlanmasını ve veri koruma

belgelendirme mekanizmaları ve veri koruma mühürleri ile işaretlerinin oluşturulmasını teşvik eder.

Kurul Birlik içerisinde, üçüncü ülkelerde ve uluslararası kuruluşlarda işleme faaliyetine ilişkin olarak gerçek kişilerin korunması ile ilgili kılavuzlar, tavsiyeler ve en iyi uygulamaların pratikte uygulamasına ilişkin bir gözden geçirmeye yer verilen bir yıllık rapor hazırlar. Rapor kamuoyuna açıklanır ve Avrupa Parlamentosu'na, Konsey'e ve Komisyon'a iletilir. Tüm bu görevlerinin yanı sıra Kurul, denetim makamlarının alacağı veri koruma etki değerlendirmesine tabi işleme faaliyetlerine ilişkin bir listenin kabul edilmesi, bir organın akreditasyonuna yönelik kistasların onaylanması, standart veri koruma şartlarının belirlenmesi tedbirlerinden herhangi birine ilişkin görüşünü inceler. Bir denetim makamının karşılıklı yardım yükümlülüklerine veya ortak çalışmalara ilişkin yükümlülükler uymaması halinde, başka bir denetim makamı, bu durumun Kurul tarafından incelenmesini talep edebilir. Bu durumda Kurul, kendisine sunulan hususla ilgili bir görüş bildirir.

GDPR'nin 65. maddesinde Kurul'un ihtilaflı durumlar halinde alacağı bağlayıcı kararlar düzenlenmiştir. Kurul ilgili denetim makamlarından hangisinin ana işletme açısından yetkili olduğuna dair çelişkili görüşler bulunduğu, yetkili bir denetim makamının Kurul görüşüne uygun hareket etmediği durumlarda ve bir denetim makamı "tek durak noktası" olarak tabir edilen hallerin varlığında gerekçeli bir itiraz ileri sürmüştü bağlayıcı bir karar alır.

IV. HAKLARIN VE MENFAATLERİN KORUNMA YOLLARI

GDPR'nin 77. ve devamı maddelerinde veri sahibinin, kişisel verilerinin işlemeye konu olması nedeniyle sahip olduğu haklarına zarar geldiği takdirde başvurabileceği yollar, zararların tazmini ve veri sorumlusuna uygulanacak yaptırımlar düzenlenmiştir.

A. İdari Başvuru Yolları

GDPR 77. ve 84. maddeleri arasında, kişisel verilerin korunması hakkının ihlalinin önüne geçebilmek için idari, hukuki ve cezai yaptırım yolları düzenlemiştir.

İdari başvuru yolları olarak şikayette bulunma ve idari para cezası konuları ele alınmaktadır.

1. Şikayet Başvurusu

Her veri sahibi, kendisine ait kişisel verilerin işlenmesinin GDPR’yi ihlal ettiğini düşündürecek hallerin ortaya çıkması durumunda yerleşim yerinde, iş yerinin bulunduğu yerde veya ihlalin meydana geldiği yerde bulunan denetim makamlarından birine şikayette bulunma hakkına sahiptir. GDPR’nin 77. maddesinde düzenlenen bu hakkı kullanmak, veri sahibinin hukuki veya cezai yollara başvurma hakkına hanel getirmez.

Şikayet başvurusunu alan denetim makamı şikayetin seyri ve sonucu hakkında veri sahibini bilgilendirir. Kişisel verilerinin ihlali ile ilgili şikayette bulunan veri sahibinin, şikayeti bildirdiği denetim makamı, şikayete ilişkin GDPR hükümleriyle getirilen çözüm yollarını ve yaptırımları uygulamalıdır. Denetim makamı bu esnada somut olayın tüm özelliklerini bir arada değerlendirip karar vermelidir. Uygulanacak çözüm yolları ile yaptırımların etkili, orantılı ve caydırıcı nitelik taşımaları ve Avrupa Birliği bünyesine meydana gelen aynı ya da benzer nitelikteki ihlallere eşdeğer yaklaşımlar geliştirilerek uygulamada tutarlılığın sağlanması denetim makamlarının sorumluluğundadır¹⁷⁸.

Denetim makamlarına tanınmış olan bu yetkilerin sınırlarını çizmek adına GDPR’nin 78. maddesinde denetim makamlarının kararlarına karşı başvuru yolları belirlenmiştir. Buna göre her gerçek veya tüzel kişi bir denetim makamının yasal bağlayıcılığı olan bir kararına karşı kanun yoluna başvurabilir. Bu başvurunun yapılması aynı zamanda diğer adli ve idari yaptırım yollarına başvurma hakkını engellemez. Denetim makamı yetkili olduğu alanda kendisine yapılan bir şikayet başvurusunu üç ay içerisinde ele almadığı veya şikayetin seyri veya sonucu hakkında veri sahibini bilgilendirmediği hallerde her veri sahibinin kanun yoluna başvurma hakkı bulunur. Denetim makamına karşı açılacak davalar denetim makamının kurulu bulunduğu üye devlet mahkemelerinde açılır.

¹⁷⁸ İpek Çimen Bulut, “Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları”, **Anadolu Üniversitesi Sosyal Bilimler Dergisi**, Cilt:20, Sayı:2, 2020, s.135.

Veri sahipleri, kişisel verilerinin GDPR'ye aykırı bir şekilde işlendiği ve kişisel verilerinin korunması hakkının ihlal edildiği yönünde bir değerlendirmede bulunduğu takdirde kanun yoluna başvurabilir. Veri sahibinin kanun yoluna başvurması halinde denetim makamına şikayette bulunmak gibi diğer şikayet hakları saklı kalmaya devam eder. Yani veri sahipleri dilerse GDPR'nin 77. maddesi kapsamında denetim makamına şikayette bulunup aynı zamanda 79. maddeye göre adli yollara da başvurabilir. Bu bağlamda bir veri sorumlusu veya veri işleyene karşı açılacak davalar, kişisel veri ihlalinin gerçekleştiren işletmenin bulunduğu üye devletin mahkemelerinde veya veri sahibinin mutlak meskeninin bulunduğu üye devletin mahkemelerinde açılabilir.

Veri sahibinin Avrupa Birliği bünyesinde faaliyet gösteren herhangi bir organın, kişisel verilerin işlenmesinde hukuka aykırı davrandığı gerekçesiyle ABAD'a başvurusunun mümkün olmasıyla birlikte; veri sahibi, veri sorumlusu, veri işleyen veya denetim makamının kendilerini ilgilendiren Avrupa Veri Koruma Kurulu'nun bir kararını iptal etmek amacıyla da ABAD'a başvurusu mümkündür. Veri sahibinin kişisel verilerin korunması hakkına riayet edilmediği gerekçesiyle yapacağı başvuru, ABAD'ın ilk derece mahkemesi olarak faaliyet gösteren Avrupa Birliği Genel Mahkemesi'ne yapılır¹⁷⁹.

Kural olarak, şikayet yollarına ancak kişisel verilerin korunması hakkı ihlale uğrayan veri sahibi bizzat başvurabilir. Ancak GDPR'nin 80. maddesinde şikayet başvurusunda bulunacak veri sahibinin temsil edilmesi hususu düzenlenmiştir. Buna göre veri sahibi, bir üye devlet hukukunca kurulmuş bulunan ve veri sahiplerinin kişisel verilerinin korunmasına ilişkin hakları ve özgürlüklerinin korunması alanında aktif olan, kâr amacı gütmeyen bir kuruluşa şikayeti kendi adına yapması için yetki verebilir. Bu durumda yetki alan organ idari başvuru yollarında veri sahibine tanınan hakları kendi adına kullanma ve tazminat alma hakkını kullanma yetkisine sahip olur. Ayrıca üye devletler de veri sahibinin verdiği yetkiden bağımsız olarak, bu kuruluşun ihlale konu işleminin gerçekleştiği üye devlette yetkin olan denetim makamına şikayette bulunma konusunda yetkilendirebilir.

¹⁷⁹ Dülger (GDPR Bağlamında Kişisel Veriler), s.163.

2. İdari Para Cezası

GDPR'nin 83. maddesine göre denetim makamlarının kişisel verilere yönelik ihlal tespit ettikleri durumlarda etkili, ölçülü ve caydırıcı nitelikte idari para cezası kesme yetkisi bulunmaktadır. Bu cezanın miktarı her durumun özelliğine göre belirlenir. Denetim makamları bir veri işleme faaliyetinin idari para cezası gerektirip gerektirmediğine, verilecek para cezasının miktarına ilgili işleme faaliyetinin mahiyeti, kapsamı veya amacı dikkate alındığında ihlalin ciddiyeti ve süresinin yanı sıra etkilenen veri sahibi sayısı ve veri sahiplerinin yaşadığı zarar düzeyini dikkate alarak belirler. Ceza miktarının belirlenmesinde ihlalin kasıtlı veya ihmalkarlık kaynaklı olup olmadığı, veri sahiplerinin yaşadığı zararın azaltılması için veri sorumlusu veya veri işleyen tarafından gerçekleştirilen herhangi bir işlem olup olmadığı, veri sorumlusu veya veri işleyenin sorumluluk derecesi, veri sorumlusu veya veri işleyenin geçmişte konuyla ilgili ihlali olup olmadığı, ihlalin düzeltilmesi ve olumsuz sonuçlarının azaltılması amacı ile denetim makamı ile gerçekleştirilen işbirliğinin ne düzeyde olduğu gibi hususlar da etkilidir.

Bir veri sorumlusu veya veri işleyenin aynı veya bağlantılı işleme faaliyetlerine yönelik GDPR'nin çeşitli hükümlerini kasıtlı olarak veya ihmalkarlıktan dolayı ihlal etmesi durumunda, verilecek toplam idari para cezası meblağı en ağır ihlal için belirtilen meblağı aşamaz.

Çocuklara ait kişisel verilerin işlenmesinde rıza koşulları, veri sahibinin kimliğinin tespit edilmesini gerektirmeyen işleme faaliyetleri, veri sorumlusunun işleme faaliyetinde yerine getirmek zorunda olduğu yükümlülükler, GDPR'ye uygun işleme yapıldığını gösteren belgelendirme faaliyetleri konularıyla ilgili ihlallerin meydana gelmesi durumunda 10.000.000 Euro'ya kadar idari para cezası verilebilir. Eğer söz konusu ihlalleri gerçekleştiren bir işletme ise bir önceki mali yılın yıllık dünya çapındaki cirosunun %2'sine kadar idari para cezasına karar verilmesi mümkündür. Bu durumda verilebilecek olan iki idari para cezası miktarından hangisi yüksekse ona hükmedilir.

Veri işleme faaliyetine dair temel ilkelere, işlemenin hukuka uygunluk hallerine, veri sahibinin rızasına yönelik hükümlere, hassas verilerin işlenmesine, veri sahibinin işleme kapsamında sahip olduğu haklara, kişisel verilerin Avrupa

Birliđi dıřındaki bir lkeye aktarılması kurallarına, ye devlet hukukuna gre ngrlen zel iřleme hallerine, denetim makamının bir emrine aykırı hareket edilmesi halinde 20.000.000 Euro'ya kadar idari para cezası uygulanabilir. Sz konusu ihlalleri gerekleřtirenin bir iřletme olması halinde bir nceki mali yılın yıllık dnya apındaki cirosunun %4'ne kadar idari para cezasına karar verilebilir. Bu durumda verilebilecek olan iki idari para cezası miktarından hangisi ykseke ona hkmedilir.

ye devletler denetleme makamlarının yetki sınırlarına girmemek kaydıyla, kamu kuruluřları ve organlara idari para cezalarının kesilip kesilemeyeceđine ve ne lde kesileceđine iliřkin kurallar belirleyebilir.

Denetim makamının idari para cezasına hkmetme yetkisine karřı yargı yolu aıktır.

ye devletin hukuk sisteminde idari para cezalarına iliřkin dzenleme olmadıđı takdirde, idari para cezasına denetim makamı tarafından bařlatılan prosedr zerine ulusal mahkemeler tarafından hkmedilir.

*GDPR ile idari para cezalarının bu derece yksek seviyelere ykseltilmesi ilk etapta byk tartıřmalara yol amıřtır. Ancak bu tartıřmalar yapılırken, kiřisel verilerin, demokratik toplum yařamının olmazsa olmazlarından biri olan temel hak ve zgrlkler bađlamında hazırlanarak Lizbon Antlařması'na atıf yoluyla dahil edilip Avrupa Birliđi hukukunda kurucu antlařmalar dzeyine ykselen Avrupa Temel Haklar řartı kapsamında tanınarak koruma altına alındıđı unutulmamalıdır. Bu sebeple kiřisel verilerin, uyumlu yasalar ve gl yaptırımlar kapsamında, Birlik dzeyinde eřit ve yksek korumadan yararlanmaları, Birlik'in etik deđerlerinin dayandıđı temel hakların korunmasının glendirilmesi bađlamında, sosyal ve toplumsal geliřim bakımından nemli olduđu gibi, bu yolla gerek ve tzel kiřiler bakımından oluřturulacak gven ortamının Avrupa dijital tek pazarında iřlem hacminin artırılmasına yardımcı olarak, ekonomik bymeye katkıda bulunması bakımından da nemlidir*¹⁸⁰.

B. Hukuki Yaptırımlar

GDPR'nin 82. maddesine gre, kiřisel verilerinin korunması hakkı ihlal edilen herhangi bir kiři maddi veya manevi zararını karřılamak amacıyla veri sorumlusu veya veri iřleyenden tazminat alma hakkına sahiptir. Veri iřleme faaliyeti srecinde etkin olan herhangi bir veri sorumlusu GDPR'yi ihlal ettiđi takdirde iřleme faaliyetinin yarattıđı zarardan sorumludur. Veri iřleyen de GDPR'nin veri iřleyenlere

¹⁸⁰ imen Bulut, s. 138.

yönelik hükümlerine aykırı davrandığı ve veri sorumlusunun talimatlarına aykırı hareket ettiği hallerde, işlemenin yarattığı zarardan dolayı sorumludur. Veri sorumlusu ve veri işleyen ancak zararı doğuran işleme faaliyetinde hiçbir sorumluluğunun olmadığını kanıtlaması halinde tazminat yükümlülüğünden kurtulur.

Bir veri işleme faaliyetinde birden fazla veri sorumlusu ve veri işleyenin müdahalesi söz konusuysa, kişisel verilerin korunması hakkı ihlal edildiği takdirde, her veri sorumlusu ve veri işleyen tüm zarardan sorumludur. Bu durumda sürecin parçası olan bir veri sorumlusu veya veri işleyenin zararı eksiksiz bir şekilde tazmin etmesi halinde, sürece müdahil olan diğer veri sorumlusu ve veri işleyenlerden sorumlulukları oranında tazminat talep hakları bulunmaktadır. GDPR'nin etkili bir hukuki düzenleme olabilmesi için GDPR'nin hükümlerini ihlal eden tarafların bu ihlal sonucunda yarattıkları zararı gidermeleri yani sorumluluk ve tazminat kurumlarının yerleşmesi gerekmektedir¹⁸¹.

C. Cezai Yaptırımlar

İdari para cezasına tabi olmayan kişisel veri ihlalleri ve GDPR'ye yönelik diğer tüm ihlaller açısından cezalara ilişkin kuralları üye devletler belirler. Ayrıca üye devletler bu cezai tedbirlerin uygulanması için gereken tüm tedbirleri alır. Belirlenen cezai tedbirlerin caydırıcı ve etkili olması gerekmektedir.

GDPR'nin 84. maddesine göre üye devletlere kişisel verilerin korunması alanında cezai yaptırımlar öngören bir kanun düzenlenmesi ve bu kanunun 28 Mayıs 2018 tarihine kadar Komisyon'a bildirilmesi yükümlülüğü getirilmiştir.

V. AVRUPA BİRLİĞİ'NDE ÖNCÜ ÜLKELER BAZINDA KİŞİSEL VERİLERİN KORUNMASI HUKUKU: ALMANYA VE FRANSA ÖRNEĞİ

Avrupa Birliği, ekonomik bir birlik olarak kurulduğu dönemden bu yana gelişmesini hızla sürdürürken, üye ülkeler arasındaki siyasi bütünlük de ilerlemiştir. Kişisel verilerin kullanımının gelişen teknoloji ile birlikte artması, Birlik içinde ilerleyen siyasi bütünlük ile birlikte ülkelerin münferit konusu olmaktan çıkmış,

¹⁸¹ Tolun vd., s. 134.

Avrupa Birliđi içinde önem kazanmıřtır. Avrupa Birliđi, kurulma ve gelişme sürecinde kişisel verilerin korunması için çeřitli düzenlemeler yapmıřtır. Bunun yanı sıra üye ülkeler de gerek Birlik bazında yapılan düzenlemelerin getirdiđi zorunluluklar, gerek kişisel verilerin münhasır alanda korunma ihtiyacının meydana gelmesiyle birlikte kendi bünyelerinde çeřitli mevzuat çalışmaları yapmıřtır.

“Avrupa içerisinde ve uluslararası sistemde gerçekleşen paralel krizler, Almanya’yı krizlere yanıt vermede yetersiz kalan AB’nin dış ve güvenlik politikasını yönetmeye ve Avrupa’nın yeni siyasi motoru olmaya zorlamıřtır.”¹⁸² Bu krizleri yönetmek adına siyasi alanda güçlenen Almanya, siyasetle birlikte hukuk sisteminde de öncü düzenlemeler yaparak Avrupa Birliđi içinde lokomotif ülkelerden biri haline gelmiřtir.

Avrupa bütünleşmesinin öncül aktörlerinden birisi olan Fransa, 1950’lerden bu yana Avrupa entegrasyonu projesinin siyasi-diplomatik lideri olarak öne çıkmıř, Almanya ise daha çok ekonomik alanda Avrupa’nın en büyük gücü olarak ilerleyen yıllarda kendisini kabul ettirmiřtir. Fransa-Almanya ikilisi, zaman zaman yaşadıkları anlaşmazlıklara rağmen, uyumlu birlikteliklerini bugüne kadar sürdürmüş ve Avrupa Birliđi projesinin derinleşmesine ve Avrupa Birliđi’nin genişlemesine birlikte büyük katkıda bulunmuşlardır. Günümüzde dünyanın en gelişmiş demokrasileri ve en rekabetçi ve müreffeh ekonomilerinin çoğunun Avrupa kıtasında ve Avrupa Birliđi içerisinde olduđu da düşünülürse, Fransız-Alman tandeminin ve genel olarak Avrupa Birliđi projesinin başarısı ortadadır”¹⁸³.

Almanya ve Fransa’nın Avrupa Birliđi’nin gerek siyasi gerek ekonomik bütünlüğünde bu denli öne çıkması hukuki alandaki düzenlemelerde de öncü rol oynamasını sağlamıřtır. Biz de bu nedenle çalışmamızda kişisel verilerin korunmasının Avrupa Birliđi’ndeki örneklerini anlatırken iki lokomotif ülke olarak Almanya ve Fransa örneklerini ele aldık.

A. Almanya’da Kişisel Verilerin Korunması

Kişisel verilerin önemini ortaya çıkaran konu, Almanya’da federal hükümetin 1983 yılında nüfus sayımını planlaması olmuřtur. Ancak Alman halkı içerisinde böyle bir sayımın gözetlenme ve haksız mahremiyet ihlaline neden olacağını

¹⁸² Can Büyükbay, “Almanya’nın AB İçerisindeki Rolü: Uluslar arası Krizler Bağlamında Dış Politikada Süreklilik ve Deđişim”, **Ege Stratejik Arařtırmalar Dergisi**, Cilt: 8, Sayı:1, 2017, s.19.

¹⁸³ Ozan Örmeci, “Fransa’nın Avrupa Birliđi Politikası”, Ağustos 2018, <http://politikaakademisi.org/2018/08/18/fransanın-avrupa-birligi-politikasi/> (10.07.2021).

düşünenlerin rahatsızlığı da sayımla birlikte gündeme gelmiştir. Halkın bu duyguları hararetli bir boykota neden olmuş ve Federal Alman Anayasa Mahkemesi'nde sayım kararının iptali için dava açılmıştır. Bunun üzerine Federal Mahkeme Aralık 1983 tarihli ve 1 BVR 209/83 sayılı kararıyla nüfus sayımını anayasaya aykırı bulmuş ve geçici olarak iptaline karar vermiştir. Bu kararıyla birlikte Federal Mahkeme, Alman hukukunda veri korumanın yasal dayanağını oluşturacak olan yeni bir temel hak olarak “bilgisel kendi kaderini tayin hakkını” ortaya koymuştur. Bu karar, Almanya kişisel verilerin korunması hukuku tarihinde en önemli karar olarak kabul edilmektedir ve Federal Mahkeme, önüne gelen uyuşmazlıklarda hâlâ bu kararı göz önüne almayı tercih etmektedir¹⁸⁴.

Federal Alman Mahkemesi'nin verdiği bu kararın akabinde Alman halkının kişisel verilerin korunmasına yönelik taleplerinin devam etmesi üzerine ilk kez 1990 yılında Almanya'da federal boyutta kişisel verilerin korunması hakkında bir kanun kabul edilmiştir. Kanun, kişisel verilerin korunması alanında yaşanan gelişmeler neticesinde 2009 ve 2010 yıllarında değişikliğe uğramıştır¹⁸⁵. Kişisel verilerin korunması alanında Birlik boyutunda yaşanan gelişmeler doğrultusunda Almanya da iç hukukunda kişisel verilerin korunması kanununda değişikliğe gitmiş ve 2017 yılında Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz – BDSG) yürürlüğe girmiştir. Federal Veri Koruma Kanunu, Alman eyaletlerinin veri koruma yasalarının öncelikli olmadığı durumlarda federal kamu kurumları veya eyaletlerin kamu kurumları tarafından veri işleme ve özel kurumlar tarafından veri işleme konularında uygulanır. Bunun yanı sıra, her Alman eyaletinin, kişisel verilerin eyalet yetkilileri tarafından işlenmesi için kendi veri koruma yasası vardır¹⁸⁶.

Dört bölümden oluşan Federal Veri Koruma Kanunu'nun ilk bölümünde ortak hükümler ele alınırken, ikinci bölümde Genel Veri Koruma Tüzüğü'nün kapsamı uyarınca veri işlemenin uygulamaya yönelik hükümleri yer almaktadır. Üçüncü bölümde ise Genel Veri Koruma Tüzüğü'nün konusu uyarınca veri

¹⁸⁴ Gerrit Hornung, Christoph Schnabel, “Data Protection In Germany I: The Population Census Decision And The Right To Informational Self-Determination”, **Computer Law& Security Report**, Cilt:25, Sayı: 1, 2009, s. 84-85.

¹⁸⁵ Göçmen Uyarer, s.83. Almanya'da kişisel verilerin korunması alanında ilk kanun Hessen Eyalatı'nda 1970 yılında kabul edilmiştir. Develioğlu, s.5.

¹⁸⁶ Data Protection and Cybersecurity Laws in Germany, <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/germany> (23.05.2021). Bunun yanı sıra Almanya'da, Alman Ceza Kanunu'nun özel hayatın gizliliğine karşı işlenen suçları düzenleyen bölümünde kişisel verilerin korunmasına karşı işlenen suçlar da yer almaktadır. Göçmen Uyarer, s. 84.

işlemenin uygulama hükümleri düzenlenmiştir. Dördüncü ve son bölümde ise özel hükümlere yer verilmiştir.

Kanun'un başlangıç hükümleri, Kanun'un kapsamını ve uygulama alanını düzenlemektedir. Buna göre Kanun federasyonun, eyaletlerin kamu kurumlarında federal ve özel kurumlarda kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesine ve bir dosyalama sisteminin bir parçasını oluşturan kişisel verilerin işlenmesine uygulanır. Almanya'da diğer federe veri koruma mevzuatları Federal Veri Koruma Kanunu'na göre öncelikli olarak uygulanır. Federe veri koruma kanunlarında hüküm olmadığı takdirde Federal Veri Koruma Kanunu'nun uygulanması gerekmektedir. Burada Kanun'un özel kanun- genel kanun ayrımı yaptığını söylemek mümkündür.

Kanun'un, veri sorumlusu veya veri işleyenin işleme faaliyetini Almanya sınırlarında gerçekleştirdiği durumlarda veya işlemenin Almanya'daki bir kuruluşun faaliyetleri kapsamında yapılması halinde uygulanacağı düzenlenmiştir¹⁸⁷. Ancak Kanun'un hükümleri Avrupa Birliği hukukunun, özellikle de Genel Veri Koruma Tüzüğü'nün doğrudan uygulandığı durumlarda geçerli olmayacaktır. Kamu kurumlarının, veri sorumlusunun sorumlu olduğu görevi yerine getirmek için bir işlemenin gerekli olması halinde kişisel verileri işlemesine izin verileceği Kanun'un başlangıç hükümleri arasında yer almaktadır.

Federal Alman Veri Koruma Kanunu, halka açık alanların video kamera yöntemiyle gözlenmesine özel bir madde de içermektedir. Buna göre halka açık alanların video ile gözetlenmesi ancak kamu kurumlarının görevlerini yerine getirmeleri, erişime kimlerin izinli veya izinsiz olduğunun tespit edilebilmesi veya özel olarak tanımlanmış amaçlar doğrultusunda meşru çıkarları korumak için gerekli olduğu takdirde yapılabilir. Spor salonları, toplu kullanılan alanlar, alışveriş merkezleri, toplu ulaşım araçları gibi kamuya açık yerlerde video yöntemiyle izleme yapılabilmesi için toplumsal sağlığın veya özgürlüğün korunması gibi meşru menfaatlerin bulunması gerekmektedir. Ancak hangi hallerde, hangi amaç için toplanmış olursa olsun, veriler toplama amacı doğrultusunda artık ihtiyaç duyulmuyorsa derhal silinecektir.

¹⁸⁷ Schengen müktesebatının uygulanması ve geliştirilmesi ile ilgili devletler, Avrupa Birliği Üye Devletleri ile eşit statüye sahip olacaktır. Diğer devletler üçüncü ülkeler olarak kabul edilecektir. (Federal Alman Veri Koruma Kanunu madde 1/7)

GDPR ile hüküm altına alındığı üzere Federal Alman Veri Koruma Kanunu da veri koruma görevlisi atanmasını düzenlemiştir. Buna göre kamu kurumları bir veri koruma görevlisi atar. Kamu kurumları veri koruma görevlisini atamanın ardından, veri koruma görevlisinin kişisel verilerin korunması ile ilgili konulara uygun şekilde ve zamanda dahil olmasını da sağlar. Veri koruma görevlisi, veri koruma mevzuatından doğan yükümlülüklerin yerine getirilmesiyle ilgili kamu çalışanlarını bilgilendirir, kamu kurum ve kuruluşlarında kişisel verilerin işleme sürecine dahil olan personeli kişisel verilerin korunması hususunda yetiştirir ve denetim makamı ile işbirliği yapar¹⁸⁸.

Kanun'un 8. ve 16. maddeleri arasında Veri Koruma ve Bilgi Özgürlüğü Federal Komiserliği kurulması düzenlenmiştir. Federal Komiserlik, veri koruma konusunda ülke içindeki en yüksek otoritedir. Federal Komiser, kamu kurumlarının, kamu hukukuna tabi işletmelerin ve telekomünikasyon hizmetleri sağlayan işletmelerin denetimini yapar. Federal Komiser, GDPR'nin uygulanmasını sağlamak için kabul edilen kişisel verilerin korunması mevzuatının uygulanmasını izler ve kişisel verilerin işlenmesiyle ilgili riskler, kurallar ve güvenceler konusunda kamuoyunu bilgilendirir. Alman Federal Meclisi'ne, Federal Hükümet'e ve diğer kamu kurumlarına kişisel veriler işlenirken temel hak ve özgürlüklerin korunmasına ilişkin yasal tedbirler konusunda tavsiyelerde bulunur. Yalnızca bu düzenleme dahi, Almanya'da kamu kurum ve kuruluşları ile hükümetin kişisel verilerin korunması hukukuna riayet etmesine ne denli önem verildiğini göstermektedir¹⁸⁹.

Federal Veri Koruma Kanunu, hassas verilerin işlenmesini özel bir başlık altında düzenlemiştir. Kanun hassas verileri kamu kurumlarının hassas verileri işlemesi ve özel kuruluşların hassas veriler işlemesi olarak ikiye ayırırken, kamu kurumlarına, özel kuruluşlara nazaran daha fazla hassas veri işleme imkanı sağlamıştır. Buna göre hem kamu kurumları hem özel kuruluşlar sosyal güvenlik ve sosyal koruma hakkından kaynaklanan hakları kullanmak için işlemenin gerekli olması, koruyucu hekimlik amaçları, çalışanın çalışma kapasitesinin

¹⁸⁸ Veri sahipleri, kişisel verilerinin işlenmesi ve veri koruma mevzuatı kapsamındaki haklarının kullanılması ile ilgili tüm konularda veri koruma görevlisi ile iletişime geçebilir. Veri koruma görevlisi, ilgili kişi tarafından bu yükümlülükten muaf tutulmadıkça, veri sahiplerinin kimliğine ve veri sahiplerinin belirlenmesini sağlayan koşullara ilişkin gizlilikle bağlıdır. (Federal Veri Koruma Kanun madde 6/5).

¹⁸⁹ Gömen Uyarer, s. 86.

değerlendirilmesi, tıbbi teşhis, sağlık veya sosyal bakım veya tedavi sağlanması, halk sağlığı alanında kamu yararı nedenleriyle işlemenin gerekli olması ve önemli kamu yararı nedenleriyle işlemenin acilen gerekli olması gibi nedenlerin varlığı halinde hassas verileri işleyebilir.

Kişisel verilerin kamu kurumları tarafından kamu kurumlarına aktarılması hususunda, aktaran kuruluşun veya verilerin aktarıldığı üçüncü kişinin görevlerini yerine getirmesi için gerekli olması ve işlenmesine izin verecek şartların yerine getirilmesi halinde izin verileceği düzenlenmiştir. Verilerin aktarıldığı üçüncü kişi, aktarılan verileri yalnızca aktarıldığı amaç için işleyebilir. Bunun yanı sıra kamu kurumlarının aktarımın gerekli olması halinde verilerin aktarıldığı üçüncü kişinin, aktarılan verilerle ilişkin bilgisine ilişkin meşru bir menfaat sunması ve veri sahibinin verilerin aktarılmaması konusunda meşru bir menfaatinin bulunmaması, yasal iddiaların oluşturulması, uygulanması veya savunulması için işlemenin gerekli olması hallerinde kişisel verileri özel kuruluşlara aktarabileceği düzenlenmiştir.

Kanun'un 26.ve 31. maddeleri arasında kişisel verilerin özel işleme halleri düzenlenmiştir. Buna göre kişisel veriler işe alımlarda, bilimsel ve tarihi araştırmalar ile istatistiksel hesaplamalarda, kamu yararına arşivleme amaçlarıyla, tüketici kredisi kullanımında işlenebilir. Çalışanların kişisel verileri, işe alım kararları veya işe alındıktan sonra, iş akdinin ifası, feshi veya kanunla veya toplu sözleşmelerle belirlenen çalışanların temsili hak ve yükümlülüklerini yerine getirmek amacıyla işlenebilir. Çalışanların kişisel verileri, yalnızca ilgili kişinin çalışırken bir suç işlediğine inanmak için belgelenmiş bir neden varsa, bu tür verilerin işlenmesi suçun araştırılması için gerekliyse ve veri sahibinin meşru menfaatinden ağır basmıyorsa, suçları tespit etmek için işlenebilir

Federal Veri Koruma Kanunu ile veri sahibinin haklarına değinilmiştir. Veri sahibinin bilgi edinme hakkı, verilerine erişim hakkı, unutulma hakkı, itiraz hakkı bulunmaktadır. Veri sahibinin bilgi alma hakkı kapsamında veri sorumlusu işlemenin amaçları, kişisel verilerinin işlenmesine ilişkin erişim, düzeltme, silme ve işlemenin kısıtlanması hakları olduğuna dair bilgilendirme yapmalı, veri sorumlusunun ve veri koruma görevlisinin isimleri ve iletişim bilgileri veri sahibiyle paylaşmalıdır. Veri sahibi, kendisiyle ilgili doğru olmayan verilerin düzeltilmesinin gecikmeksizin sağlanacağı güvencesine sahiptir.

Veri sahibine tanınan haklarla birlikte veri sorumlusu ve veri işleyene bir takım yükümlülükler de getirilmiştir. Veri sorumlusu ve veri işleyen de sürekli olarak otomatik işleme ile uğraşan en az 20 kişiyi istihdam ediyorsa bir veri koruma görevlisi atamakla yükümlü kılınmıştır. Veri sorumlusu kendi adına veri işleme faaliyetini bir başka veri sorumlusuna devretti ise kişisel verilerin korunması mevzuatına uygun işleme yapıldığını denetlemek zorundadır. Bunun yanı sıra veri sorumlusu ve veri işleyen uygulama maliyetlerini ve işlemenin niteliğini, kapsamını, bağlamını ve amaçlarını dikkate alarak özellikle hassas verilerin işlenmesiyle ilgili olarak riske uygun bir güvenlik düzeyini sağlamak için gerekli teknik önlemleri alır. Bir kişisel veri ihlali durumunda, veri sorumlusu derhal ve en geç ihlal tespit edildikten sonra en geç 72 saat içinde Federal Komiseri bilgilendirme yükümlülüğü altındadır. Bununla birlikte bir kişisel veri ihlalinin, gerçek kişilerin yasal olarak korunan çıkarları için önemli bir riskle sonuçlanması muhtemelse veri sorumlusu, veri öznesini kişisel veri ihlali konusunda gecikmeden bilgilendirecektir. Özellikle yeni teknolojilerin kullanıldığı ve işlemenin niteliği, kapsamı, bağlam ve amaçları dikkate alındığında bir işleme türünün, veri sahiplerinin yasal olarak korunan menfaatleri için önemli bir riske yol açmasının muhtemel olduğu durumlarda veri sorumlusu işlemeden önce, öngörülen işleme faaliyetlerinin veri sahipleri üzerindeki etkisinin bir değerlendirmesini gerçekleştirmek zorundadır.

Veri sorumlusu Federal Komiser ile işbirliği içinde hareket eder. Veri işleme faaliyetleri yerine getirilirken veri sorumlusu özellikle veri sorumlusunun ve veri koruma görevlisinin adı ile iletişim bilgilerini içeren kayıtları işlemenin amaçları ile birlikte yer vererek tutmak zorundadır. Bununla birlikte veri sorumlusu, hem işleme araçlarının belirlendiği esnada hem de işleme sırasında, yasal mevzuata uygunluğu sağlamak için veri minimizasyonu gibi veri koruma ilkelerini etkin bir şekilde uygulamak için uygun önlemleri alır.

Federal Veri Koruma Kanunu veri sorumlusuna işlenen verilerin kategorilere ayrılması yükümlülüğünü getirmiştir. Veri sorumlusu kişisel verileri işlerken, mümkün olduğunca farklı veri sahibi kategorileri arasında net bir ayırım yapmalıdır. Özellikle suç işlediklerine dair ciddi gerekçeler bulunan kişiler, hakkında bir suç işleyeceklerine inanmak için ciddi gerekçeleri bulunan kişiler ve bir suçtan hüküm giymiş kişiler ile ilgili veriler işlenirken bu ayırımın yapılması zorunludur.

Kanun 42. maddesinde kişisel veri ihlallerinde hapis cezası öngörmüştür. Kamuya açıklanmış olmayan kişisel verilerin veri sahibinden izin alınmadan üçüncü kişilere aktarılması veya ticari amaçlar için verilerin erişilebilir kılınması halinde üç yıla kadar hapis veya para cezası verileceği ifade edilmiştir. Kişisel verilerin yetkisiz olarak işlenmesi, sahtekarlıkla elde edilmesi ve bunun kendini veya bir başkasını zengin etme amacıyla yapılması halinde fail iki yıla kadar hapis veya para cezası ile cezalandırılır. Bu suçların takibi şikayete bağlı olmakla birlikte veri sahibi, veri sorumlusu, Federal Komiser veya denetim makamı şikayette bulunma hakkına sahiptir.

İdari para cezasına tabi olacak ihlaller de Kanun'un 43. maddesinde düzenlenmiştir. Veri sahibinin bilgi alma hakkına riayet etmemek, tüketiciyi bilgilendirmemek veya yanlış bilgilendirmek hallerinde bu eylemlerin kasıtlı veya ihmal yoluyla gerçekleştiğine bakılmaksızın, 50.000 Euro'ya kadar idari para cezası uygulanabilir.

Kanun'un 46. maddesi ile kişisel verilere ilişkin kişisel veri, işleme, işlemenin kısıtlanması, profil çıkarma, psödonimizasyon gibi temel kavramlar tanımlanırken 47. madde ile veri işlemenin temel prensipleri açıklanmıştır. Buna göre kişisel verilerin yasal ve adil bir şekilde, belirli açık ve meşru amaçlar için, sınırlı seviyede bilgi ile doğru ve gerektiğinde güncel olarak, işleme süresiyle sınırlı olarak saklanarak, yetkisiz işlemeye karşı uygun tedbirler alınarak işlenebileceği belirtilmiştir.

Kişisel verilerin rızaya dayalı olarak işlenmesi halinde veri sahibine tanınan olanaklar ayrı bir madde altında düzenlenmiştir. Kişisel veriler, rıza temelinde işleniyorsa, veri sorumlusu veri sahibinin rızasına ilişkin kanıt sunabilmelidir. Veri sahibinin rızasının başka hususları da içeren yazılı bir beyan kapsamında verilmiş olması halinde, muvafakat talebinin diğer hususlardan açıkça ayırt edilebilecek şekilde, anlaşılır ve kolay erişilebilir bir şekilde sunulması, açık ve sade bir dil kullanılması gereklidir. Veri sahibi, herhangi bir zamanda rızasını geri çekme hakkına sahiptir. Rızanın geri çekilmesi, geri çekilmeden önce rızaya dayalı işlemenin yasallığını etkilemeyecektir. Veri sahibi, onay vermeden önce bu konuda bilgilendirilecektir. Rıza, yalnızca ilgili kişinin özgür kararına dayandığında geçerli olacaktır. Rızanın serbestçe verilip verilmediği değerlendirilirken, rızanın verildiği

koşullar dikkate alınmalıdır. Veri sahibi, işlemenin amaçlanan amacı hakkında bilgilendirilir. Münferit durumda veya talep üzerine gerekirse, veri sahibi, rızanın geri alınmasının sonuçları hakkında da bilgilendirilecektir. Hassas veriler işlenecekse, rızanın bu verilere de açıkça atıfta bulunması gerekir.

Genel kapsamı itibarıyla açıklandığı üzere Federal Veri Koruma Kanunu pek çok maddede GDPR'yi izlemiş ancak kendine özgü bazı düzenlemeler ile veri koruma mevzuatına eklemeler de yapmıştır. Bunlardan biri olarak da Kanun, kişisel verilerin devlet ödülleri ve onurları için özel olarak işlenmesini de düzenlemiştir. Ödüller ve onurlar için hükümet prosedürlerini hazırlamak ve yürütmek için, hem sorumlu kuruluşlar hem de diğer kamu ve özel kuruluşlar, hassas veri kategorileri de dahil olmak üzere gerekli kişisel verileri işleyebilir.

GDPR'nin günümüzde hâlâ tam olarak anlaşılamadığı da düşünülmektedir. Zira Almanya'da, GDPR mevzuatının farklı yorumlarını takip eden 16 denetim makamı bulunmaktadır. Bu şekilde bir farklılığın olması da mahremiyetle ilgili konularda tavsiye vermeyi zorlaştırmaktadır. Bu nedenle Almanya'da denetim makamları bireylerin veri koruma haklarını kullanma sürecinde her zaman yer almayabilir. Bunun yerine, veri sorumlularına yönelik şikayetler önce şirket içi veri koruma görevlisine sunulmaktadır. Şirketin veri koruma görevlisi ile tatmin edici olmayan iletişim durumunda, denetim makamı ve hukuk mahkemelerine başvuru gündeme gelmektedir¹⁹⁰.

B. Fransa'da Kişisel Verilerin Korunması

Fransa İnsan Hakları Evrensel Beyannamesi, Avrupa İnsan Hakları Sözleşmesi ve Avrupa Birliği Temel Haklar Şartı'nı onaylayan ülkelerden birisidir. Bu yasal araçlar bir mahremiyet hakkını içermektedir. Fransız Anayasası özel hayatın gizliliğine ilişkin bir düzenleme barındırmamaktadır ancak özel hayatın gizliliği hakkı, 17 Temmuz 1970 tarihli Parlamento Yasası ile eklenen Fransız Medeni Kanunu'nun 9. Maddesinde yer almaktadır ve herkes kendi değerlerine, özel hayatına saygı gösterilmesi hakkına sahiptir. Özel hayatın yasal bir tanımı olmamasına rağmen, Fransız mahkemeleri özel hayatın bir kişinin aşk hayatını,

¹⁹⁰ Alan Charles Raul (Ed.), **The Privacy, Data Protection and Cybersecurity Law Review**, sixth edition, The Law Reviews, London, 2019, s.188.

arkadaşlıklarını, aile koşullarını, boş zaman faaliyetlerini, siyasi görüşlerini, sendika veya dini üyeliği ve sağlık durumunu içerdiği yönünde ilke kararlar vermiştir¹⁹¹.

Fransa’da kişisel verilerin korunması ilk olarak 1978 yılında Fransız Bilgi teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu ile düzenlenmiştir. Fransız Veri Koruma Kurulu olan CNIL da bu Kanun ile kurulmuştur¹⁹². Kanun günümüze değin değişikliklere uğramıştır. Bununla birlikte Fransız Hukukunda 95/46/CE sayılı Yönerge’nin hükümlerinin uygulanmasına ilişkin 2004-801 sayılı Kanun ve 2016/679’un sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü’ nün belirli hükümlerinin uygulanmasını öngören 2016-1321 sayılı Kanun yürürlüğe konarak kişisel verilerin korunması konusunda güncel gelişmeler mevzuata yansıtılmaya çalışılmıştır. Ancak en önemli değişiklik Fransız Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu’nu değiştiren ve GDPR’deki hükümlerin uygulanmasını hedefleyen 20 Haziran 2018 tarih ve 2018-493 sayılı Kanun ile yapılmıştır. 2018-493 Sayılı Fransız Veri Koruma Kanunu olarak da adlandırılan bu Kanun ulusal hukukun GDPR ile uyumluluğunu yasama düzeyinde tamamlamıştır¹⁹³.

Fransa’da bilgi teknolojisinin özel bir önem verilmiş ve bu husus 1978 tarihli Fransız Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu ile koruma altına alınmıştır. Günümüz gelişmelerine uyarlanarak geçerliliğini koruyan Kanun’un 1. maddesi bilgi teknolojilerini her vatandaşın hizmetine tahsis ederek bilgi teknolojilerinin gelişimini uluslar arası işbirliğine bağlamıştır¹⁹⁴. Bununla birlikte Kanun’un hangi veriler için uygulanacağı da başlangıç hükümlerinde ele alınmıştır. Buna göre Fransız Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu kişisel verilerin otomatik olarak işlenmesinin yanı sıra, bir kişisel veri dosyalama sisteminde yer alan kişisel verilerin otomatik olmayan şekilde işlenmesi için geçerlidir.

¹⁹¹ Bart Custers et al, **EU Personal Data Protection in Policy and Practice**, Springer, The Hague, 2019, s.137.

¹⁹²Göçmen Uyarer, s.78. Kurul, veri işlemenin Fransız Veri Koruma Hukuku’na uygun gerçekleşmesini sağlamakla yükümlüdür. Bilgi sistemleri otoritelerinin talepleri ile ilgili çalışmalar yapar ve bu konuda kararlar alır. Oğuz, s.13.

¹⁹³ Benjamin May, Farah Bencheliha, “Data protection and privacy in France” <https://www.lexology.com/library/detail.aspx?g=eea3a783-f360-469d-986f-9434a7893c7f> (13.06.2021)

¹⁹⁴ Uluslar arası işbirliği içerisinde gerçekleşen bilgi teknoloji hizmeti insan kimliğini, insan haklarını, mahremiyeti, bireysel veya kamusal özgürlükleri ihlal edemez. (Fransız Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu, madde 1)

Fransa’da kişisel veri bir kimlik numarasına, kendilerine özgü bir veya daha fazla faktöre atıfta bulunularak doğrudan ve dolaylı olarak kimliği tespit edilen veya edilebilecek gerçek bir kişiye ilişkin her türlü bilgi anlamına gelmektedir. Bir kişinin tanımlanabilir olup olmadığının tespiti için veri sorumlusunun veya başka bir kişinin kullandığı ve erişebileceği tüm araçlar dikkate alınmalıdır¹⁹⁵. Veri sorumlusunun Fransa topraklarında yerleşik olması, Fransa ve diğer Avrupa Birliği ülkelerinden birinde yerleşik olmamasına rağmen Fransa’da veya diğer Avrupa Birliği ülkelerinin herhangi birinde bulunan işleme araçlarını kullanması halinde uygulanır.

Kişisel verilerin işlenmesi ile ilgili kurallar GDPR’de belirtilenler olarak belirlenmiş ve Kanun da bu ilkelere de yer verilmiştir. Buna göre veri işleme adil olmalı ve veri dosyalama sistemindeki veriler yasal yollarla elde edilmelidir¹⁹⁶. Veriler, belirli, açık ve meşru amaçlar için elde edilmeli ve daha sonra bu amaçlarla bağdaşmayan bir şekilde işlenmemelidir. Yine veriler doğruluk ilkesi gereğince doğru ve eksiksiz olmalı, gerektiğinde güncel tutulmalıdır. Elde edilme ve işleme amaçlarına göre yanlış ve eksik olan verilerin silinmesi ve düzeltilmesi gerekmektedir. Kişisel veriler, elde edilme ve işleme amaçları için gerekli olan süre boyunca saklanmalıdır.

Kişisel verilerin işlenmesinde hukuka uygunluk nedenleri Kanun’un ikinci bölümünde Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Şartları Başlığı altında düzenlenmiştir. Buna göre; GDPR ile benzer şekilde kişisel verilerin işlenmesinde asıl olan veri işlemenin hukuka aykırılığıdır. Ancak belli hallerin varlığı halinde veri işleme hukuka uygun hale gelir. Veri işlenmesine veri sahibinin rıza göstermesi, veri sorumlusunun tabi olduğu bir yasal zorunluluk, veri sahibinin hayatının korunması, veri sorumlusunun bir kamu hizmeti görevini yerine getirmesi, veri sahibinin taraf olduğu bir sözleşmenin ifası ve veri sahibinin çıkarları ile ters düşmediği takdirde veri sorumlusunun meşru menfaatinin gözetilmesi kişisel verilerin işlenmesinde hukuka uygunluk nedenleridir.

¹⁹⁵ Fransız hukukunda kişisel verilerin işlenmesi kullanılan mekanizma ne olursa olsun, özellikle elde etme, kaydetme, düzenleme, saklama, kullanma, verilerle ilgili herhangi bir işlem veya işlem dizisi yapma anlamına gelmektedir. (Fransız Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu madde 2)

¹⁹⁶ Kişisel veri dosyalama sistemi, Fransız Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu’ nun 2. maddesinde belirli kriterlere göre erişilebilen herhangi bir yapılandırılmış ve istikrarlı kişisel veri seti olarak tanımlanmaktadır.

Fransız Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu'nun 8. maddesinde hassas veriler düzenlenmiştir. Hassas veri düzenlemesi içinde kişilerin ırk ve etnik kökenlerini, siyasi, felsefi, dini görüşlerini veya sendika üyeliğini doğrudan veya dolaylı olarak ortaya çıkaran, sağlıklarını, cinsel yaşamlarını ilgilendiren kişisel verilerin toplanması ve işlenmesi yasak olarak kabul edilmiştir. Hassas verilerle ilgili düzenlemenin devamında hassas verilerin işlenmesine ilişkin istisnalara yer verilmiştir. Buna göre veri sahibinin açık rızası, işlemenin hayati olduğu durumlarda veri sahibinin insan rızasının açıklayamayacak durumda olması, bir dernek veya kâr amacı gütmeyen diğer herhangi bir dini, felsefi, siyasi veya sendika kuruluşu tarafından gerçekleştirilen işlemlerde dernek veya kuruluşun amacına karşılık gelen verilerin işlenmesi, veri sahibinin kamuya açıkladığı kişisel verilerle ilgili işleme, koruyucu hekimlik, tıbbi teşhis veya tedavi sağlanması için gerekli olan işleme, istatistiki faaliyetler için işlemlerde hassas verilerin işlenmesinin hukuka uygun olduğu düzenlenmiştir¹⁹⁷.

Fransız Veri Koruma Hukuku'nda 1978 tarihli Fransız Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu ile kurulan Fransız Veri Koruma Kurulu CNIL önemli bir yer tutmaktadır. Kanun'un 11. maddesine göre CNIL, bağımsız bir idari otoritedir. CNIL, Fransız hukukunun uzun süren tartışmalar neticesinde ortaya çıkan ilk bağımsız idari otoritesidir¹⁹⁸. CNIL'ın temel görevleri tüm veri sahiplerini ve veri sorumlularını kişisel verilerle ilgili bilgilendirmek, sıklıkla işlenen kişisel veri kategorilerinin tabi olacağı kuralları belirlemek, gerekli durumlarda kişisel verilerle ilgili yönetmelik yayımlamak, izne tabi olarak işlenen kişisel veriler için izin vermek, devlet güvenliğine ilişkin bilgilere erişim taleplerine yanıt vermek, veri işleme faaliyetlerine ilişkin şikayetleri incelemek olarak sıralamak mümkündür.

Fransız Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu'na göre kişisel verilerin otomatik yollarla işlenmesinin CNIL'e bildirilmesi gerekmektedir. Bildirim, işlemenin kanuni yükümlülüklerle uygun yapıldığını

¹⁹⁷ İstisnai durumların varlığı haricinde hassas veriler, CNIL'in onayladığı bir anonimleştirme prosedürü doğrultusunda işleme kategorilerine göre işlenebilir. Kişisel verilerin tıbbi araştırma amacıyla işlenmesi, kişisel tıbbi verilerin bakım ve önleme uygulamalarının değerlendirilmesi amacıyla işlenmesi halleri ise anonimleştirme prosedürünün dışında kalmaktadır. (Fransız Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu madde 8)

¹⁹⁸ Çağla Tansuğ, "Fransız Hukukunda Kişisel Verileri Koruma Otoritesi: CNIL" **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:14, Sayı:2, 2017, s. 342.

gösteren bir taahhüt içermesi gerekmekte olup elektronik yolla da bildirim yapılması mümkündür.

GDPR’de olduğu gibi Fransız Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu da veri sorumlusu ve veri işleyene, veri sahibini bilgilendirme yükümlülüğü getirmiştir. Buna göre veri sorumlusu ve veri işleyen, veri sahibine veri sorumlusunun ve temsilcisinin bilgilerini vermek, verilerin işleme amaçlarını, verilerin paylaşılacağı kişileri, verilerin işlenmesiyle ilgili veri sahibinin haklarını açıklamak zorundadır. Bununla birlikte veri sorumlusu, verilerin niteliğine ve işlemenin risklerine ilişkin olarak, verilerin güvenliğini korumak ve özellikle bunların değiştirilmesini, zarar görmesini veya yetkisiz üçüncü şahıslar tarafından erişimini önlemek için tüm yararlı önlemleri almak zorundadır.

Alınan tüm önlemlere rağmen, veri ihlali yaşanması halinde veri sorumlusu derhal CNIL’ı bilgilendirir. Söz konusu ihlalin kişisel veri güvenliğini veya bir abonenin veya başka bir bireyin gizliliğini ihlal etmesi muhtemel olduğunda, veri sorumlusu, veri sahibini de derhal bilgilendirecektir. Bununla birlikte CNIL, kişisel verilerin yetkisiz kişilerce deşifre edilemez hale getirilmesini sağlamak için veri sorumlusu tarafından uygun koruma önlemlerinin uygulandığını tespit ederse, etkilenen tarafa kişisel verilerin ihlalinin bildirilmesi gerekmeyecektir. Ancak CNIL, ihlalin ciddiyetini araştırdıktan sonra, veri sorumlusuna, veri sahibini bilgilendirmek için resmi bir bildirimde bulunabilir.

Veri sorumlusunun yükümlülükleri ile birlikte, veri sahibine de bir takım haklar tanınmıştır. Buna göre, herhangi bir gerçek kişi meşru gerekçelerle, kendisiyle ilgili herhangi bir verinin işlenmesine itiraz etme hakkına sahiptir. Veri sahipleri kendileriyle ilgili verilerin, özellikle ticari amaçlarla mevcut veya daha sonraki bir veri işlemenin denetleyicisi tarafından kullanılmasına itiraz edebilir. Bununla birlikte veri sahibi olan herkes, kimliğini ispatlamak kaydıyla kişisel verilerinin işlenip işlenmediğini, kişisel verilerini işleme amaçlarını ve uygulanan veri kategorilerini, otomatik işlemeye dayalı olarak alınan bir karar ve otomatik işlemenin içerdiği mantığı öğrenme hakkına sahiptir. Ancak, veri sahibine iletilen bilgiler, telif hakkını olumsuz etkilememelidir. Veri sahipleri, istekleri üzerine kişisel verilerin bir kopyasını alabilir. Kişisel verilerin gizlenmesi veya kaybolması riskinin ortaya çıkması halinde, yetkili yargıç, kısa yargılama yoluyla dahi, bu gizlenme veya

kaybolmayı önlemek için gerekli tüm tedbirlere karar verebilir. Veri sahibi, veri sorumlusundan kendisiyle ilgili yanlış, eksik, belirsiz, süresi dolmuş veya toplamı, kullanımı, ifşası olan kişisel verileri düzeltmesini, tamamlamasını, güncellemesini, engellemesini veya silmesini isteyebilir. Veri sorumlusu, veri sahibinin bu talebini ücretsiz olarak yerine getirmelidir. Uyuşmazlık halinde ispat yükü, itiraz edilen verilerin ilgili kişi tarafından veya rızasıyla açıklandığının tespit edildiği durumlar dışında, erişim hakkının kullanıldığı veri sorumlusuna aittir.

CNIL, tüm yetki ve görevlerinin yanı sıra bu yetki ve görevlerini etkili bir şekilde yerine getirmesini sağlayan bir yaptırım gücüne sahiptir. Bu bağlamda CNIL, mevzuat kapsamındaki yükümlülüklerini ihlal eden bir veri işleyici veya veri sorumlusuna uyarı, işleme faaliyetinde geçici veya kesin bir sınırlama, işleme yasağı veya verilen bir yetkinin geri alınması gibi yaptırımlar uygulayabilir. Bununla birlikte, işleme faaliyetlerinin mevzuata aykırı olarak devam ettiği her gün için 100.000 Euro'yu aşmayan bir ceza ile birlikte bir ihtiyati tedbir uygulama, üçüncü bir ülkedeki bir alıcıya veya uluslararası bir kuruluşa veri akışını askıya alma emri verme, bağlayıcı kurumsal kuralları onaylayan bir kararın kısmen veya tamamen askıya alınması yetkisine sahiptir. CNIL, ihlal durumuna göre 10 milyon Euro veya bir teşebbüsün önceki mali yıla ait dünya çapındaki toplam yıllık cirosunun %2'si veya 20 milyon Euro veya bir teşebbüsün önceki mali yılda dünya çapındaki toplam yıllık cirosunun %4'ü oranında ceza kesebilir. Bu seçimlik oranlar arasında daha yüksek olan baz alınarak ceza uygulanır.

Teknolojik değişimlerin hızlı yaşanmasıyla birlikte ortaya çıkan bilgisel dolaşım Fransa'yı da etkilediğinden, geçmişten günümüze veri koruma mevzuatında güncellemelere gidilmiştir. Bu gelişmeler neticesinde Fransız veri koruma hukuku GDPR'ye uyumlu hale getirilmiştir.

SONUÇ

1900'lü yılların ikinci yarısından itibaren teknolojiye yaşanan gelişmeler neticesinde toplumsal açıdan hızlı ilerlemeler yaşanmış ve insanlık için pek çok hizmet alanında kolaylıklar sağlanmıştır. Teknolojinin getirdiği imkanlar sayesinde insanlar tek tuşla bulundukları yerden başka yerdeki insanlarla iletişim kurabilmeye, anlık olarak görüntülerini kaydetmeye, paylaşmaya, tek tuşla bankacılık, alışveriş gibi tüm ihtiyaçlarını karşılamaya başlamışlardır. Bilgi teknolojilerinde yaşanan bu hızlı ilerlemelerle birlikte sağlanan kolaylıklara insanların gösterdiği talep, sonuç itibariyle yüksek miktarlarda verinin de toplanmasını beraberinde getirmiştir. İletişim teknolojilerine talebin artması kişisel verilerin her geçen gün biraz daha fazla üretilmesine ve toplanmasına neden olmaktadır. Hızla ucuzlayan ve daha çok kitleye ulaşabilir hale gelen teknolojiyle birlikte mahremiyetin korunması sorunu da ortaya çıkmaktadır.

Bir diğer yandan bakıldığında, kamu kurumlarının da içinde olduğu pek çok kurum ve kuruluş, bankalar, mağazalar ve şirketler bilgi teknolojilerini kullanarak aynı anda pek çok kişiye çok düşük maliyetlerle çok sayıda hizmet sunabilmekte ve bu sayede büyük oranda enerji ve zaman tasarrufu da sağlamaktadır. Teknolojinin getirdiği büyük miktardaki işlem hacmi ve hızı sayesinde milyarlarca veri tek tuşla Dünya'nın dört bir yanına aktarılabilir hale gelmiştir. Bu yönüyle değerlendirildiğinde kişisel verilerin işlenmesinin faydalı ve gerekli olduğunu söylemek mümkündür.

Temel haklardan olan özel yaşamın gizliliği içerisinde yer alan mahremiyet ve bilgisel anlamda kendi kaderini tayin hakkının korunması konusunda sorunlar da bu gelişmelerin yaşanmasıyla birlikte gündeme gelmektedir. Kişisel verilerin korunması hukuku da, ortaya çıkan verileri kimin, nasıl ve ne süre ile işleyeceği gibi sorulara yanıt arar. Bu yönüyle kişisel verilerin korunması yeni ortaya çıkan ve hukuki olarak korumaya muhtaç olan herhangi bir konudan farklıdır. Zira toplumsal hayatta yerini alan her insanın, kişiliğini korumaya ve geliştirmeye devam edebilmesi için bilgisel kendi kaderini tayin hakkına ihtiyacı vardır. Bu bağlamda kişisel verilerin korunması da bireyin bilgisel olarak kendini gerçekleştirmesiyle doğrudan

ilgilidir. Bu yönüyle değerlendirildiğinde kişisel verilerin korunması temel hak ve özgürlük olarak kabul edilmektedir.

İnsan ancak kendisini özgür hissettiği bir ortamda kendi öz benliğini gerçekleştirebilir. Gözetlendiğini hisseden ve bunu düşünerek yaşamak zorunda kalan kişi, birey olmanın sağladığı temel hak ve özgürlüklerini kullanmaktan kaçınır ve bunun neticesinde birey olma özelliğini kaybeder. Bu kaybın yarattığı zarar da bir o kadar büyük ancak tespiti zor bir noktaya gidebilir. Bu nedenle kişisel verilerin korunmasının toplumsal yaşamdaki huzurun korunması açısından dikkate alınması gerekmektedir.

Bir temel hak olarak kişisel verilerin korunmasının özel hayatın gizliliği, haberleşmenin gizliliği, mahremiyet, düşünce ve ifade özgürlüğü gibi birçok alan ile gösterdiği yakın ilişki, bu alandaki yapılacak çalışmaların ve düzenlemelerin çok geniş olması ile sonuçlamaktadır. Bu sebeple, kişisel verilerin işlenebileceği haller, ülkelerin mevzuatlarında kısıtlı bir alan içerisinde düzenlenip bir takım temel kurallara bağlanmıştır.

İnsan onuru kavramında yer bulan kişisel verilerin korunması hakkı günümüzde sahip olduğu önem nedeniyle çeşitli düzenlemelere konu edilmiştir. Bu düzenlemeler 1970’li yıllarda Avrupa’nın öncülüğünde başlamış ve gelişerek devam etmiştir. İlk kez 1970 yılında Almanya’nın Hessen eyaletinde kabul edilen kişisel verilerin korunması kanununun devamında Avrupa Konseyi tarafından 1981 tarihli Kişisel Verilerin Korunması Sözleşmesi ile ilk uluslararası belge kabul edilmiştir. Avrupa Birliği gerek bilgi teknolojileri alanında gerek Birlik içinde yaşanan gelişmeleri takip ederek mevcut düzenlemenin yetersiz kalması nedeniyle yeni çalışmalar yapmıştır. Bu çalışmalar neticesinde 1995 yılında 95/46/EC Sayılı Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiki Yönergesi hazırlanmış ve kişisel verilerin korunması konusunda mevzuat bağlamında bir düzenleme ortaya çıkmıştır.

95/46/EC sayılı Avrupa Birliği Veri Koruma Yönergesi; bilgi teknolojilerinin yeni gelişmeye başladığı bir dönemde kabul edilmiştir ve güncel gelişmeleri takip etmekten geri kalmıştır. Bunun yanı sıra yönergenin Avrupa Birliği’ne üye ülkelerin iç hukukunda doğrudan uygulanabilirliğinin olmaması da yeni bir düzenlemenin temel etkenlerinden olmuştur. Bu ihtiyaçlardan hareketle Mayıs 2016’da Avrupa

Birliđi Genel Veri Koruma Tüzüğü kabul edilmiştir. Tüzük ile birlikte kişisel verilerin korunması güçlendirilmiş ve veri işleyenlere önceki düzenlemelerle yüklenen sorumluluklar arttırılmıştır. Kişisel verilerin işlenmesinin hukuka uygunluk, adalet ve şeffaflık, amaç ile sınırlılık, en az seviyede bilgi, doğruluk, sınırlı süre ile saklama, bütünlük ve gizlilik, hesap verilebilirlik ilkeleri çerçevesinde yapılması gerektiđi 95/46/EC Sayılı Yönerge'nin geliştirilmesi niteliğinde Tüzük ile de vurgulanmıştır.

Tüzük'te, asıl olanın kişisel verilerin işlenmesinin yasak olduđu vurgulanmakla birlikte, verilerin veri sahibinin rızası, sözleşmenin geređinin yerine getirilmesi, hukuki yükümlülüğün yerine getirilmesi, hayati menfaatlerin korunması, kamu görevinin yerine getirilmesi ve meşru çıkarların korunması sebepleriyle işlenebileceđi belirtilmiştir. Bununla birlikte veri sahibine verileri işlenirken bilgi alma, verilerine erişme, düzeltme, unutulma, işlemenin kısıtlanması, verilerin taşınabilirliđi, itiraz hakkı tanınırken veri sorumlusuna da gerekli tedbirleri alma, işbölümü yapma, temsilci atama, kayıt tutma, uygun veri işleyen seçme gibi yükümlülükler getirilmiştir.

Veri sahibine tanınan tüm bu haklar ve veri sorumlusuna getirilen yükümlülüklerin uygulanmasının kontrolü de denetleyici ve düzenleyici kurumlara bırakılmıştır. Buna göre her üye ülkenin kendi bünyesindeki denetim makamları ve Avrupa Veri Koruma Kurulu denetleyici makamlar olarak kişisel verilerin korunmasında etkin kılınmıştır. Veri koruması idari, hukuki ve cezai başvuru yolları ile güvence altına alınmıştır.

Kişisel verilerin korunmasına yönelik geliştirilen mevzuatlarda temel olan kişisel verilerin işlenmesinin hukuka aykırı olmasıdır. Ancak bu temel kurala bazı istisnalar getirilerek veri işlemesi mümkün kılınmak istenmiştir. Zira toplumsal hayatın bir parçası olan insanların hayatının kolaylaşabilmesi, birtakım hizmetlerden faydalanabilmesi ve ticari faaliyetlerin verimli bir biçimde yürütülebilmesi için kişisel verilerin işlenmesi zorunludur. Bu zorunluluktan yola çıkılarak veri sorumlularına getirilen yükümlülükler, uygulanan yaptırımlar ile birleşince anlamlı hale gelmiştir.

Kişisel verilerin tarihsel süreç içerisindeki gelişmeleri ve tüm bu düzenlemeler veri korumasını bir üst boyuta taşımakla birlikte, halen tam anlamıyla

bir korumanın varlığından bahsetmek de güçtür. Zira üye ülkelerin denetim makamlarının kararlarına konu olduğu üzere, sonsuz genişlikteki bilgi teknolojilerinde tam anlamıyla koruma sağlanamamakta özellikle büyük miktarlarda veri işleyen işlem hacmi yüksek şirketlerden veri sızıntıları yaşanabilmektedir. Bunların önüne geçmek için de denetim makamları rekor miktarda cezalar uygulayarak emsal oluşturmaya çalışmakta ve veri sorumluları ile veri işleyenlerin yükümlülüklerini tam anlamıyla uygulamasını sağlamaya çalışmaktadır.

Çalışmamızın bütününde kişisel verilerin korunması hukukunun hayatımıza sağladığı katkılara işaret edilmiştir. Kişisel verilerin tarihsel gelişimi, kişisel verilerin korunmasının hukuk alanında yerini alması ve geçmişten günümüze Avrupa Birliği'nde yapılan düzenlemeler açıklanmıştır. Bu yönüyle bakıldığında kişisel verilerin korunmasının teorik ve pratik yönlerini içinde barındıran bir çalışma olmuştur.

Kişisel verilerin korunması hukuku ile ilgili yapılan çalışmaların değerlendirmeye alınarak veri korumasının artırılması ise uygulayıcılara düşen bir görevdir. Zira veri koruması ile ilgili getirilen kurallara veri işleyenlerin uymasını sağlamak yalnızca tek bir yöntemle mümkün değildir. Bu noktada, hem denetleme kurumları veri işleyenleri dikkatli bir şekilde takip etmeli ve gerektiğinde müdahale etmeli hem de veri sahipleri verilerine gereken önemi vermelidir. Zira, veri sahipleri verilerinin değerini anlayarak bu konuya hassas yaklaşmadıkları müddetçe veri işleyenlerin de sadece yüksek miktarlardaki cezalarla caydırılması mümkün değildir. Bu hususta denetim makamları ve ülkeler birlikte veri sahiplerinin bilinçlenmesi için sivil toplum çalışmaları yürütmeli, kişisel verinin ne anlama geldiği ve önemi veri sahiplerine öğretilmelidir. Bunun yanı sıra, veri sorumluları ve veri işleyenlerle de ortak çalışmalar yapılarak kişisel verilerin bir amaç değil araç olması gerektiği gerçeğiyle de yüzleşilmelidir.

Kişisel verileri işleyerek hizmet sunan kurum ve kuruluşlar, kişisel verilere amaç değil araç olarak yaklaşabildiği takdirde pek çok ihlalin önüne geçilmesi de mümkündür. Bunun için kurum ve kuruluşlarının reklam politikalarını bu bilinçle oluşturması ve hedef kitlesine sunduğu hizmeti bu yönde şekillendirmesi gerekmektedir. Örneğin, sosyal medya platformlarının kişisel veri toplayıp işleyerek kazanç sağlaması yerine üyelerinden üyelik bedeli alması pek çok ihlalin önüne

geçilmesinde etkin bir rol oynayacaktır. Ancak günümüzde bunun yerine kişisel veriler reklam amaçlı işlenmeye devam edilmekte ve ihlal engelini aşabilmek adına kullanıcılar verilerinin işlenmesine izin vermeye yönlendirilmektedir. Pek çok kişinin verdiği iznin içeriğini bilmeden işaretlediği küçük kutucuklar ile kişisel verilerin işlenmesinin önü açılmaktadır.

Tüm bu kötü niyetli uygulamaların önüne geçilmesinde en önemli görev ise devletlere ve denetim makamlarına düşmektedir. GDPR'nin kabulü ile, Avrupa Birliği'ne üye ülkelerin genelinde kişisel verilerin korunması konusunda hakim otoriteler ülkelerin denetim makamları olmuştur. Çalışmamızda değindiğimiz üzere denetim makamları emsal teşkil etmek adına rekor miktarlarda cezalar uygulayarak ihlallerin önüne geçmeye çalışmıştır. Ancak bu cezaların münferit olarak uygulanması kişisel verilerin korunmasının münhasır alanda kalmasına da neden olmuştur. Örneğin, Belçika denetim makamının Google Belçika için uyguladığı bir veri ihlali cezası, Google Inc.'nin veri ihlaline neden olan tutumunu yalnızca Belçika ve Birlik genelinde bakıldığında Avrupa Birliği ülkeleri için değiştirmesine neden olmaktadır. AB'ye üye olmayan ülkelerin vatandaşları ise tabi oldukları ülke hukuku politikasında değerlendirilmekte ve belki de aynı konuda ihlale maruz kalmaya devam etmektedir.

Dünya genelinde yeknesak bir uygulama sağlanmasının çok zor olmasıyla birlikte, üçüncü ülkelerin denetim makamlarının da veri ihlallerine yönelik kararları takip ederek kendi ülkesi açısından değerlendirmeye alması sorunun çözümü için etkili bir yöntem olabilecektir. Zira bu bilinçle hareket eden ülkeler karşısında veri işleyen kurum ve kuruluşlar da veri işleme politikalarını yeniden gözden geçirme gereği duyacaklardır. Bu sayede kişisel verilerin korunması hukuku, tarihsel süreçte de olduğu gibi Avrupa Birliği önderliğinde gelişecektir.

KAYNAKÇA

KİTAP

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

Altındere, Murat. **Kişisel Verilerin Korunması Hukuku ve Uygulaması**, Adalet Yayınevi, Ankara, 2020.

Aşıkoğlu, Şehriban İpek. **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, On İki Levha Yayıncılık, İstanbul, 2018.

Avrupa Birliği Temel Haklar Ajansı, **Handbook on European Data Protection Law**, Avrupa Birliği Temel Haklar Ajansı Yayınları, Luxemburg, 2018.

Aydın, Sedat Erdem. **AIHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, Oniki Levha Yayıncılık, İstanbul, 2015.

Ayözger, Ayşe Çiğdem. **Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması**, 2. Baskı, Beta Yayınları, İstanbul, 2019.

Aysun, Melike Köse. **Kişisel Verilerin Kaydedilmesi Suçu**, Seçkin Yayıncılık, Antalya, 2018.

Bart Custers, Alan M. Sears, Francien Dechesne, Ilina Georgieva, Tommaso Tani ve Simone Van der Hof. **EU Personal Data Protection in Policy and Practice**, Springer, The Hague, 2019.

Başar, Cemal. **Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması**, On İki Levha Yayınları, İstanbul, 2020.

Bayındır, Hamza. **Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması**, On İki Levha Yayınları, İstanbul, 2020.

Bilgi Edinme Değerlendirme Kurulu, **25 Soruda Bilgi Edinme Hakkı**, Bilgi Edinme Değerlendirme Kurulu Yayınları, Ankara, 2015.

Çekin, M. Serdar. **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, 2. Baskı, On İki Levha Yayınları, İstanbul, 2019.

Develioğlu, H. Murat. **6698 Sayılı Kişisel Verilerin korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayınları, İstanbul, 2017.

Fuster, G. Gonzalez. **The Emergence of Personel Data Protection as a Fundamental Right of the EU**, Springer, Belçika, 2014.

Gemicioğlu, Bora ve Zeynephan Gemicioğlu. **Kişisel Verilerin Korunması Mevzuatı Uluslararası Düzenlemeler ve İhtihatlar**, On İki Levha Yayınları, İstanbul, 2020.

Göçmen Uyarer, Sinem. **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, 2. Baskı, Seçkin Yayıncılık, Ankara, 2020.

Gür, İkbâl. **Kişisel Verilerin Korunması Hususunda AB İle ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Turhan Kitabevi, Ankara, 2010.

Helvacı, Serap. **Gerçek Kişiler**, 7. Baskı, Legal Yayıncılık, İstanbul, 2016.

Hizarci, Emine. **6698 Sayılı Kişisel Verilerin Korunması Kanununun AB Veri Koruma Hukuku Işığında Değerlendirilmesi**, Yetkin Yayınları, Ankara, 2020.

Kama Işık, Sezen. **Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış**, On İki Levha Yayıncılık, İstanbul, 2020.

Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, KVKK Yayınları, Ankara, 2019.

Küzeci, Elif. **Kişisel Verilerin Korunması**, Turhan Kitabevi, Ankara, 2010.

Mutlu, Muhammet Sefa. **Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması**, Adalet Yayınevi, Ankara, 2020.

Özcan, Göknıl. **Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması**, On İki Levha Yayınları, İstanbul, 2020.

Özek, Çetin. **Türk Basın Hukuku**, İstanbul Üniversitesi Hukuk Fakültesi Yayınları, İstanbul, 1978.

Özkan, Oğulcan. **Kişisel Verilerin Korunması**, Yetkin Yayınları, Ankara, 2020.

Raul, Alan Charles (Ed.). **The Privacy, Data Protection and Cybersecurity Law Review**, 6. Basım, The Law Rewiev, Londra, 2019.

Room, Stewart. **Data Protection&Compliance in Context**, Swindon, United Kingdom, The British Computer Society Publishing and Information Product, 2007.

Sert, Şeyma. **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Seçkin Yayıncılık, İstanbul, 2019.

Şimşek, Oğuz. **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Yayınları, İstanbul, 2008.

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

Tolun, Yüksel ve İslam Safa Kaya. **Uygulayıcılar İçin Türkiye’de ve Avrupa’da Kişisel Verilerin İşlenmesi KVKK- GDPR Karşılaştırması**, Adalet Yayınevi, Ankara, 2020.

Voight Paul ve Axel Von Dem Bussche. **The EU General Data Protection Regultaion (GDPR) A Practical Guide**, Springer, Almany, 2017.

Westin, Alan. **Privacy and Freedom**, ABD, 1970.

Yakışır, Ceren. **Türk Ceza Kanunu’nda Kişisel Verilerin Basın Yayın Yoluyla Açıklanması Suçu**, On İki Levha Yayınları, İstanbul, 2019.

MAKALE

Akçay, Ekrem Yaşar, Çiğdem Argun ve Elvettin Akman. “AB’nin Tarihsel Gelişimi ve Ortak Dış ve Güvenlik Politikası”, **Süleyman Demirel Üniversitesi Vizyoner Dergisi**, Cilt:3, Sayı:4, 2011, ss.117-131.

Akgül, Aydın. “Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı”, **Türkiye Barolar Birliği Dergisi**, Sayı: 116, 2016, ss.11-38

Akıllıoğlu, Tekin. “Yönetimde Açıklık-Gizlilik ve Bilgi Alma Hakkı”, **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, Cilt:46, Sayı:3-4, 1991, ss.1-12.

Akkurt, Sinan Sami. “Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış”, **Kişisel Verileri Koruma Dergisi**, Cilt:2, Sayı:1, 2020, ss.20-32.

Aşıkoğlu, Şehriban İpek. “Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-”, **Kişisel Verileri Koruma Dergisi**, Cilt:1, Sayı:2, 2019, ss.41-65.

Atak, Songül. “Avrupa Konseyi’nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler”, **Türkiye Barolar Birliği Dergisi**, Sayı:87, 2010, ss.90-120.

Bartow, Ann. “Our Data, Ourselves: Privacy, PropertizationandGender”, **University of San Francisco Law Review**, Cilt:34, 2000, ss. 685-760.

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

Başara, Gamze Turan. “Kişisel Veri İşleme Sözleşmesi”, **Uyuşmazlık Mahkemesi Dergisi**, Sayı:16, 2020, ss.57-90.

Bayraktar, Köksal. “Özel Yaşamın Gizliliğine Saygı İlkesi” **Maltepe Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:1,Sayı:1, 2007, ss.111-124.

Bulut, İpek Çimen.“Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları”, **Anadolu Üniversitesi Sosyal Bilimler Dergisi**, Cilt:20, Sayı:2, 2020, ss.127-145.

Büyükbay, Can. “Almanya’nın AB İçerisindeki Rolü: Uluslar arası Krizler Bağlamında Dış Politikada Süreklilik ve Değişim”, **Ege Stratejik Araştırmalar Dergisi**, Cilt: 8, Sayı:1, 2017, ss.19-38.

Dal, Ufuk. “Avrupa Birliği Genel Veri Koruma Tüzüğü’ nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslar arası Hukukta Meşruiyeti”, **Kişisel Verileri Koruma Dergisi**, Cilt: 1, Sayı: 1, 2019, ss.21-33.

Deniz, Bahar Yeşim.“Avrupa Birliği Hukukunda Temel Haklar ve Avrupa İnsan Hakları Sözleşmesi ile Etkileşim”, **Türkiye Barolar Birliği Dergisi**, Sayı:97, 2011, ss.49-74.

Dülger, Murat Volkan. “İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması”, **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:5, Sayı:1, 2018, ss.71-143.

Dülger, Murat Volkan.“Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”, **Yaşar Hukuk Dergisi**, Cilt: 1, Sayı: 2, 2019, ss.71-174.

Elmalica, Hasan .“Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:65, Sayı:4, 2016, ss.1603-1636.

Engels, Barbara.“Data Portability Among Online Platforms”, **Internet Policy Review- Journal on Internet Regulation**, Cilt:5, 2016, ss. 1-17.

Gülener, Serdar. “Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak 'Unutulma Hakkı’”, **Türkiye Barolar Birliği Dergisi**, Sayı: 102, 2012, ss.219-240.

Hornung, Gerritve ChristophSchnabel. “Data ProtectionIn Germany I: The Population Census Decision And The Right To Informational Self-Determination”, **Computer Law& Security Report**,Cilt:25, Sayı: 1, 2009, ss. 84-88.

İzgi, M. Cumhuriyet.“Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri”, **Türkiye Biyoetik Dergisi**, Cilt:1, Sayı:1, 2014, ss.25-37.

Karakaş, Işıl. “Ulusalüstü Anayasada Temel Haklar Problematığı: Teorik ve Pratik Sorunlar”, **Anayasa Yargısı Dergisi**, Cilt:21, Sayı:1, 2005, ss.31-38.

Kaya, Cemil. “ Avrupa Birliđi Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: 69, Sayı: 1-2, 2011, ss.317-334.

Kaygısız, Ümmühan. “Düşünce Özgürlüğüne Verilen Önem Açısından Hukuk Sistemlerine Kavramsal Bir Yaklaşım”, **Akademik Bakış Dergisi**, Sayı:52, 2015, ss.99-110.

Kılınç, Dođan. “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 61, Sayı: 3, 2012, ss.1089-1169.

Korkmaz, İlhan. “Facebook ve Mahremiyet: Görmek ve Gözetle(n)mek” **Yalova Sosyal Bilimler Dergisi**, Cilt:3, Sayı:5, 2013, ss.107-122.

Metin, Yüksel .“Avrupa Birliđi Temel Haklar Şartı”, **Ankara Üniversitesi Siyasal Bilimler Fakültesi Dergisi**, Cilt:57, Sayı:4, 2001, ss.35-63.

Nalbantođlu, Seray. “Bir Temel Hak Olarak Unutulma Hakkı”, **Türkiye Adalet Akademisi Dergisi**, Sayı:35, 2018, ss.583-605.

Ođuz, Habip.“ Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum”, **Uyuşmazlık Mahkemesi Dergisi**, Cilt:1 Sayı:3, 2013, ss. 1-38.

ROßNAGEL, Alexander .“Konflikte Zwischen Informationsfreiheit und Datenschutz?”, **MMR**, 2007.

Samuelson, Pamele. “Privacy As Intellectual Property?”, **Stanford Law Review**, Cilt: 52, 2000, ss.1130-1170.

Selek, Ozan. “Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 21, Sayı:2, 2019, ss.911-951.

Stuart, Allyson Haynes.“Google Search Results: Buried If Not Forgotten”, **North Carolina Journal Of Law&Technology**, Cilt: 15, 2014, ss. 463-518.

Tansuğ, Çağla. “Fransız Hukukunda Kişisel Verileri Koruma Otoritesi: CNIL” **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:14, Sayı:2, 2017, ss. 335-353.

Tatar, Volkan ve Nuri Gökhan Toprak, “Kendi Kaderini Tayin Kavramının Hukuki ve Siyasi Yönleri Üzerine Bir İnceleme”, **Bilge Strateji Dergisi**, Cilt:7, Sayı:13, 2015, ss.55-69.

Tekin, Nurullah. “Kişisel Verilerin Korunması İle İlgili Türkiye’deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi”, **Uyuşmazlık Mahkemesi Dergisi**, Sayı:4, 2014, ss.222-262.

Tezcan, Durmuş. “Bilgisayar Karşısında Özel Hayatın Korunması”, **Anayasa Dergisi**, Cilt: 8, 1991, ss. 385-392.

Yücedağ, Nafiye. “Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler”, **Kişisel Verileri Koruma Dergisi**, Cilt:1, Sayı:1, ss.47-63.

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, ss.765-789.

Yüksel, Mehmet. “Mahremiyet Hakkı ve Sosyo- Tarihsel Gelişimi”, **Ankara Üniversitesi Siyasal Bilimler Fakültesi Dergisi**, Cilt:58, Sayı:1, 2003 (Mahremiyet Hakkı), ss.181-213.

Yüksel, Mehmet. “Modernleşme ve Mahremiyet”, **Kültür ve İletişim Dergisi**, Cilt:6, Sayı:1, 2003, ss.75-108.

TEZ

Akgül, Aydın. **Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi**, (Yayımlanmamış Doktora Tezi), Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli, 2013.

Avcıoğlu, Nur Halet. **Türk Hukukunda Kişisel Verilerin Korunması Hakkı**, (Yayımlanmamış Yüksek Lisans Tezi), KTO Karatay Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2018.

Bozkurt, Habip. **Kişisel Verilerin İşlenmesinin Hukuki Boyutu**, (Yayımlanmamış Yüksek Lisans Tezi), Kadir Has Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul, 2019.

Mendos Kuşkonmaz, Elif. **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, (Yayımlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013.

Öz Demetoğlu, Gizem. **Türk ve Avrupa Birliği Veri Koruma Hukuku Bağlamında Blok Zincir Teknolojisinde Unutulma Hakkı**, (Yayımlanmamış Yüksek Lisans Tezi), Marmara Üniversitesi Avrupa Birliği Enstitüsü, İstanbul, 2019.

Türkel, Nagihan. **Özel Hayatın Gizliliğini İhlal Suçu**, (Yayımlanmamış Yüksek Lisans Tezi), Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir, 2010.

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

Yörük, Onur Doğan. (AB) 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Kişisel Verilerin Korunması, (Yayımlanmamış Yüksek Lisans Tezi), İzmir Ekonomi Üniversitesi Lisansüstü Eğitim Enstitüsü, İzmir, 2019.

İNTERNET

“What does it mean if you are joint controllers?” <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/> (01.05.2021).

2000/C 364/01 Sayılı Temel Haklar Şartı: https://sbb.gov.tr/wpcontent/uploads/2018/11/Avrupa_Birligi_Temel_Haklar_Sarti%E2%80%8B.pdf (06.04.2021).

Ahi, Şebnem. “Kişilere Kişisel Verileri Üzerinde Kontrol Yetkisi Veren Hak” **Aylık Bilişim Kültür Dergisi**, Ocak 2014, <http://www.bilisimdergisi.org.tr/bilisim-dergisi-sayilari/s161.pdf> (27.04.2021).

Avrupa Birliği Antlaşması <https://ab.gov.tr/files/pub/antlasmalar.pdf> (15.04.2021).

Benjamin May, Farah Bencheliha, “Data Protection And Privacy In France” <https://www.lexology.com/library/detail.aspx?g=eea3a783-f360-469d-986f-9434a7893c7f> (13.06.2021).

Data Protection and Cybersecurity Laws in Germany, <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/germany> (23.05.2021).

Federal Alman Veri Koruma Yasası “Undesgesetz zum Schutz natürlicher Personen beider Verarbeitung personenbezogener Daten” <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597> (04.01.2021).

Özgür Eralp, "Veri Sorumlusunun Meşru Menfaatleri için Veri İşlenmesinin Zorunlu Olması", <https://www.ozgureralp.com.tr/soru-327-ilgili-kisinin-temel-hak-ve-ozgurluklerine-zarar-vermemek-kaydiyla-veri-sorumlusunun-mesru-menfaatleri-icin-veri-islenmesinin-zorunlu-olmasi-ne-anlama-gelmektedir/> (13.03.2021).

The History of the General Data Protection Regulation, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (11.04.2021).

KARARLAR

Avrupa Konseyi Bakanlar Komitesi R(85) 20 Sayılı ve 25 Ekim 1985 tarihli kararı: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804bd336> (31.03.2021).

Avrupa Konseyi Bakanlar Komitesi R(86) 1 Sayılı ve 23 Ocak 1986 tarihli kararı: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804dd352> (31.03.2021).

ABAD'ın 12 Aralık 2013 tarihli ve C-486/12 sayılı kararı <https://curia.europa.eu/juris/document/document.jsf?text=&docid=145533&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5350641> (24.04.2021).

ABAD'ın 13.05.2014 tarihli ve C-131/12 sayılı kararı: <https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en> (19.03.2021).

ABAD'ın 1 Ekim 2015 tarihli ve C-201/14 sayılı kararı <https://curia.europa.eu/juris/document/document.jsf?text=&docid=168943&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=10950936> (24.04.2021).

ABAD'ın 24.09.2019 tarihli, C-136/7 sayılı kararı <http://curia.europa.eu/juris/document/document.jsf?docid=218106&doclang=EN> (14.01.2021).

Belçika Denetim Makamı'nın 14 Temmuz 2020 tarih ve 37/2020 sayılı kararı <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-372020.pdf> (28.04.2021).

CNIL'in SERGIC'e uyguladığı cezaya ilişkin karar <https://www.cnil.fr/en/node/114081> (23.01.2021).

Federal Alman Anayasa Mahkemesi 1 BvR 209/83 sayılı ve 15 Aralık 1983 tarihli kararı https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html (03.01.2021).